将多个ISE集群与基于TrustSec的策略的安全网络 设备集成

目录

简介 先决条件 要求 使用的组件 限制 网络图 配置 ISE 配置 启用SXP 在群集节点上配置SXP 在汇聚节点上配置SXP 在聚合节点上启用pxGrid pxGrid自动审批 网络设备TrustSec设置 网络设备授权 SGT 授权策略 在ISE汇聚节点上启用ERS(可选) 将用户添加到ESR管理员组(可选) 安全Web设备配置 pxGrid证书 在安全Web设备上启用SXP和ERS 标识配置文件 基于SGT的解密策略 交换机配置 AAA **TrustSec** 验证 相关信息

简介

本文档介绍通过pxGrid将来自多个ISE部署的安全组标记(SGT)信息发送到单个思科安全网络设备 (正式版网络安全设备WSA)以在TrustSec部署中利用基于SGT的Web访问策略的过程。

在版本14.5之前,安全网络设备只能与单个ISE集群集成基于SGT的身份策略。通过引入此新版本 ,安全网络设备现在可与来自多个ISE集群的信息进行互操作,并在它们之间汇聚一个单独的ISE节 点。这带来了巨大的好处,使我们能够导出来自不同ISE集群的用户数据,并自由控制用户可以使 用的退出点,无需1:1集成。

先决条件

要求

Cisco 建议您了解以下主题:

- •身份服务引擎 (ISE)
- 安全Web设备
- RADIUS协议
- TrustSec
- pxGrid

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 安全Web设备14.5
- ISE版本3.1 P3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

限制

1. 所有ISE集群需要为SGT维护统一的映射。

- 2. ISE汇聚节点必须拥有其他ISE集群的SGT名称/编号。
- 3. 安全Web设备只能根据SGT标记识别策略(访问/解密/路由),而不能识别组和用户。
- 4. 报告和跟踪基于SGT。
- 5. 现有的ISE/安全Web设备规模调整参数继续适用于此功能。

网络图



Process:

1.当最终用户连接到网络时,他们根据ISE中的授权策略接收SGT。

2.然后,不同的ISE集群通过SXP将此SGT信息以SGT-IP映射的形式发送到ISE汇聚节点。

3. ISE汇聚节点接收此信息并通过pxGrid与单个安全网络设备共享。

4.安全Web设备使用它学到的SGT信息,根据Web访问策略向用户提供访问权限。

配置

ISE 配置

启用SXP

步骤1.选择三行图标 ____ 位于左上角,在Administration > System > Deployment中选择。

步骤2.选择要配置的节点,然后点击编辑。

E Cisco ISE			Administration • S	ystem			a	0 23	1
Deployment Licensing	Certificates	Logging	Maintenance	Upgrade He	alth Checks Bac	kup & Restore	Admin Access	Setting	5
Deployment	• De	eployme	nt Nodes				Selected 1 Tota		
는 꽃 Deployment 35- PAN Failover	0	late 🔒 Region	r D Syncup 🗟	Deregister				M ~	
	C	Hostname	A Personas		Role(s)	Services		Node Status	
		ise01-CL1	Administratio	n, Monitoring, Policy S	envice STANDALONS	SESSION, PROFILE	R		

步骤3.要启用SXP,请勾选框Enable SXP Service

E Cisco	SE		A	dministration • S	ystem			Q.	0580
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 🕣					
			C 646	ie Threat Centric NAC 5	iervice 🕞				
			-	Enable SXP Se	rvice 🧿				
				Use interface	GigabitEthernet	0	~		

步骤4.向下滚动到底部,然后点击保存

注意:对每个集群中的其他ISE节点(包括汇聚节点)重复所有步骤。

在群集节点上配置SXP

步骤1.选择三行图标 ── 位于左上角,然后选择 **工作中心> TrustSec > SXP。**

步骤2.点击+Add将ISE汇聚节点配置为SXP对等体。

≡ Cisco	ISE	W	ork Centers - T	rustSec					Q	0	58	0
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings				
SXP Devices All SXP Mappings		SXP Devi	ces 💿									
						Rows/Page 2	✓ K < 1	/>>) [Go	2	Total R	OWS
		C Refresh + Ad	id 🛛 Trash 🗸 🖉	East A	ssign SXP (Domain				⊽ ra	# ~	٥

