Intégrer plusieurs clusters ISE avec une appliance Web sécurisée pour les stratégies basées sur TrustSec

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Limites Diagramme du réseau Configuration **Configuration ISE** Activer SXP Configurer SXP sur les noeuds de cluster Configurer SXP sur le noeud d'agrégation Activer pxGrid sur le noeud d'agrégation Approbation automatique pxGrid Paramètres TrustSec des périphériques réseau Autorisation des périphériques réseau SGT Stratégie d'autorisation Activation de l'ERS sur le noeud d'agrégation ISE (facultatif) Ajouter un utilisateur au groupe d'administration ESR (facultatif) Configuration sécurisée des appareils Web certificat pxGrid Activer SXP et ERS sur l'appliance Web sécurisée **Profil d'identification** Stratégie de déchiffrement basée sur SGT Configuration du commutateur AAA **TrustSec** Vérification Informations connexes

Introduction

Ce document décrit la procédure à suivre pour envoyer des informations SGT (Security Group Tag) de plusieurs déploiements ISE à un seul appareil Web sécurisé Cisco (officiellement Web Security Appliance WSA) via pxGrid afin de tirer parti des stratégies d'accès Web basées sur SGT dans un déploiement TrustSec.

Avant la version 14.5, Secure Web Appliance ne peut s'intégrer qu'à un seul cluster ISE pour les stratégies d'identité basées sur SGT. Avec l'introduction de cette nouvelle version, Secure Web Appliance peut désormais interagir avec des informations provenant de plusieurs clusters ISE avec un noeud ISE distinct qui s'agrège entre eux. Cela apporte un grand avantage et nous permet d'exporter des données utilisateur de différents clusters ISE et de contrôler le point de sortie qu'un utilisateur peut utiliser sans avoir besoin d'une intégration 1:1.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Identity Services Engine (ISE)
- Appareil Web sécurisé
- protocole RADIUS
- TrustSec
- pxGrid

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil Web sécurisé 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Limites

- 1. Tous les clusters ISE doivent maintenir des mappages uniformes pour les balises de groupe de sécurité.
- 2. Le noeud d'agrégation ISE doit avoir le nom/numéro des SGT des autres clusters ISE.
- L'appliance Web sécurisée peut uniquement identifier la stratégie (accès/déchiffrement/routage) en fonction de la balise SGT et non de de groupe ou de nom d'utilisateur.
- 4. Le reporting et le suivi sont des basées sur SGT.
- 5. Les paramètres de dimensionnement ISE/Secure Web Appliance existants continuent de s'appliquer à cette fonctionnalité.

Diagramme du réseau



Process:

1. Lorsque l'utilisateur final se connecte au réseau, il reçoit une SGT basée sur les stratégies d'autorisation dans ISE.

2. Les différents clusters ISE envoient ensuite ces informations SGT sous forme de mappages SGT-IP au noeud d'agrégation ISE via SXP.

3. Le noeud d'agrégation ISE reçoit ces informations et les partage avec l'appliance Web sécurisée unique via pxGrid.

4. Secure Web Appliance utilise les informations SGT qu'il a apprises pour fournir un accès aux utilisateurs en fonction des stratégies d'accès Web.

Configuration

Configuration ISE

Activer SXP

Étape 1. Sélectionner l'icône des trois lignes situé dans le coin supérieur gauche et sélectionnez Administration > System > Deployment.

Étape 2. Sélectionnez le noeud à configurer et cliquez sur Modifier.

		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 Support Support	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

Étape 3. Pour activer SXP, cochez la case Activer le service SXP

E Cisco S	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	ia Profiling Service 🕣					
			C Enel	le Threat Centric NAC 5	iervice 🕞				
			-	Enable SXP Se	rvice 🧿				
				Use interface	GigabitEthernet	0	~		

Étape 4. Faites défiler la page vers le bas et cliquez sur Enregistrer

Note: Répétez toutes les étapes pour les autres noeuds ISE de chaque cluster, le noeud d'agrégation inclus.

