Integrate Multiple ISE Clusters with Secure Web Appliance for TrustSec Based Policies

Contents

Introduction **Prerequisites** Requirements **Components Used** Limitations **Network Diagram** Configure **ISE Configuration** Enable SXP Configure SXP on the cluster nodes Configure SXP on the aggregation node Enable pxGrid on the aggregation node pxGrid Auto Approval Network devices TrustSec settings **Network Device Authorization** SGT **Authorization Policy** Enabling ERS on ISE Aggregation Node (Optional) Add user to ESR Admin group (Optional) Secure Web Appliance Configuration pxGrid Certificate Enable SXP and ERS on Secure Web Appliance **Identification Profile** SGT Based Decryption Policy Switch Configuration AAA **TrustSec** Verify **Related Information**

Introduction

This document describes the procedure to send Security Group Tag (SGT) information from multiple ISE Deployments to a single Cisco Secure Web Appliance (Formally Web Security Appliance WSA) through pxGrid in order to take advantage of SGT-Based Web Access Policies in a TrustSec deployment.

Prior to version 14.5, Secure Web Appliance can only integrate with a single ISE cluster for identity policies based on SGT. With the introduction of this new version, Secure Web Appliance

can now interoperate with information from multiple ISE clusters with a separate ISE node that aggregates between them. This brings great benefit and enables us to export user data from different ISE clusters and the liberty to control the exit point a user can use without the need for a 1:1 integration.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE)
- Secure Web Appliance
- RADIUS protocol
- TrustSec
- pxGrid

Components Used

The information in this document is based on these software and hardware versions:

- Secure Web Appliance 14.5
- ISE version 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. If your network is live, ensure that you understand the potential impact of any command.

Limitations

- 1. All ISE Cluster need to maintain uniform mappings for SGTs.
- 2. ISE Aggregation Node must have the SGTs name/number of the rest of the ISE clusters.
- 3. Secure Web Appliance can only identify policy (Access/Decryption/Routing) based on SGT Tag and not group nor username.
- 4. Reporting and Tracking is SGT based.
- 5. Existing ISE/Secure Web Appliance sizing parameters continue to apply for this feature.

Network Diagram



Process:

1. When the end user connects to the network, they receive an SGT based on Authorization policies in ISE.

2. The different ISE clusters then send this SGT information in form of SGT-IP mappings to ISE Aggregation Node through SXP.

3. ISE Aggregation Node receive this information and share with the single Secure Web Appliance through pxGrid.

4. Secure Web Appliance uses the SGT information it has learnt to provide access to users based on Web Access Policies.

Configure

ISE Configuration

Enable SXP

Step 1. Select the three lines icon located in the upper left corner and select on Administration > System > Deployment.

Step 2. Select the node you want to configure and click Edit.

E Cisco ISE			Administration • \$	System			Q,	0 53
Deployment Licensing	Certificates	Logging	Maintenance	Upgrade H	ealth Checks Ba	ckup & Restore	Admin Access	Settings
Deployment	• De	eploymer	nt Nodes				Selected 1 Total 1	00
> 뷰 Deployment 과 PAN Failover	0	late 🛞 Registe	D Syncup	Deregister				u× ⊽
	C	Hostname	A Personas		Role(s)	Services	No	ode Status
		ise01-CL1	Administrati	ion, Monitoring, Policy !	Service STANDALON	E SESSION, PROFILE	R 🛛	1

Step 3. To enable SXP, tick the box Enable SXP Service

E Cisco	SE		A	dministration - S	ystem			Q.	0 53 0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
			2 ~	Enable Session	Services G)			
				Include Node in Nod	le Group None		~ 0		
			Enab	ie Profiling Service 🕣					
			Cneb	ie Threat Centric NAC 5	iervice 🕞				
			-	Enable SXP Se	rvice 🕢				
				Use Interface	GigabitEthernet	0	~		

Step 4. Scroll down to the bottom and click Save

Note: Repeat all the steps for the rest of the ISE nodes in each cluster, the aggregation node included.