步骤3.定义ISE聚**合节**点**的名**称和IP地址,选择对等角色作为LISTENER。在**连接的PSN**、所需的 SXP域下选择所需的PSN,在"状态"下选择**启用**,然后选择**密码类型**和所需的**版本**。



Overview Component	TrustSec Policy Policy Sets SXP	ACI
SXP Devices	SXP Devices > SXP Connection	
All SXP Mappings	 Upload from a CSV file 	
	- Add Single Device	
	Input fields marked with an asterisk (*) are required.	
	Name ISE Aggregation node	
	IP Address * 10.50.50.125	
	Peer Role • LISTENER V	
	Connected PSNs * ise01-CL1 ×	



Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI
SXP Devices		SXP Domains *			
All SXP Mappings		default ×		\sim	
		Status *			
		LINDIGU			
		Password Type * CUSTOM		~	
		Password			
		Version *			
		Advanced Cettings			
		 Advanced Settings 	Cancel	Save	

步骤4.单击保存

注意:对每个集群中的其他ISE节点重复所有步骤,以构建与汇聚节点的SXP连接。在汇聚节点上重复相同的过程,并选择SPEAKER作为对等角色。

在汇聚节点上配置SXP

步骤1.选择位于左上角的三行图标,然后在"工作中心">"TrustSec">"设置"中进行选择

第二步:单击SXP Settings选项卡

步骤3.要传播IP-SGT映射,请勾选在pxGrid上发布SXP绑定复选框。



第4步(可选):在Global Password下定义SXP设置的默认密码



步骤5.向下滚动并点击保存。

在聚合节点上启用pxGrid

第1步:选择位于左上角的三行图标,然后在Administration > System > Deployment上选择。

步骤2.选择要配置的节点,然后点击编辑。

E Cisco ISE	Admini	stration • System				····· • Q. @	- 50 ·	0
Deployment Licensing Certificates	Logging Maint	enance Upgrade	Health Checks	Backup & P	Nestore Adr	min Access S	lettings	
Deployment C C C C C C C C C C C C C	Deployment	Nodes	v			Selected 1 T	obei 1 (2) Ali V	0 7
Ab Long Lamburg	Hostname	Personas		Role(s)	Services		Node Sta	atus
	E 100-000	Administration, Monitori	ng, Policy Service	STANDALONE	SESSION, PROFILER		•	

步骤3.要启用pxGrid,请点击pxGrid旁边的按钮。

Cisco ISE	Administration - System	0.0510
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
	Enable Session Services ()	
	inclute Notes in Notes Group Notes 🗸 😲	
	🚺 Enable Probing Service 💮	
	🗌 Enatin Tread Centre NHC Server 💿	
	Enable SXP Service ()	
	Use montain disposit/Dennet 0 V	
	📄 Enaltie Geura Admin Sanura 💿	
	📄 Enative Paracear country Service 💿	
	Shirks	

步骤4.向下滚动到底部,然后点击**保存。**

pxGrid自动审批

第1步:导航到左上角的三行图标并选择管理> pxGrid服务>设置。

第二步:默认情况下,ISE不会自动批准pxGrid来自新pxGrid客户端的连接请求,因此必须通过选中Automatically approve new certificate-based accounts复选框启用该设置。

≡ Cisc	O ISE		Administration - pxGrid Services
Summary	Client Management	Diagnostics	Settings
Sett	tings		
☑ A	utomatically approve new certific llow password based account cre	ate-based accounts ation	
	Use (Default Sa	ove

步骤3.点击保存

网络设备TrustSec设置

对于思科ISE处理来自支持TrustSec的设备请求,您必须在思科ISE中定义这些支持TrustSec的设备。

步骤1.导航至位于左上角的三个行图标,然后在Administration > Network Resources > Network Devices中选择。

第二步:单击+Add。



步骤3.在Network Devices部分和RADIUS Authentication Settings中输入所需的信息。

步骤4.选中Advanced TrustSec Settings复选框以配置启用TrustSec的设备。

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

第5步:点击Use Device ID for TrustSec Identification**复选框**,以自动填充Network Devices(网络 设备)部分中列出**的设备**名称。在**密码**字段中输入密码。