Configurer SXP sur les noeuds de cluster

Étape 1. Sélectionner l'icône des trois lignes situé dans le coin supérieur gauche et sélectionnez **Centre de travail > TrustSec > SXP.**

Étape 2. Cliquez sur **+Ajouter** pour configurer le noeud d'agrégation ISE en tant qu'homologue SXP.

■ Cisco ISE	W	fork Centers • Tru	stSec					Q	0	78	0
Overview Comp	onents TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings				
SXP Devices All SXP Mappings	SXP Devi	ces o									
					Rows/Page 2	✓ IC < _1		Go	2 %	stal Rov	N'S
	Ø Refresh + Ad	ld 🔋 Trash 🗸 🖉 (Edit Ass	lign SXP D	omain				V Filter	~ (Þ

Étape 3. Définissez le nom et l'adresse IP du noeud d'agrégation ISE, sélectionnez le rôle homologue en tant que LISTENER. Sélectionnez les PSN requis sous PSN connectés, les domaines SXP requis, sélectionnez Activé sous l'état, puis Type de mot de passe et Version requise.

Overview Compon	ents TrustSec Policy	Policy Sets	SXP	AC
SXP Devices	SXP Devices > SXP (Connection		
All SXP Mappings	 Upload from a CS 	SV file		
	- Add Single Device	0		
	Input fields marked	with an asterisk (*)	are required	i.
	Name ISE Aggregation i	node		
	IP Address * 10.50.50.125			
	Peer Role * LISTENER		~	
	Connected DSNs +			
	ise01-CL1 ×			



Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI
SXP Devices		SXP Domains *			
All SXP Mappings		default ×		~	
		Status • Enabled		~	
		Password Type * CUSTOM		~	
		Password			
		Version * V4		~	
		 Advanced Settings 	1		
			Cancel	Save	

Étape 4. Cliquez sur Save (enregistrer)

Note: Répétez toutes les étapes pour les autres noeuds ISE de chaque cluster pour créer une connexion SXP au noeud d'agrégation. **Répétez le même processus sur le noeud d'agrégation et sélectionnez SPEAKER comme rôle homologue.**

Configurer SXP sur le noeud d'agrégation

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez dans **Centre de travail > TrustSec > Paramètres.**

Étape 2. Cliquez sur l'onglet Paramètres SXP

Étape 3. Pour propager les mappages IP-SGT, cochez la case Publier les liaisons SXP sur pxGrid.



Étape 4 (facultatif). Définir un mot de passe par défaut pour les paramètres SXP sous Mot de passe global

≡ Cisco	ISE	W	/ork Centers • T	rustSec				
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings
General TrustSec S TrustSec Matrix Se	Settings	SXP Settings						
Work Process Sett	ings	Publish SXP bindir	ngs on PxGrid 🛃 Ad	d radius map	pings into S	XP IP SGT mapping table	0	
SXP Settings		Global Passwor	a					
ACI Settings		Global Password						
		This global passwor the device specific	rd will be overriden password	by				

Étape 5. Faites défiler la liste vers le bas et cliquez sur Enregistrer.

Activer pxGrid sur le noeud d'agrégation

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez Administration > System > Deployment.

Étape 2. Sélectionnez le noeud à configurer et cliquez sur Modifier.

Cisco ISE		Administration • S	lystem			• 12 0 0
Deployment Licensing Certifica	tes Logging	Maintenance	Upgrade Health	Checks Backup &	Restore Ad	min Access Settings
Deployment	Deployr	nent Node	S			Selected 1 Total 1 👩 🔕
> 3% Deployment	1 60 8	legister 🖒 Syncup	S Deregister			${\bf A} {\bf e} \sim - \nabla$
Ab have herebeet	Host	name 🗠 Perso	onas	Role(s)	Services	Node Status
	- 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10	N Admir	istration, Monitoring, Policy	Service STANDALONE	SESSION, PROFILE	•

Étape 3. Pour activer pxGrid, cliquez sur le bouton en regard de pxGrid.