Configure SXP on the cluster nodes

Step 1. Select the three lines icon located in the upper left corner and select on Work Center > TrustSec > SXP.

Step 2. Click +Add to configure the ISE aggregation node as an SXP peer.

≡ Cisco	ISE	W	ork Centers - T	rustSec					Q	0	53	0
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings				
SXP Devices All SXP Mappings		SXP Devi	ces o			Daves Plane 2	u 16 6		- 00		Scotal D	0.000
		C Refresh + Ad	8 0 Trach 🗸 8	ese A	ssign SXP	Domain				V Filter	~	•

Step 3. Define the Name and IP address of the ISE aggregation node, select peer role as

LISTENER. Select required PSNs under Connected PSNs, required SXP Domains, select Enabled under status, then select Password Type and required Version.

≡ Cisco	ISE		Work Cer	nters • Tru	stSe
Overview	Components	TrustSec Policy	Policy Sets	SXP	AC
SXP Devices		SXP Devices > SXP C	onnection		
All SXP Mappings		 Upload from a CSV 	/ 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 Domaine *			
All SXP Mappings		default ×		12121	
		Status *			
		Enabled		<u> </u>	
		Deseword Tune *			
		CUSTOM		\sim	
		Paceword			
		Passwurd			
		Version *			
		V4		\sim	
		 Advanced Settings 	1		
			Cancel	Save	

Step 4. Click Save

Note: Repeat all the steps for the rest of the ISE nodes in each cluster to build an SXP connection to the aggregation node. **Repeat the same process on the aggregation node and select SPEAKER as peer role.**

Configure SXP on the aggregation node

Step 1. Select the three lines icon located in the upper left corner and select on Work Center > TrustSec > Settings

Step 2. Click the tab SXP Settings

Step 3. To propagate the IP-SGT mappings, tick the **Publish SXP bindings on pxGrid** check box.



Step 4 (Optional). Define a default password for SXP settings under Global Password



Step 5. Scroll down and click Save.

Enable pxGrid on the aggregation node

Step 1. Select the three lines icon located in the upper left corner and select on **Administration > System > Deployment.**

Step 2. Select the node you want to configure and click Edit.

E Cisco ISE	Administr	ation - System		
Deployment Licensing Certificate	s Logging Mainten	ance Upgrade Health Checks	Backup & Restore	Admin Access Settings
Deployment C T O	Deployment M	Dyncup 🔒 Deregister		Selected 1 Total 1 😒 🔮
ap root resource	Hostname	Personas	Role(s) Services	Node Status
	ise-app	Administration, Monitoring, Policy Service	STANDALONE SESSION/PRO	FLER 🖸

Step 3. To enable pxGrid, click the button next to pxGrid.

Cisco ISE	Administration - System	C @ 58 @
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
	Enable Session Services	
	inclute Node in Node Group None 👻 🕐	
	🚺 Enable Probing Sarviya 💮	
	🗌 Enatin Tread Centre NAC Server 💿	
	Enable SXP Service	
	Use monton dispositionement 0 V	
	📄 Enalma (Iwacus Admini Sanacus 💿	
	📄 Enative Paraver constity Service 💿	
	🕢 bribu	

Step 4. Scroll down to the bottom and click Save.

pxGrid Auto Approval

Step 1. Navigate to three lines icon located in the upper left corner and select Administration > pxGrid Services > Settings.

Step 2. By default, ISE does not automatically approve pxGrid the connection requests from new pxGrid clients, therefore you must enable that setting by select the checkbox **Automatically approve new certificate-based accounts.**



Step 3. Click Save

Network devices TrustSec settings

For Cisco ISE to process requests from TrustSec-enabled devices, you must define these TrustSec-enabled devices in Cisco ISE.

Step 1. Navigate to the three lines iconlocated in the upper left corner and select on **Administration > Network Resources > Network Devices.**



Step 3. Enter the required information in the Network Devices section and in RADIUS Authentication Settings.