Cisco ISE		Administration • Netw	vork Resources
Network Devices	Network Device Groups	Network Device Profile	s External RADIUS Servers
Network Devices	🗹 🗸 Advar	nced TrustSec Setting	gs
Default Device Device Security Settings	V Devic Use Devic Identificati	e Authentication Se ^{b ID for TrustSec}	ttings
	Device Id	SW1	
	* Passwor	nd Sh	low

注意:ID和密码必须与随后在交换机上配置的"cts credentials id <ID> password <PW>"命令 匹配。

步骤6.选中**Send configuration changes to device复**选框,以便ISE可以向设备发送TrustSec CoA通 知。

Cisco ISE		Administration - Network	Resource	205			
Network Devices	Network Device Groups	Network Device Profiles	Externa	I RADIUS Ser	rvers	RADIUS Server Sequences	More 1
Network Devices							
Default Device	V Tru	stSec Notifications and U	pdates				
Device Security Settings			1				
	* Down	ricad environment data every	Days	~			
			1				
	* Dow	rioad peer authorization policy every	Days	~			
			1				
	* Real	thertication every	Days	¥ (0)			
			1				
	* Down	ricad SGACL lists every	Days	v			
	Other 1	ivatfiec devices to trust this device					
	Send o	onfiguration changes to device		sing 🔘 Co	4 0	cu	

步骤7.选中Include this device when deploying Security Group Tag Mapping Updates复选框。

步骤8.要让ISE编辑网络设备的配置,请在EXEC Mode Username和EXEC Mode Password字段中 输入用户凭证。或者,在启用模式密码字段中提供启用密码。

注意:对要成为TrustSec域一部分的所有其他NAD重复上述步骤。

网络设备授权

第1步:选择位于左上角的三行图标,然后依次选择工作中心(Work Centers)> TrustSec > TrustSec**策略(TrustSec Policy)。**

第二步: 在左侧窗格中, 单击网络设备授权。

Overview Components	TrustSec Policy	Policy Sets	SIP	ACI	Troubleshoot	Reports	Settings			
press Policy ~	Network [Device A	uthor	izatio	n	ines. Dran and	dross subre to channe to	The center		
						rotal or equip of the	Contraction of the state			
Matrix Source Tree	Curla Curla	aut Rule		no ruhes defin	and or no match	then The	thet_Devices	tot ×		

步骤3.在右侧,使用上文Edit 和Insert new row 旁边的下拉列表创建新的NDA规则。



第4步:定义规则名称、条件,并从Security Groups下的下拉列表选择适当的SGT。

步骤5.点击最右边的**完成。**

E Cisco ISE	Work (Q. ©	50 d						
Overview Components	TrustSec Policy Policy Sets	SXP ACI Troubleshoot	t Reports Settings						
Egress Policy ~ ~	Network Device A	Network Device Authorization							
Source Tree	Rule Name	Conditions	Security Group						
Destination Tree	🗄 🖪 🔧 NDAD	# DEVICE Device Type equals to	v ten Tustler,Devices v Dove						
	Default Bule	If you rules defined or no match	thes Trustlast Devices 540 -						

步骤6.向下滚动并点击保存。

SGT

第1步:选择位于左上角的三行图标,然后在"工作中心"(Work Centers)>"TrustSec"(TrustSec)>"组 件"(Components)中选择。

第二步: 在左侧窗格中,展开Security Groups。

步骤3.点击+Add以创建新的SGT。

I Cisco	ISE	Work Centers - TrustSec							0.0000
Overview	Components	TrustSec Policy	Policy Sets	SIP	ACI	Troubleshoot	Reports	Settings	
Security Groups	_	A							
P 567 State Mapp	ing .	Security	Groups						
Security Group ACI	La .	For Policy Expert print	Adventitution - Santa	n - Dathap K	Index - Pa	ka Expert Page			
Network Devices		_							Selected 1 Total 18 门
Traduct Servers		1 400 + 400	de travel d	5 Baset V	0.14	a v 💿 na	() Yests Depte		м. – У

步骤4.输入名称,然后在相应字段中选择一个图标。

Cisco ISE	Work Centers · TrustSec							
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoo							
Security Groups	Security Groups List > New Security Group							
P SGT Static Mapping	Security Groups							
Security Group ACLs								
Network Devices	* Name							
Trustsec Servers >	Cluster1_Endpoints							
	* Icon							
	🖵 🖨 🛢 🗨 🕸 🜲 🗲							