Cisco ISE	Administration - System	୍ ୦୦ ହୋବ
Deployment Uconsing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
	Enable Session Services ()	
	Include Hande or None diricup	
	🚺 Enalite Profiling Sarvice 💿	
	🗌 Emaile Thread Canter, NHC Service 💿	
	Enable SXP Service ()	
	Une insertion dispatificmented 0 V	
	📄 Enaine Device Admit Service 💿	
	📄 Enable Passes controls Service 💿	
	() brites	

Étape 4. Faites défiler la page vers le bas et cliquez sur Enregistrer.

Approbation automatique pxGrid

Étape 1. Accédez à l'icône de trois lignes située dans le coin supérieur gauche et sélectionnez Administration > pxGrid Services > Settings.

Étape 2. Par défaut, ISE n'approuve pas automatiquement pxGrid les demandes de connexion des nouveaux clients pxGrid. Par conséquent, vous devez activer ce paramètre en cochant la case **Approuver automatiquement les nouveaux comptes basés sur des certificats**.



Étape 3. Cliquez sur Save (enregistrer)

Paramètres TrustSec des périphériques réseau

Pour que Cisco ISE traite les demandes des périphériques compatibles TrustSec, vous devez définir ces périphériques compatibles TrustSec dans Cisco ISE.

Étape 1. Accédez à l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez Administration > Network Resources > Network Devices.

Étape 2. Cliquez sur +Ajouter.

Cisco ISE		Administration	Network Resources	5		9.0	53 Ø
Network Devices	Network Device Groups	Network Device	Profiles External P	ADIUS Servers	RADIUS Server Sequences	More \sim	
Network Devices Default Device	Network	Devices					
Device Security Settings	0 ta + 40	d Duplicate	🕁 Import 🖞 Export	- A Generate PM	C Delete ~	Selected 0 Total 2 🖉	3 0 7
	Name	 IP/Mask 	Profile Name	Location	Type	Description	

Étape 3. Entrez les informations requises dans la section Périphériques réseau et dans Paramètres d'authentification RADIUS.

Étape 4. Cochez la case Advanced TrustSec Settings pour configurer un périphérique compatible 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

Étape 5. Cochez la case Utiliser l'ID de périphérique pour l'identification TrustSec pour renseigner automatiquement le nom de périphérique répertorié dans la section Périphériques réseau. Entrez un mot de passe dans le champ Mot de passe.



Note: L'ID et le mot de passe doivent correspondre à la commande " cts identifiants id <ID> password <PW> " qui est configurée ultérieurement sur le commutateur.

Étape 6. Cochez la case Envoyer les modifications de configuration au périphérique afin que ISE puisse envoyer des notifications TrustSec CoA au périphérique.

Cisco ISE		Administration - Network	Resources		
Network Devices	Network 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		
	* Dow	ricad environment data every	Days 👻		
	* Dow	rioad peer authorization policy every	Days V		
			,		
	* Real	thertication every	Days Y ()		
	* Dow	rioad SGACL lists every	Days ¥		
	Other 1	fruitfiec devices to trust this device			
	Send o	orfiguration changes to device	Using O CoA (O cu	

Étape 7. Cochez la case Inclure ce périphérique lors du déploiement des mises à jour de mappage de balises de groupe de sécurité.

Étape 8. Afin de permettre à ISE de modifier la configuration du périphérique réseau, entrez les informations d'identification de l'utilisateur dans les champs **Nom d'utilisateur du mode EXEC** et **Mot de passe du mode EXEC**. Le cas échéant, indiquez le mot de passe enable dans le champ **Mot de passe du mode enable**.

Note: Répétez les étapes pour tous les autres NAD qui sont destinés à faire partie du domaine TrustSec.

Autorisation des périphériques réseau

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez dans **Centres de travail > TrustSec > Stratégie TrustSec.**

Étape 2. Dans le volet gauche, cliquez sur Network Device Authorization.

E Cisco ISE	Work Centers + TrustSea		0 © 50	0
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports	Settings		
Egreen Policy ~	Network Device Authorization			
Matrix	Define the Network Device Authorization Policy by assigning 507s to network devices. Drag and	drop rules to change the orde	er.	