Step 4. Check the **Advanced TrustSec Settings** check box to configure a TrustSec-enabled device.

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

Step 5. Click the **Use Device ID for TrustSec Identification** check box to automatically populate the Device Name listed in the **Network Devices** section. Enter a password in the **Password** field.

Cisco ISE	Administratio	n · Network Resources
Network Devices	Network Device Groups Network Devic	e Profiles External RADIUS Servers
Network Devices	Advanced TrustSec	c Settings
Default Device Device Security Settings	V Device Authentica Use Device ID for TrustSec Identification	ition Settings
	Device Id	SW1
	* Password	Show

Note: The ID and password must match the "cts credentials id <ID> password <PW>" command that is later configured on the switch.

TrustSec CoA notifications to the device.

Cisco ISE		Administration - Network	Resources		
Network Devices Networ	k Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More ~
Network Devices					
Default Device	V Tru	stSec Notifications and U	pdates		
Device Security Settings			1		
	* pow	itual environment data every	Days V		
			1		
	* Down	rioad peer authorization policy every	Days 🗸		
	* Real	thertication every	Days ¥ ()		
	* Down	Road SSACL lists every	1		
			Days Y		
	Other 1	institute devices to must this device.			
	Send o	onfiguration changes to device	Using O CoA () cu	

Step 7. Check the Include this device when deploying Security Group Tag Mapping Updates check box.

Step 8. In order to let ISE edit the configuration of the network device, enter the user credentials in the **EXEC Mode Username** and **EXEC Mode Password** fields. Optionally, provide enable password in the **Enable Mode Password** field.

Note: Repeat the steps for all other NADs that are intended to be a part of the TrustSec domain.

Network Device Authorization

Step 1. Select the three lines icon located in the upper left corner and select on **Work Centers > TrustSec > TrustSec Policy.**

Step 2. In the left pane, click Network Device Authorization.

E Cisco ISE	Work Centers - Trust/Sec		0 0 ps 0
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports	Settings	
Ryseen Policy	Network Device Authorization Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Define the Network Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag and d Device Authorization Policy by assigning 50% to retwork devices. Drag available to retwork devices.	top rules to change the orde	r. 107 -
Destination Tree			

Step 3. On the right, use the drop-down next to **Edit** and **Insert new row above** to create a new NDA rule.



Step 4. Define a Rule Name, Conditions and select the appropriate SGT from the drop-down list under Security Groups.

Step 5. Click Done to the far right.

E Cisco ISE	Work	Centers - TrustSec		9.0 PI (
Overview Components	TrustSec Policy Policy Sets	SXP ACI Troublesho	ot Reports Settings	
Egress Policy 🗸 🗸	Network Device A	Authorization		
Matrices List Matrix	Define the Network Device Authorizat	ion Policy by assigning SGTs to network	k devices. Drag and drop rules to change the order.	
Matrixes List Matrix Source Tree	Define the Network Device Authorizat Rule Name	ion Policy by assigning SGTs to network Conditions	k devices. Drag and drap rules to change the order. Security Group	
Matrices List Matrix Source Tree Destination Tree	Define the Network Device Authorizat Rule Name	tion Policy by assigning SGTs to network Conditions	t devices. Drag and drop rules to change the order. Security Group	

Step 6. Scroll down and click Save.

SGT

Step 1. Select the three lines icon located in the upper left corner and select on **Work Centers > TrustSec > Components.**

Step 2. In the left pane, expand Security Groups.

Step 3. Click +Add to create a new SGT.

III Cisco ISE	Work Centers - TrustSec	0.0.01.0
Overview Components	TrustSec Policy Policy Sets SVP ACI Trushieshoot Reports Settings	
Security-Drouges	0	
IP 907 Static Mapping	Security Groups	
Security Group AGLs	For Policy Expert prior Advancementation + Section & Realistic + Policy Expert Page	
Nation's Devices		Selected II Test 18 🔅
Instant Servers >	🖉 K.K. 🕂 AAB 💩 Impurt 🛆 Export 🗸 🛔 Trank 🗸 🛞 Park 🛞 Yardy Dapley	м×

Step 4. Enter the name and choose an icon in the appropriate fields.