步骤5.(可选)为其提供说明并输入标记值。

注意:为了能够手动输入标记值,导航到工作中心(Work Centers)> TrustSec >设置 (Settings)> General TrustSec设置(General TrustSec Settings),并选择安全组标记编号 (**Security Group Tag Numbering)下的选项User Must Enter SGT Number**。

步骤6.向下滚动并点击Submit

注意:对所有必需的SGT重复这些步骤。

授权策略

第1步:选择位于左上角的三行图标,然后在Policy > Policy Sets中选择。

第二步:选择适当的策略集。

步骤3.在策略集中,展开授权策略。

= C	sco ISE	1	Policy + Policy Sets				Q. 0	53 O
Policy 5	Sets-+ Wired Access					Reset	Reset Policyset Hitcourts	lave -
514	tus Policy Set Name	Description	Condition				Allowed Protocols / Server Sequence	- 18%
(0,	Search							
	Wood Access				DEVICE Device Paper EQUALS AT Device PapersHaltschutes		Default Network Access	
					Radio NG Part Type EQUICS Etherne			
) Aith	entication Policy (2)							
) Auto	orization Policy - Local Exception	pra.						
> Auto	orization Policy - Global Except	iona						
> Auto	origation Policy (1)							



 Antesentation month (1) 					
		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

第5步:定义所需的规则名称、条件和配置文件,然后从Security Groups下的下拉列表中选择适当的SGT。

- Authorization Policy (1)				
		Results		
Status Rule Name	Conditions	Profiles	Security Groups	Hits Actions
Q Sect				
O Datte-Pallay	(C Winters, 812.1X	PermitAccess x	V 🔶 Chuster 1, Endpoints 🛛 🗠 V	+ 0

步骤6.点击保存。

在ISE汇聚节点上启用ERS(可选)

外部RESTful API服务(ERS)是WSA可以查询组信息的API。默认情况下,ISE上禁用ERS服务。启 用后,如果客户端作为ISE节点上的**ERS Admin组成员进行身份验证,则可**以查询API。要在ISE上 启用服务并将帐户添加到正确的组,请执行以下步骤:

步骤1.选择位于左上角的三行图标,然后在Administration > System > Settings上选择。

第二步:在左侧窗格中,单击ERS Settings。

≡ Cisco IS	SE		A	dministration • S	ystem			Q	0 🖓
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Client Provisioning FIPS Mode	Í	ERS S	Settings						
Alarm Settings		✓ Genera	d.						
Posture		External RE The DRS so An ISE Add	STM Services (D rivice is disabled t rivistrator with the	(5) is a REST API based y default. "ERS-Admin" or "ERS	on HTTPS over p	ort 9060. assignment is required to a	use the API.		
Profiling		For more in https://10.5	0 50 125 9000/ers	visit the ERS SDK page look	at:				
Protocols									
Endpoint Scripts	>	✓ ERS Se	tting for Adr	ninistration Node					
Proxy		O Enable	DIS forhead Write						
SMTP Server		O Daubh	DAS						
SMS Gateway									
System Time									
ERS Settings		CSRF (CSR	Check						

步骤3.选择选项Enable ERS for Read/Write。

步骤4.单击保存并使用OK确认。

将用户添加到ESR管理员组(可选)

第1步:选择位于左上角的三行图标,然后选择Administration > System > Admin Access

第二步: 在左侧窗格中,展开Administrators,然后单击Admin Users。

第3步:点击+Add并从下拉列表中选择Admin User。

≡ Cisco I	SE		Ac	iministration • S						
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	
Authentication		Admir	nistrators	5						
Authorization	>			-				Selected () Total 1 🦪	٥
Administrators	~	O ton .	+ Add 🛞 o	hange Status	Delese 0 0	uplicate			AL V	V
Admin Users		-								
Admin Groups			Create an Admir	User	Description	First Name	Last Name Email /	Address Admin G	oups	
			Select from Net	work Access Users	> Default Admir	User		Super Adr	nin	
Settings	>									