Étape 3. À droite, utilisez la liste déroulante en regard de **Modifier** et **Insérer une nouvelle ligne ci**dessus pour créer une nouvelle règle NDA.



Étape 4. Définissez un nom de règle, des conditions et sélectionnez la SGT appropriée dans la liste déroulante sous Groupes de sécurité.

Étape 5. Cliquez sur Terminé à l'extrême droite.

E Cisco	SE	Work Centers - TrustSec							-	10	98	0
Overview	Components	TrustSec Policy	Policy Sets	SIP	ACI Tro	ubleshoot	Reports	Settings				
Egress Policy Matrices List	Ÿ	Network (Device Al	uthori:	zation	ó network devi	ces. Drag and	drop rules to cha	inge the order.			
Source Tree		Rule	Name		Conditions			Security Group				
Destination Tree		🗄 🖬 🗠 NDA	0	# DEV	ACE Device Type eq	an 1. 🗸	then Trail	Sec.Devices	V Done			
Network Device Aut	horization	Deh	nuit Rule	1.10	rules defined or n	e-match	then True	Sec_Devices	fat v			

Étape 6. Faites défiler la liste vers le bas et cliquez sur Enregistrer.

SGT

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez dans **Centres de travail > TrustSec > Composants.**

Étape 2. Dans le volet gauche, développez Groupes de sécurité.

Étape 3. Cliquez sur +Ajouter pour créer une nouvelle SGT.

III Cisco ISE	Work Centers - TrustSec	0.0 00 0
Overview Components	TrustSec Policy Policy Sets SVP ACI Trusheshoot Reports Settings	
Security-Droops	0	
IP SGT State Mapping	Security Groups	
Security Group ACLs	For Policy Expert prior Administration + Society & Restors + Policy Expert Prope	
Nataork Devices		Selected II Total 18
Instant Servers	🖉 Elle 🕂 Add 💩 Ingant 🛆 Engant 🗸 🏦 Trank 🗸 🛞 Pault 🛞 Yanda Dagday	м×

Étape 4. Entrez le nom et choisissez une icône dans les champs appropriés.

Cisco ISE	Work Centers · TrustSec						
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoo						
Security Groups	Security Groups List > New Security Group						
IP SGT Static Mapping	Security Groups						
Security Group ACLs							
Network Devices	* Name						
Trustsec Servers >	Cluster1_Endpoints						
	* Icon						

Étape 5. Vous pouvez éventuellement lui donner une description et saisir une valeur de balise.

Note: Afin de pouvoir saisir manuellement une valeur de balise, accédez à Centres de travail > TrustSec > Paramètres > Paramètres généraux TrustSec et sélectionnez l'option L'utilisateur doit saisir manuellement le numéro de balise de groupe de sécurité sous Numérotation de balise de groupe de sécurité.

Étape 6. Faites défiler la liste vers le bas et cliquez sur Soumettre.

Note: Répétez ces étapes pour toutes les balises de groupe de sécurité requises.

Stratégie d'autorisation

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez **Stratégie > Jeux de stratégies.**

Étape 2. Sélectionnez le jeu de stratégies approprié.

Étape 3. Dans le jeu de stratégies, développez la stratégie d'autorisation.

E Cisco ISE	Policy -	Policy	Sets	9.05	2 0
Policy Sets-+ Wired Access			Res	 Reset Policyset Hitcourts	
Status Policy Set Name Description	Conditi	iuna i		Allowed Protocols / Server Sequence	Hits
Q Seat					
Wind Access	440		DEVICE Onvice Type EQUILS AT Device Types/Elasticities	Default Network Access - 68 🗸 🕂	
			Radius NAS-Part-Type EQUALS Ethernet		
) Authentication Policy (2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
> Authorization Policy (1)					

Étape 4. Cliquez sur le bouton pour créer une stratégie d'autorisation.

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

Étape 5. Définissez le nom de la règle requise, les conditions et les profils et sélectionnez la SGT appropriée dans la liste déroulante sous Groupes de sécurité.

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

Étape 6. Click Save.