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

Step 5. Optionally, give it a description and enter a Tag Value.

Note: In order to be able to manually enter a Tag Value, navigate to Work Centers > TrustSec > Settings > General TrustSec Settings and select the option **User Must Enter SGT Number Manually** under **Security Group Tag Numbering**.

Step 6. Scroll down and click Submit

Note: Repeat these steps for all required SGTs.

Authorization Policy

Step 1. Select the three lines icon located in the upper left corner and select on **Policy > Policy** Sets.

Step 2. Select the appropriate policy set.

Step 3. Within the policy set, expand the Authorization Policy.

E Cisco ISE	Policy - P	holicy	Sets		9.05	2 0
Policy Sets-+ Wired Access				Reset	Reset Policyset Hiscourts	
Status Policy Set Name Description	Condition				Allowed Protocols / Server Sequence	1016
Q Seed						
Wind Access	440	9	DEVICE Onview Pyper EQUALS All Device Pyper/ESubstantia		Default Network Access 🛛 😨 🗸 🕸	
			Radius NAS-Part-Type EQUALS Ethernet			
> Authentication Policy (2)						
> Authorization Policy - Local Exceptions						
> Authorization Policy - Global Exceptions						
> Authorization Policy (1)						

Step 4. Click the

and Restauration Restory (11)



button to create an Authorization Policy.

		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

Step 5. Define the required **Rule Name, Condition/s**, and **Profiles** and select the appropriate SGT from the drop-down list under **Security Groups.**

Watched and a short \$ (1)		Results	Results				
Status Rule Name	Conditions	Profiles	Security Groups	Hits Actions			
Q Search							
Contra-Policy	() Winters, 812.1X	PermitAccess ×	v 4 Outert, Endpoints 🛛 👁 v	+ o			

Step 6. Click Save.

Enabling ERS on ISE Aggregation Node (Optional)

The External RESTful API Service (ERS) is an API that can be queried by the WSA for group information. The ERS service is disabled by default on ISE. Once it is enabled, clients can query the API if they authenticate as members of the **ERS Admin** group on the ISE node. To enable the service on ISE and add an account to the correct group, follow these steps:

Step 1. Select the three lines icon located in the upper left corner and select on **Administration > System > Settings.**

Step 2. In the left pane, click ERS Settings.

E Cisco I	SE	Administration - System						Q	0 50 (
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Client Provisioning FIPS Mode Security Settings	ĺ	ERS S	ettings						
Alarm Settings		✓ Genera	1						
Posture		External RE The DRS se An ISE Adm	External RESTML Services (ERS) is a REST API based on HTTPS over port 9000. The ERS service is disabled by default. An ISE Administrator with the "ERS-domin" or "ERS-Operator" group assignment is required to use the API						
Profiling		For more in https://10.5	formation, please 0.50 125 9060/ers	visit the ERS SDK page look	at:				
Protocols									
Endpoint Scripts		✓ ERS Se	tting for Adr	ninistration Node	9				
Proxy		O Enable	Dis forheastWrite						
SMTP Server		O Deable	045						
SMS Gateway									
System Time									
ERS Settings		✓ CSRF C	heck						

Step 3. Select the option Enable ERS for Read/Write.

Step 4. Click Save and confirm with OK.

Add user to ESR Admin group (Optional)

Step 1. Select the three lines icon located in the upper left corner and select Administration > System > Admin Access

Step 2. In the left pane, expand Administrators and click Admin Users.

Step 3. Click +Add and select Admin User from the drop-down.