步骤4.在相应的字段中输入用户名和密码。

I Cisco ISE	Administration - System	0.0 23 0		
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings		
Authentication	Administrators Dat 3 with			
Authorization >	→ Admin User			
Administrators \sim	*Name with			
Admin Usors	11 M ⁻¹			
Admin Groups	Ernal Enabled V			
berings 2	External Only Defendence Court never disabled			
	~ Password			
	* Password			
	* Ro-Enter Parssond			

第5步:在Admin Groups字段中,使用下拉菜单选择ERS Admin。

≡ Cisco	ISE		A	dministration • S	ystem			Q,	0 58 O
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		First Name							
Authorization	>	Last Name							
Administrators	~								
Admin Users		w harme	. Outines						
Admin Groups		Description	ie Opeions						
Settings	>								
		 Admin Ξ 	Groups ERS Admin		× +				
								Save	Reset

步骤6.点击保存。

安全Web设备配置

根证书

如果集成设计使用内部证书颁发机构作为WSA和ISE之间的连接的信任根,则必须在两台设备上安 装此根证书。

第1步:导航到Network > Certificate Management,然后单击Manage Trusted Root Certificates以添加CA证书。

	Secure web Appliance		Secure Web Appliance is getting a new look. Try				
Reporting	Web Security Manager	Security Services	Network	System Administration			
Certificat	e Management						
Appliance Cer	tificates						
Add Certificat							
Certificate	Common Name Issuer	d By Domains	Status Time I	Remaining Expiration	Date Delete		
Weak Signate	re Usage Settings						
	Restrict Weak Signature Usage:	Disabled					
					Fully Cathlorne		
					the second		
					(List Month)		
Certificate FQ	ON Validation Settings			_			
Certificate 1Q	DN Validation Settings Certificate FQDN Validation Usage:	Disabled					
Certificate 1Q	DN Validation Settlings Certificate FQDN Validation Usage:	Disabled			Edit Settings		
Certificate 10	DN Validation Settings Certificate FQDN Validation Usage:	Disabled	_		Edit Settings		
Certificate 1Q	DN Validation Settings Certificate FQDN Validation Usage:	Disabled	=		tok Semiga		
Certificate IQ Certificate Lis Updates	ON Validation Settings Certificate FQDN Validation Usage: Is	Disabled		Consult Interior	Edit Settings		
Certificate IQ Certificate Lis Updates File Type	ON Validation Settings Certificate FQDN Validation Usage: Is	Disabled Last Update	E-12-47 3033	Current Version	Edit Settings		
Certificate 1 Q Certificate 1 is Updates File Type Cisco Trutted R Cisco Crutted R	ON Validation Settings Certificate FQDN Validation Usage: Is oot Certificate Bundle • Nocked Use	Disabled Last Update Success - Thu Jun 30 1 Success - Wed Min 11	15:32:47 2022 31:04:06 2022	Current Version 2.1 1.3	Edit Settings		
Certificate 10 Certificate 18 Updates File Type Caco Trutted R Caco Certificat No updates in 1	ON Validation Settings Certificate FQDN Validation Usage: Is oot Certificate Bundle e Biocked Ust morress.	Disabled Last Update Success - Thu Jun 30 1 Success - Wed May 11	15:32:47 2022 21:04:06 2022	Current Version 2.1 1.3	Edit Settings New Update Not Available Not Available		
Certificate I Q Certificate I is Updates File Type Cisco Trusted R Cisco Certificat No updates in p	ON Validation Settings Certificate FQDN Validation Usage: Is oot Certificate Bundle e Biocked Ust migness.	Disabled Lest Update Success - Thu Jun 30 1 Success - Wed May 11	15:32:47 2022 21:04:06 2022	Current Version 2.1 1.3	Edit Settings New Update Not Available Not Available Update New		
Certificate I Q Dydates File Type Cisco Trusted R Cisco Certificat No updates in p Certificate	ON Validation Settings Certificate FQDN Validation Usage: Is oot Certificate Bundle e Blocked Ust migness. Hanagement	Disabled Last Update Success - Thu Jun 30 1 Success - Wed May 11	5:32:47 2022 21:04:06 2022	Current Version 2.1 1.3	Cole Settings New Update Not Available Not Available Update New		