Activation de l'ERS sur le noeud d'agrégation ISE (facultatif)

Le service ERS (External RESTful API Service) est une API qui peut être interrogée par le WSA pour obtenir des informations sur le groupe. Le service ERS est désactivé par défaut sur ISE. Une fois qu'il est activé, les clients peuvent interroger l'API s'ils s'authentifient en tant que membres du groupe **ERS Admin** sur le noeud ISE. Pour activer le service sur ISE et ajouter un compte au groupe approprié, procédez comme suit :

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez Administration > System > Settings.

Étape 2. Dans le volet gauche, cliquez sur Paramètres ERS.

E Cisco ISE	E		A	dministration • S	ystem			C © 21			
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	- 1	External PE	e STM Services (D	(5) is a REST API based	on HTTPS over pr	rt 9060.					
Posture		An 15E Adre For more in	The DVS service is desided by density. An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API. For more information, please visit the ERS SDK page at:								
Profiling		https://10.5	0 50 125 9060/ers	5dk							
Protocols											
Endpoint Scripts	,	✓ ERS Se	tting for Adr	ninistration Node	,						
Proxy		O Enable	DIS forhead/Write								
SMTP Server SMS Gateway		0.000									
System Time											
ERS Settings		CSRF (CSR	Check								

Étape 3. Sélectionnez l'option Activer ERS pour lecture/écriture.

Étape 4. Cliquez sur Enregistrer et confirmer avec OK.

Ajouter un utilisateur au groupe d'administration ESR (facultatif)

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez Administration > System > Admin Access.

Étape 2. Dans le volet gauche, développez Administrateurs et cliquez sur Utilisateurs Admin.

Étape 3. Cliquez sur +Ajouter et sélectionnez Utilisateur Admin dans la liste déroulante.

≡ Cisco IS	SE		Ad	dministration - S	ystem	Q Q 20 0					
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & F	Restore	Admin Access	Settings	4
Authentication		Admir	nistrators	s							
Authorization	>								Selected	0 Total 1 🦪	0
Administrators	~	0 Edit -	- Add 🛞 C	hange Status	Delete D C	uplicate				AL V	V
Admin Users											
Admin Groups			Create an Admir	n User	Description	First Name	Last Name	Email Addre	ss Admin G	roups	
			Select from Net	work Access Users	> Default Admi	n User			Super Adr	min	
Settings	>										

Étape 4. Entrez un nom d'utilisateur et un mot de passe dans les champs appropriés.

≡ Cisco	SE		Ad	dministration • S	ystem			Q.	0 28 0
Deployment	Licensing	Certificates Lo	ogging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Administrators List 3	1150						
Authorization	>	✓ Admin User	r						
Administrators	~	"Name with							
Admin Users									
Admin Groups		Status 🔤 En	ubied 🛩						
Settings		Ernall			D Inclusion	system alarms in emails			
	· · · ·	External 🛄 🧕							
		Read Only							
		inactive account n	vever disable	•					
		✓ Password							
		* Password			Q				
		* Re-Enter Passe	eord		G				

Étape 5. Dans le champ Groupes d'administrateurs, utilisez la liste déroulante pour sélectionner Administrateur ERS.

≡ Cisco	SE		A	dministration • Sy	ystem			Q,	o ⊊a e
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

Étape 6. Click Save.

Configuration sécurisée des appareils Web

Certificat racine

Si la conception d'intégration utilise une autorité de certification interne comme racine de confiance pour la connexion entre le WSA et ISE, ce certificat racine doit être installé sur les deux appliances.

Étape 1. Accédez à Network > Certificate Management et cliquez sur Manage Trusted Root Certificates pour ajouter un certificat CA.