≡ Cisco IS	SE		Ac	dministration • S	ystem	Q (0) 53				0	
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & F	Restore	Admin Access	Settings	
Authentication		Admi	nistrators	S							
Authorization	>								Selected	0 Total 1 🦪	۲
Administrators	~	Ø Edit	+ Add 🛞 C	hange Status	Delete 0 0	Puplicate				AI V	∇
Admin Users		-									
Admin Groups			Create an Admir	User	Description	First Name	Last Name	Email Addr	ess Admin G	roups	
			Select from Net	work Access Users	> Default Admir	n User			Super Ad	min	
Settings	>										

Step 4. Enter a username and password in the appropriate fields.

😄 Cisco 🗄	SE		A	dministration • S	ystem			Q	0 23 0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Administrations List	> wear						
Authorization)	✓ Admin Usi	er						
Administrators	~	"Name wS	A						
Admin Users									
Admin Groups		Datus 🔤 I	Enabled 🗸			auton sheres is emply			
Settings	>	External III	O I never disable	~	0				
		 Password Password 	5		C				
		* Ro-Enter Par	meord		G				

Step 5. In the Admin Groups field, use the drop-down to select ERS Admin.

≡ Cisco	SE		A	dministration • Sy	ystem			Q,	o ⊊a o
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		First Name							
Authorization	>	Last Name							
Administrators	~								
Admin Users		V Account	Octions						
Admin Groups		Description					*		
Settings	>								
		 Admin ∃ 	Groups ERS Admin		× +				
								Save	Reset

Step 6. Click Save.

Secure Web Appliance Configuration

Root certificate

If the integration design uses an internal certificate authority as the root of trust for the connection between the WSA and ISE, then this root certificate must be installed on both appliances.

Step 1. Navigate to Network > Certificate Management and click on Manage Trusted Root Certificates to add a CA certificate.

Cisco S	Secure Web Applian	ce		Secure Web Appliance is get	ting a new look. Try it
Reporting	Web Security Manager	Security Services	Network	System Administration	
Certificate	Management				
Appliance Certi	ficates				
Add Certificate.					
Certificate	Common Name Iss	sued By Domains	Status Time I	Remaining Expiration	Date Delete
Export Certifica	1e				
Weak Signature	e Usage Settings				
	Restrict Weak Signature Usage	e: Disabled			
					Edit Settings
Certificate FQD	N Validation Settings				
0	ertificate FQDN Validation Usag	e: Disabled			
					Edit Settings
Certificate Lists					
Updates					
File Type		Last Update		Current Version	New Update
Cisco Trusted Rox	ot Certificate Bundle	Success - Thu Jun 30	15:32:47 2022	2.1	Not Available
Cisco Certificate	Blocked List	Success - Wed May 1	1 21:04:06 2022	1.3	Not Available
No updates in pr	ogress.				Update Now
Certificate H	lanagement				
				-	
	Trust Root Certificate	 244 certificates in Cisco 	trusted root certificate i	former form	

Step 2. Click on Import.



Step 3. Click on Choose File to locate the generated Root CA and click Submit.

Step 4. Click Submit again.

Step 5. At the upper right corner, click Commit Changes.

Cisco Secure Web Appliance			Secure Heb Applance is getting a new look. Try 8 1			Bragel to an admin or annumericalitation References - Dates - Support and help -	ľ		
•	Reporting	Web Security Manager	Security Services	Notwork.	System Administration				1
								Canoni Danges n	ſ

Step 6. Click Commit Changes again.

pxGrid Certificate

In the WSA, the creation of the key pair and certificate for use by pxGrid is completed as part of the ISE services configuration.

Step 1. Navigate to Network > Identity Service Engine.

Step 2. Click on Enable and Edit Settings.

Step 3. Click on Choose File to locate the generated Root CA and click Upload File.

Identity Services Engine	
Edit Mentily Dervices Engine Settings	
C Exable 150 Dervice	
Primary 158 petickl Node:	The Web Applance will communicate with the Diff pedial roads to support Web Applance data subscription (impains updates). A primary Diff pediad node (server) must be configured.
	(Sustance or (Pv4 address)
	thit pedate Node Cartificate:
	IF the ISE ps/cvi node certificate is signal by a Certificate Authority, confere that the Certificate Authority is taked in the Trusteel Bost Carification for Jose Network + Carificate Menogenerics and splace the CA-apped not carificate below. If the carificate and speed, exploritive antificate from the SL purcher ded to also below. Two carificate locations in includes any intermediate carificates.
	Cartificate: Onese file Institute chosen

Note: A common misconfiguration is to upload the ISE pxGrid certificate in this section. The root CA certificate must be uploaded to the ISE pxGrid Node Certificate field.