步骤3.单击Choose File以查找生成的根CA,然后点击Submit。

步骤4.重新点击Submit。

步骤5.在右上角,点击Commit Changes。

1	Cisco Secure Web Appliance			Decare Web Applance is getting a new look. Try if I			 Engel 8 in adult of anti-anti-physical References - Canara - Support and 9 		
•	Reporting	Web Security Manager	Security Services	Network	System Administration				
									Connet Charges a

步骤6.重新点击Commit Changes。

pxGrid证书

在WSA中,创建密钥对和证书供pxGrid使用作为ISE服务配置的一部分完成。

步骤1.导航到网络>身份服务引擎。

步骤2.单击启用和编辑设置。

步骤3.单击Choose File以查找生成的根CA,然后点击Upload File。

Infer The Imb Appliance will communicate with the 200 period node to support Imb Appliance data subscription (sequing updates). A primary 20 period mole (server) must be configured.
(Instrume or Dvet address)
ttill pedint teole Centricate:
If the ISE patient orable conflictent is signed by a Confliction Authority, confirm that the Conflicte Authority is balant in the Tonabal floot Cartification link (see Network is Cartificate Network) and splote the CA-signed not cartificate balant, the cartificate is self-append, expand the cartificate from the ISE patient inde to add balant. You can uplant the orablest and that includes any intermediate cartificate
Certification Onesee File No The Ocean

注意:常见的错误配置是上载此部分中的ISE pxGrid证书。必须将根CA证书上传到ISE pxGrid节点证书字段。

第4步:在Web设备客户端证书部分,选择使用生成的证书和密钥。

Web Appliance Client Certificate:	For secure communication between the Web Appliance and the ISE peGrid servers, provide a client certificate. This may need to be uploaded to the ISE peGrid node(s) configured above.
	O Use Uploaded Certificate and Kay
	Certificate: Crucos File As the chosen Upload Files
	Key: Crocos Fin has the chosen
	Key is Encrypted
	No certificate has been uploaded.
	Use Generated Certificate and Key Generate New Certificate and Key

第5步:单击Generate New Certificate and Key按钮并填写所需的证书字段。

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

步骤6.点击Download Certificate Signing Request。

注意:建议选择**Submit**按钮提交对ISE配置的更改。如果在提交更改之前会话超时,则即使已 下载CSR,生成的密钥和证书也会丢失。

第7步:在与CA签署CSR后,点击选择文件以查找证书。

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
	Kiey is Encrypted
	No certificate has been uploaded.
	Use Generated Certificate and Key Generate New Certificate and Key
	Common name: wsa.security/ab.net
	Organizational Unit: Security
	Country: SI
	Expiration Date: May 10 19:19:26 2024 GMT
	Basic Constraints: Not Critical
	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

步骤8.点击上传文件。

步骤9.提交并提交。

在安全Web设备上启用SXP和ERS

步骤1.单击SXP和ERS的Enable按钮。

194 907 elicharge Protocol (3947) Service:	Enabling the service, Web Applance will retrieve SHP Binding Typic from ISE Services.
	- Fourier
Enable INE External Restful Service (URS)	
The Web Applance retrieves Active Directory proups, and iscal 201 pr Group Tape (2007)0, you whost anothe 2001.	supe from 25E using the 28S. If you are configuring the Web Applanor's policies using Active Directory groups, or in combination with facure

第2步:在ERS Administrator Credentials字段中,输入在ISE上配置的用户信息。

步骤3.选中与ISE pxGrid节点相同**的服务器名称的复选框,**以继承早期配置的信息。否则,请在此 处输入所需信息。

C Enable ISE External Restful Service (ERS)			
	ERS Administrator Credentials		
	Username:	WSA	
	Password:		
	ERS Servers		
	Server name same as 15E pxGrid Node		
	Primary:	ise-agg.securitylab.net	(Hostname or IPv4 address)
	Secondary (Optional):		(Hostname or IPv4 address)
	Port:	9060 (Enter the port m	mber specified for ERS in ISE)

步骤4.提交并提交。

标识配置文件

为了在WSA策略中使用安全组标记或ISE组信息,必须首先创建标识配置文件,该配置文件利用 ISE作为透明标识用户的方法。

步骤1.导航到Web Security Manager > Authentication > Identication Profiles。

步骤2.单击Add Identification Profile。

步骤3.输入名称和说明(可选)。

第4步:在Identification and **Authentication部分,**使用下拉菜单选择**Transparently identify users** with ISE。