Cisco Se	cure Web Appliance		Secure Web Appliance is getting a new look. Try it			
Reporting	Web Security Manager	Security Services	Network	System Adm	inistration	
Certificate M	Management					
Appliance Certific	ates					
Add Certificate						
Certificate (Common Name Issued	Dy Domains	Status Tir	me Remaining	Expiration Date	Delete
Export Certificate.						
Weak Signature U	Isage Settings					
P	Restrict Weak Signature Usage:	Disabled				
						Edit Settings
Certificate FQDN	Validation Settings					
Cert	tificate FQON Validation Usage:	Disabled				
						Edit Settings
Certificate Lists						
Updates						
File Type		Last Update		Curren	t Version	New Update
Cisco Trusted Root	Certificate Bundle	Success - Thu Jun 30 1	5:32:47 2022	2.1		Not Available
Cisco Certificate Blo	icked List	Success - Wed May 11	21:04:06 2022	1.3		Not Available
No updates in progr	ress.					Update Now
Certificate Har	sagement					
Certificate Har	Trust Root Certificates:	244 certificates in Cisco tr	usted rook certifica	te lut		

Étape 2. Cliquez sur Importer.

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.

Étape 3. Cliquez sur Choose File pour localiser l'autorité de certification racine générée et cliquez sur Submit.

Étape 4. Cliquez de nouveau sur Soumettre.

Étape 5. Dans le coin supérieur droit, cliquez sur Valider les modifications.



Étape 6. Cliquez à nouveau sur Valider les modifications.

certificat pxGrid

Dans le WSA, la création de la paire de clés et du certificat à utiliser par pxGrid est terminée dans le cadre de la configuration des services ISE.

Étape 1. Accédez à Network > Identity Service Engine.

Étape 2. Cliquez sur Activer et modifier les paramètres.

Étape 3. Cliquez sur Choose File pour localiser l'autorité de certification racine générée et cliquez sur Upload File.

Identity Services Engine		
Edit Identity Services Engine Bellings		
C Exable 150 Service		
Prim	ny 158 petinti Node:	The Blob Appliance will communicate with the 202 partial node to support Blob Appliance data subscription (separing updates). A primary 202 profession node (server) must be configured. (Institution or IPv4 address)
		INF pedint Node Contribute: IF the INF pedint Node Contribute is signed by a Certificate Authority, southern that the Certificate Authority is faited in the Trastell Root Certificates list (see Network in Certificate Messagement) and cables (the CA-aqued not certificate below. If the certificate is self-aqued, seport the certificate from the Landow Authority, the certificate of the CA-aqued not certificate and rescale and rescale Certification. The Certificate and the certificate is a certificate of the CA-aqued not certificate is a certificate. Certificate (Certificate Term Text) and below. The certificate of the CA-aqued not certificate is a certificate. Certificate (Certificate Term Text) for the chosen

Note: Une erreur de configuration courante consiste à télécharger le certificat ISE pxGrid dans cette section. Le certificat d'autorité de certification racine doit être téléchargé dans le champ ISE pxGrid Node Certificate.

Étape 4. Dans la section Certificat client de l'appliance Web, sélectionnez Utiliser le certificat et la clé générés.

For secure communications to the ISE peGrid node(s)	on between the Web Appliance and the ISE particle servers, provide a client certificate. This may need to be uploade 10 configured above.
O Use Uploaded Cert	Those and Key
Certificate:	Choose Fite Nas file chosen. Upload Files
Key:	Choose File May file choosen
	Rey is Encrypted
	No certificate has been uploaded.
	For secure communication to the SE performance of the SE performan

Étape 5. Cliquez sur le bouton Générer un nouveau certificat et une nouvelle clé et renseignez les champs de certificat requis.

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

Étape 6. Cliquez sur Télécharger la demande de signature de certificat.

Note: Il est recommandé de sélectionner le bouton **Soumettre** pour valider les modifications apportées à la configuration ISE. Si le délai d'attente de la session est dépassé avant l'envoi des modifications, les clés et le certificat générés peuvent être perdus, même si le CSR a

été téléchargé.

Étape 7. Après avoir signé le CSR avec votre CA, cliquez sur Choose File pour localiser le certificat.

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.securitylab.net						
	Organization: Circo						
	Organizational Unit: Security						
	Controls: No. 15 10:15:16 10:16 00:17						
	Basic Constraints: Not Oritical						
	Download Certificate Download Certificate Signing Request						
	Signed Certificate:						
	To use a signed certificate, first download a certificate signing request using the linit 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						

Étape 8. Cliquez sur Télécharger le fichier.