Step 4. In the Web Appliance Client Certificate section, select Use Generated Certificate and Key.

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 to the ISE particle node(s) configured above.	10
	O Use Uploaded Certificate and Key	
	Certificate: Choose File Into the chosen	
	Keyi Choose File Itile chosen	
	Key is Encrypted	
	No certificate has been uploaded.	
	Use Generated Certificate and Key Generate New Certificate and Key	

Step 5. Click the **Generate New Certificate and Key** button and complete the required certificate fields.

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

Step 6. Click on Download Certificate Signing Request.

Note: It is recommend to select the **Submit** button to commit the changes to the ISE configuration. If the session is left to timeout before the changes are submitted, the keys and certificate that were generated can be lost, even if the CSR was downloaded.

Step 7. After you have signed the CSR with your CA, click on **Choose File** to locate the certificate.

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 Upload Files
	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/ab.net
	Organization: Cisco
	Organizational Unit: Security
	Country: SE
	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.

Step 8. Click Upload File.

Step 9. Submit and Commit.

Enable SXP and ERS on Secure Web Appliance

Step 1. Click the Enable buttons for both SXP and ERS.



Step 2. In the **ERS Administrator Credentials** field, enter the user information that was configured on ISE.

Step 3. Check the box for **Server name same as ISE pxGrid Node** to inherit the earlier configured information. Otherwise, enter the required information there.

C 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	umber specified for ERS in ISE)			

Step 4. Submit and Commit.

Identification Profile

In order to use security group tags or ISE group information in the WSA policies, an identification profile must first be created that utilizes ISE as a means to transparently identify users.

Step 1. Navigate to Web Security Manager > Authentication > Identification Profiles.

Step 2. Click on Add Identification Profile.

Step 3. Enter a name and optionally a description.

Step 4. In the Identification and Authentication section, use the drop-down to choose Transparently identify users with ISE.

Identification Profiles: Add Profile

ient / User Identification Profile Settings	
C Enable Edentification Profile	
Name: 🕐	ISE Profile (e.g. my IT Profile)
Description:	Identification profile for ESE Integration. (Hastimum allowed characters 256)
Insert Above:	2 (Slobel Profile) w
ser Identification Hethod	
Identification and Authentication: 🕐	Transparently identify users with ISE
Fallback to Authentication Realm or Guest Privileges: 1	If user information is not available from the Identity Services Engine:
	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).
embership Definition	
embership is defined by any combination of the A	ollowing 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, 2001:420:80:11:5, 2000:458::1-2000:458::10)
Define Members by Protocol:	HTTP/HTTPS
F Advanced	Define additional group membership criteria.

Step 5. Submit and Commit.

SGT Based Decryption Policy

Step 1. Navigate to Web Security Manager > Web Policies > Decryption Policies.

Step 2. Click Add Policy.

Step 3. Enter a name and optionally a description.

Step 4. In the Identification Profiles and Users section, use the drop-down to choose Select One or More Identification Profiles.

Step 5. In the **Identification Profiles** section, use the drop-down to choose the name of the ISE identification profile.

Step 6. In the Authorized Users and Groups section, select Selected Groups and Users.

eranp is denine by the combination of the r	concerning operands. Her choice a must	t de met ne one ponty to take enert.		
Identification Profiles and Users:	Select One or More Identification Profiles 🗸			
	Identification Profile	Authorized Users and Groups	Add Identification Pr	
	ISE Profile	All Authenticated Users Selected Groups and Users ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered Occests fusers falling	9	
	Authentication information may prove traffic, user agent inform	authentication)	ne. For transparent	

Step 7. Click the hyperlink next to ISE Secure Group Tags.