Identification Profiles: Add Profile

Enable Identification Profile	
Name: 🕐	ISE Profile (e.g. my IT Profile)
Description:	Identification profile for ISE Integration. (Hastimum allowed characters 256)
Insert Above:	2 (Global Profile) 🛩
Identification Hethod	
Identification and Authentication: 🕐	Transparently identify users with ISE V
Fallback to Authentication Realm or Guest Privileges: 1	If user information is not available from the Identity Services Engine:
	Support Guest Privileges V
	Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).
arabia Pafialtian	
section is defined for any combination of the f	clination and one. All reliants so at he must for the notice in take affect
an proprior commend by any companies of the A	where A shows we make a make on the bard to take party.
Unive Members by Subnet:	(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 3001:420:80:1:15, 2000:408::1-3000:408::10)
Define Members by Protocol:	нттрунттря

步骤5.提交并提交。

基于SGT的解密策略

步骤1.导航到Web Security Manager > Web Policies > Decryption Policies。

步骤2.点击Add Policy。

步骤3.输入名称和说明(可选)。

第4步:在标识配置文件和用户部分,使用下拉菜单选择选择一个或多个标识配置文件。

第5步:在Identification Profiles部分,使用下拉列表选择ISE标识配置文件的名称。

第6步:在Authorized Users and Groups部分,选择Selected Groups and Users。

Identification Profiles and Users:	Select One or More Identification	Profiles 👻	
	Identification Profile	Authorized Users and Groups	Add Identification P
	ISE Profile V	All Authenticated Users Selected Groups and Users ISE Secure Group Tage: No tage entered ISE Groups: No groups entered Users: No users entered Users: No users entered Guests (users failing authentication)	8
	Authentication information may not proxy traffic, user agent information	be available at HTTPS connection tim is unavailable for decryption policies	e. For transparent
h Advanced	Aufles additional areas manhaukin		

步骤7.点击ISE Secure Group Tags旁边的超链接。

第8步:在Secure Group Tag Search部分,选中所需SGT右侧的框,然后点击Add。

f Secure Group Tags. To remove ided in this policy.	Secure Group Taps from this policy, use the Delete option	n.	
SGT Number	SGT Description	Delete	Ī
111	Endpoints residing in ISE Cluster-1	0	
111	Endpoints residing in ISE Cluster-1	A4	
	I Secure Group Tags. To remove ded in this policy. SGT Number 111	I Secure Group Tage. To remove Secure Group Tage from this policy, use the Delete optio ded in this policy. BGT Number BGT Description 111 Endpoints residing in ISE Cluster-1	I Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option. ded in this policy. BGT Number BGT Description Delete All 111 Endpoints residing in ISE Cluster-1 Image: Cluster-1

ecure Group Tag Search			
Enter any text to search for a Se Add button to add to this policy. Search	oure Group Tag name, number, or o	lescription. Select one or more Secure Group Tags from th	e list and use the
0 Secure Group Tag(s) select	ed for Add		
Secure Group Tag Name	SGT Number	SGT Description	Select At
Production_Servers	11	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
8Y00	15	8YOO Security Group	0
PCI_Servers	14	PCI Servers Security Group	0
Guests	6	Guest Security Group	0
ANY	65535	Any Security Group	0
Unknown	0	Unknown Security Group	0
Network_Services	3	Network Services Security Group	0
TrustSec_Devices	2	TrustSec Devices Security Group	0
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	
Employees	4	Employee Security Group	