Étape 9. Envoyer et valider.

Activer SXP et ERS sur l'appliance Web sécurisée

Étape 1. Cliquez sur les boutons Activer pour SXP et ERS.



Étape 2. Dans le champ Informations d'identification de l'administrateur ERS, saisissez les informations utilisateur configurées sur ISE.

Étape 3. Cochez la case Nom de serveur identique au noeud ISE pxGrid pour hériter des informations configurées précédemment. Sinon, saisissez les informations requises.

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 1SE)

Étape 4. Envoyer et valider.

Identification Profiles: Add Profile

Profil d'identification

Afin d'utiliser des balises de groupe de sécurité ou des informations de groupe ISE dans les stratégies WSA, il faut d'abord créer un profil d'identification qui utilise ISE comme moyen d'identifier les utilisateurs de manière transparente.

Étape 1. Accédez à Web Security Manager > Authentication > Identification Profiles.

Étape 2. Cliquez sur Ajouter un profil d'identification.

Étape 3. Saisissez un nom et éventuellement une description.

Étape 4. Dans la section Identification et authentification, utilisez la liste déroulante pour sélectionner Identifier de manière transparente les utilisateurs avec ISE.

Enable Identification Profile	
Name: 🕐	ISE Profile (e.g. my IT Profile)
Description:	Identification profile for ISE Integration.
Insert Above:	2 (Global Profile) 🛩
dentification 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 V
	Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).
ership Definition	
ership 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, 2000:408:11-2000:408:110
Define Members by Protocol:	HTTP/HTTPS

Étape 5. Envoyer et valider.

Stratégie de déchiffrement basée sur SGT

Étape 1. Accédez à Gestionnaire de sécurité Web > Stratégies Web > Stratégies de

déchiffrement.

Étape 2. Cliquez sur Ajouter une stratégie.

Étape 3. Saisissez un nom et éventuellement une description.

Étape 4. Dans la section **Profils et utilisateurs d'identification**, utilisez la liste déroulante pour sélectionner **Sélectionner un ou plusieurs profils d'identification**.

Étape 5. Dans la section **Profils d'identification**, utilisez la liste déroulante pour choisir le nom du profil d'identification ISE.

Étape 6. Dans la section Utilisateurs et groupes autorisés, sélectionnez Groupes et utilisateurs sélectionnés.



Étape 7. Cliquez sur le lien hypertexte en regard de Balises de groupe sécurisé ISE.

Étape 8. Dans la section Recherche de balises de groupe sécurisé, cochez la case à droite de la SGT souhaitée et cliquez sur Ajouter.

Authorized 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	Π
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	0	-
()			•	11
			Delete	

Secure Group Tag Search			
Enter any text to search for a Se Add button to add to this policy. Search	cure Group Tag name, number, or o	lescription. Belect one or more Secure Group Tags from th	e list and use the
0 Secure Group Tag(s) select			A66
Secure Group Tag Name	SGT Number	SGT Description	Select Aa
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
BYOD	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	191	Endpoints residing in ISE Cluster-1	
Employees	4	Employee Security Group	
4	1.	1	•

Étape 9. Cliquez sur Terminé pour revenir.

Étape 10. Envoyer et valider.

Configuration du commutateur

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 Ciscol23
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 Cisco123
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 $\tt Ciscol23$ (This is configured in Privileged EXEC Mode) cts role-based enforcement

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

Vérification

Affectation de balises de groupe de sécurité entre ISE et terminal.