Step 8. In the **Secure Group Tag Search** section, check the box to the right of the desired SGT and click **Add.**

Use the search function below to	add Secure Group Tags. To remove	Secure Group Tags from this policy, use the Delete optio	e.
Secure Group Tag(s) currently in Secure Group Tag Name	suded in this policy.	80T Description	Delete
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 o	lescription. Select one or more Secure Group Tags from th	e list and use the
Search	х		
0 Secure Group Tag(s) select	nd 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	
evop	15	8YOO Security Group	0
PCI_Servers	14	PCI Servers Security Group	0
Guests	6	Guest Security Group	0
wer .	65535	Any Security Group	0
Jnknown	0	Unknown Security Group	0
letwork_Services	3	Network Services Security Group	0
rustSec Devices	2	TrustSec Devices Security Group	0
Cluster1_Endpoints	191	Endpoints residing in ISE Cluster-1	
Employees	4	Employee Security Group	

Step 9. Click Done to return.

Step 10. Submit and Commit.

Switch Configuration

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 Ciscol23 (This is configured in Privileged EXEC Mode) cts role-based enforcement

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

Verify

SGT assignment from ISE to endpoint.

Here you can see an endpoint from ISE Cluster 1 assigned an SGT after successful authentication and authorization:

 v
 Monty
 Degate 0
 Degate 0
 Automatic Nature
 Automatic Natomatic Natur

Here you can see an endpoint from ISE Cluster 2 assigned an SGT after successful authentication and authorization:



SXP Mappings

Since SXP communication is enabled between the cluster ISE nodes and ISE aggregation node, these SGT-IP mappings are learned by ISE aggregation through SXP:

III Cieco ISE		Work Center	+TrustSec			A Deservation	
Overview Components	Trustlec Policy Po	icy Sen . 50P . ACL	houtiestoo	Reports Settings			
DP-Instan Al 107 Magings	All SXP Map	pings o			hardings <u>4</u>	w (<u>1</u>)	1) 💼 the fee
	Ø Ration - And State Do	tan Maraga DP Jonan	there.				Vine - 0
	IP Address	967	ww.	Learned From	Learned By	\$10 ⁹ Domain	PSNs involved
	10.00.00.0.02	Turtles, Jacob (1993)		10/06/08 10121-08/08/08 0	5.07	anut	14 400
		Souther Descent Linearity		100-000 AND 1000 AND AND AND A	147	-	14.400
	10.00000.0000						
	16.06.00.10.00	Durier1_Endpoints (111/2007)		16.04.08.1(C.10.06.04.0	247	defect.	144 400

These SXP mappings, from different ISE clusters, are then sent to WSA over pxGrid through the ISE aggregation node:



SGT based policy enforcment

Here you can see the different endpoints match its respective policies and traffic are blocked based on their SGT:

Endpoint that belongs to ISE Cluster 1



and the second se				
				Items Displayed 50 🛩
Displaying 1 - 50 of 1	37 items.			< Previous 1 2 3 Next
Time (GHT +02:00) *	 Website (sourd) Display All De 	tals Disposition	Bandwidth	User / Client IP
54 34 2022 54 28 37	https://bbc.asexu45/Taviper.ice Contrast 1995 - Use: Control of Block URLs CL1 Control. Control (II) - Octavity. Control (II) - Octavity. Control Failory 1958_Cluster11, WBRS: No 5 Malware Analytics File Verdict: -	Bleck - URS Cat	¢6	isemp_10.50.50.121_sgR11_10.50.50.1 (Identified by 155 10.50.50.1

Endpoint that belongs to ISE Cluster 2



Related Information

- Web Security Appliance and Identity Service Engine Integration Guide
- Configure WSA Integration with ISE for TrustSec Aware Services
- <u>Cisco Identity Services Engine Administrator Guide, Release 3.1</u>
- User Guide for AsyncOS 14.5 for Cisco Secure Web Appliance