步骤9.单击"**完成**"返回。

步骤10.提交并提交。

交换机配置

AAA

aaa new-model

```
aaa group server radius ISE
server name ise01-cl1
server name ise02-cl1
ip radius source-interface Vlan50
```

```
aaa authentication dotlx default group ISE
aaa authorization network ISE group ISE
aaa accounting update newinfo periodic 2440
aaa accounting dotlx default start-stop group ISE
```

```
aaa server radius dynamic-author
client 10.50.50.120 server-key Ciscol23
client 10.50.50.121 server-key Ciscol23
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 Ciscol23

TrustSec

cts credentials id SW1 password Ciscol23 (This is configured in Privileged EXEC Mode) cts role-based enforcement

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

验证

从ISE到终端的SGT分配。

在这里,您可以看到来自ISE集群1的终端在成功身份验证和授权后分配了SGT:



在这里,您可以看到来自ISE集群2的终端在成功身份验证和授权后分配了SGT:



SXP映射

1

由于群集ISE节点和ISE汇聚节点之间启用了SXP通信,这些SGT-IP映射通过SXP通过ISE汇聚获取

III Oleco ISE		Work Centers	+ TrustSec			A Description	
Overview Components	Trustlec Policy P	No 90 AD	Troubleshoot	Reports Settings			
Self-Services All SAF-Beggings	All SXP Ma	ppings o					
					2000/Page	<u>v</u> (<u>)</u> (1) In A Southeast
	(2 hotes) And Set	Senain Star - Maraga StP Donain S	itere .				View - 0
	IP Address	907	100	Loarond From	Learned By	SNP bonain	PDNs involved
	10.00.00.0/02	Turbs, Jacob (2003)		103030121210030303	547	anut	14 100
	10.00.00.1102	Testino, Jacob (2001)		10.00.001123.10.00.007	547	arout	144-400
	16.06.00.12/38	DenterT_Evaluations (117,0000)		10.00.00.121.20.00.00.0	547	default.	144-400
	10/00/10/10/10	Owner, Endprint (20210000)		10/06/00 123,70 00:00 7	547	defect.	144-100

这些SXP映射来自不同的ISE集群,然后通过pxGrid通过ISE汇聚节点发送到WSA:



基于SGT的策略实施

在这里,您可以看到不同的终端与其各自的策略匹配,并且根据其SGT阻止流量:

属于ISE集群1的终端

This	Page Cannot Be Displayed
Based been b	on your organization's access policies, access to this web site (https://bbc.com/) has locked.
If you h codes :	ave questions, please contact your organization's network administrator and provide the shown below.
Date: T	hu, 14 Jul 2022 14:28:16 CEST
Usema	ne: lsesxp_10.50.50.121_sgt111_10.50.50.12 IP: 10.50.50.12

Recounts					
					Items Displayed 50 🛩
Displaying 1 - 50 of 13	7 items.				< Previous 1 2 3 Next
Time (GRT +02:00) +	Website (zourt)	Display All Details	Disposition	Bandwidth	User / Client 3P
54 34 2022 54 28 57	Masu//bio.com/dt/Taricon.ico content invel. os.contexton Block URLs CL1 contentation UP. contexton U	r1", WBRS: No Score,	Block - URL CH	ce	isessg_10.50.50.121_sg111_10.50.50.12 (SeeRified by 10) 10.50.50.11

属于ISE集群2的终端

r

	() Notification: Policy: Destination ×				+
\leftarrow	\rightarrow	C	Ô	https://www.fa	cebook.com

This	Page Cannot Be Displayed								
Based (https:	Based on your organization's access policies, access to this web site (https://www.facebook.com/) has been blocked. If you have questions, please contact your organization's network administrator and provide the codes shown below.								
If you codes									
Date: Usern Souro URL: Categ Reaso Notific	Thu, 14 Jul 2022 14:23:58 CEST ame: isesxp_10.50.50.122_sgt222_10.50. e IP: 10.50.50.13 GET https://www.facebook.com/ ory: Block URLs CL2 m: UNRNOWN ation: BLOCK_DEST	50.13							
Displaying 1 - 2 of 2 ite	ma								
Time (GMT +02:00) *	Website (count) Display Al Details	Disposition	Bandwidth	User / Clark IP					
14 Jul 2022 14:23-58	https://www.facebook.com/403/favion.los comment inne - us. CATEGON Block URLs CL2 DESTRUCTION IN - CONTINUE - Constraint - Palloy: "255_Chater2", w885: No Score, Malware Analysis File VenSct -	Block - URL CH	08	isesus_10.50.50.122_sgt222_10.50.50.13 (Destified by 158) 10.50.50.13					

相关信息

- 网络安全设备和身份服务引擎集成指南
- <u>为 TrustSec 感知服务配置 WSA 与 ISE 的集成</u>
- 思科身份服务引擎管理员指南,版本3.1
- 思科安全网络设备AsyncOS 14.5用户指南