Vous pouvez voir ici un point de terminaison du cluster ISE 1 affecté à une SGT après une authentification et une autorisation réussies :



Vous pouvez voir ici un point de terminaison du cluster ISE 2 affecté à une SGT après une authentification et une autorisation réussies :

	v	identify.	Ordpatric D	Delpare Polite	Automation Party	Autorization Pulloy	Autorization Profiles	P Address v	Becarity Group	berner .
ALC: DOD DOD AT \$1		lose the second	141010-	Monath Bark	West Access to D	Writed Succession in the	Participation	10.06.00.12	Dunct, Dances	1011-013

Mappages SXP

Puisque la communication SXP est activée entre les noeuds ISE du cluster et le noeud d'agrégation ISE, ces mappages SGT-IP sont appris par l'agrégation ISE via SXP :

III Cieco 156		Work Centers	+ TrustSec			A Transition	
Overview Components	Trustlec Policy P	No 50 AC	Troubleshoot	Reports Settings			
SIP Inviore	All SVD Mar	onings o					
All DAP Maggings	All GAP may	bhuilte o					
					Providence &	¥ < 1 - 1	1) In Plant Root
	C Reference Autor (1997)	Donas that Maraga SIP Donas 1	ne s				View V 0
	IP Address	907	WN	Learned From	Learned By	SNP Domain	PSNs involved
	10.00.00.0/02	Tratfore, Joseph (2000)		10.06.001.121.70.06.06.0	547	annut	144-1020
	10.00.00.1102	Testino, January (2001)		10.00.00.102.00.00.00.0	547	annet	144-400
	10.00.00.10.02	Deniert, Johnson (111,0007)		10.00.001121.10.00.00.0	547	defect.	104-000
	10,00,00,10,00	Council Engineering (Conceptual)		10.00.001101.00.00.00.0	147	4444	10.000

Ces mappages SXP, provenant de différents clusters ISE, sont ensuite envoyés à WSA via pxGrid via le noeud d'agrégation ISE :



Application des politiques basée sur SGT

Vous pouvez voir ici que les différents points d'extrémité correspondent à ses stratégies respectives et que le trafic est bloqué en fonction de leur SGT :

Point de terminaison appartenant au cluster ISE 1



This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site (https://bbc.com/) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Thu, 14 Jul 2022 14:28:16 CEST Usemame: isesxp_10.50.50.121_sgt111_10.50.50.12 Source IP: 10.50.50.12 URL: GET https://bbc.com/ Category: Block URLs CL1 Reason: UNKNOWN Notification: BLOCK_DEST

Results					
					Items Displayed 50 👻
Displaying 1 - 50 of 13	7 items.				< Previous 1 2 3 Next -
Time (GNT +02:00) +	Website (munt)	Display All Details	Disposition	Bandwidth	User / Client IP
54 Jul 2022 54:28:57	Masu/Net.com/42/Texicon.ice content mitty - de. Ortfolder Block URLs CL1 content-form III - content-former Paicer "158_Coat Malware Analytics File Verdict: -	er1", WBRS: No Score,	Block - URL CH	ce	isesup_10.50.50.121_sg7111_10.50.50.12 (2dentified by 158) 10.50.50.12

Point de terminaison appartenant au cluster ISE 2

		rage sumeras a	is prayed			
	Based (https://	d on your organization's ac s://www.facebook.com/) h	cess policies, a as been blocked	ccess to this I.	s web site	
	If you have questions, please contact your organization's network administrator and provide the codes shown below.					
	Date: Usem Souro URL: Categ Reaso Notific	Thu, 14 Jul 2022 14:23:58 ame: isesxp_10.50.50.122 e IP: 10.50.50.13 GET https://www.facebook ory: Block URLs CL2 m: UNKNOWN ation: BLOCK_DEST	CEST _sgt222_10.50: .com/	50.13		
Results						
Displaying	1 - 2 of 2 its	ma.				
Time (GHT	+02:00) =	Website (count)	Display All Details	Disposition	Bandwidth	User / Clant IP
14 34 2023	14:22:58	Migas //www.facebook.com/s42/favioo concentration unit. Critecom Block URLs CL2 DESTINATION IP CONST. Decoyption Pulicy: "158_Clue Malware Analytics File Verdict: .	nice ter2", w845: No Score,	Block - URL Cat	08	isesus_10.50.50.122_s9(222_10.50.50.13 (25est)fed by 158 30.50.50.13

Informations connexes

• Guide d'intégration de l'appliance de sécurité Web et de Identity Service Engine

- Configurez l'intégration du WSA au moyen des services ISE TrustSec
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1
- Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance