# Configuration de la position VPN Linux avec ISE 3.3

# Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Diagramme du réseau
Configurations sur FMC/FTD
Configurations sur ISE
Configurations sur Ubuntu
Vérifier
<u>Dépannage</u>
Informations connexes

# Introduction

Ce document décrit comment configurer la position VPN Linux avec Identity Services Engine (ISE) et Firepower Threat Defense (FTD).

# Conditions préalables

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Client sécurisé Cisco
- VPN d'accès à distance sur Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

## Composants utilisés

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

- Ubuntu 22.04
- Cisco Secure Client 5.1.3.62
- Cisco Firepower Threat Defense (FTD) 7.4.1
- Cisco Firepower Management Center (FMC) 7.4.1
- Cisco Identity Services Engine (ISE) 3.3

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.

# Configurer

## Diagramme du réseau



Topologie

## Configurations sur FMC/FTD

Étape 1. La connectivité entre le client, FTD, FMC et ISE a été correctement configurée. Comme enroll.cisco.com est utilisé pour les terminaux qui effectuent des tests de redirection (référez-vous aux <u>documents</u> CCO de flux de posture<u>Comparaison de style de posture ISE pour Pre et Post 2.2</u> pour plus de détails). Assurez-vous que la route du trafic vers enroll.cisco.com sur FTD est correctement configurée.

Étape 2. Téléchargez le nom cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg du package à partir de <u>Cisco Software</u> <u>Download</u> et assurez-vous que le fichier est correct après le téléchargement en confirmant que la somme de contrôle md5 du fichier téléchargé est identique à celle de la page Cisco Software Download.

Étape 3. Accédez à Objects > Object Management > VPN > Secure Client File. Cliquez sur Add Secure Client File, indiquez le nom, recherchez File Name pour sélectionner cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, sélectionnez Secure Client Image dans la liste déroulanteFile Type. Cliquez ensuite sur Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policie	s Devices Objects Integration		Deploy	Q 💕 🔅 🔕 admin 🗸 '	dide SECURE
> Distinguished Name DNS Server Group	Secure Client File			Add Secure	Client File Q, Filter	
> External Attributes	File objects represent files used for remote access V	PN policy configurations. They can contain Secure Client profile and image files.				
File List > FlexConfig Geolocation		Add Secure Client File	0			
Interface Key Chain Network	Name client_image	Name:*		n-5.1.3.62-webdeploy-k9.pkg	Type Secure Client Image	1/1
> PKI Policy List	Default-External-Browser-package hostscan5_1_3_62	linux_5_1_3_62		36-webdeploy-k9.zip +-5.1.3.62-k9.pkg	Secure Client External Browser Pa HostScan Package	± 4 ii ± 1 ii
Port Prefix List Route Map	linux_image	File Name:*	Browse	ux64-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	±/¥
> Security Intelligence Sinkhole		File Type:*				
SLA Monitor Time Range		Secure Client Image				
Time Zone Tunnel Zone URL		Description:				
Variable Set VLAN Tag						
V VPN						
Certificate Map Custorn Attribute Group Policy IKEV1 IPsec Proposal IKEV1 Policy IKEV2 IPsec Proposal		С	ancel			
IKEv2 Policy Secure Client Customizatio						
Secure Client File				Displ	lying 1 - 4 of 4 rows IC ⊂ Page 1	of 1 >> I C

Image\_Client\_Sécurisé\_Téléchargement\_FMC

#### Étape 4. Accédez à Objects > Object Management > Network.

Étape 4.1. Créez un objet pour le serveur DNS. Cliquez sur Add Object, indiquez le nom et l'adresse IP DNS disponible. Cliquez sur Save.

Center Overview Analysis Policier	Devices Objects Integration		Deploy	Q 🗳 🌣 🙆 admin v	eisee SECURE
Network A network object represents one or more IP addresse	is. Network objects are used in various places, including acce	iss control policies, network variables, intrus	Add Network Add Network Ion rules, identity rules, network discovery rule Import Add G	v     Q, Filter     bject     Object     orts, and so on.	Dbjects
Name			Value	Type Override	
any	New Network Object	0	0.0.0.0/0	Group	<b>₽</b> < ; #
any-ipv4			0.0.0/0	Network	¶a. ⊕ #
	Description  Network Host Range Network Allow Overrides	Gancel Save			
	Center Overview Analysis Policies           Network         An etwork object represents one or more IP addresse           Name         any           any         any-ipv4	Center Overview Analysis Policies Devices Objects Integration  Network  A network object represents one or more IP addresses. Network objects are used in various places, including accompany my my my my Description Description Network Host Range Network Allow Overrides	Center Overview Analysis Peticles Devices Objects Integration  Network  A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrus  Name  Name  Name  Name  Name  Network  Name  Network  Network Networ	Center Overview A adaptis Policies Devices Opligetts Integration Depicy   A data Device   A data Device A data Device A data Device A data Device A data Device   A retwork doject represents one or more P addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network dilcomery rule   Name View   Name 0.0.0.00   Network   Description   Network   Host   Range   Network   A llow Overrides   Sive	Center Overview Analysis Decker Opjects Interest on the presents one or more IP addresses. Network Objects are used in various places, including access control policies, network variables, intrusion rules, identify rules, network discovery rule Add Decivity <t< td=""></t<>

FMC\_Add\_Object\_DNS



Remarque : le serveur DNS configuré ici doit être utilisé pour les utilisateurs VPN.

Étape 4.2. Créez un objet pour ISE PSN. Cliquez sur Add Object, indiquez le nom et l'adresse IP PSN ISE disponible. Cliquez sur Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policie	s Devices Objects Integration		Deploy	ର୍ 🚱 🌣 🙆 admin 🗸 ଅନେଥିକ SECURE
Distinguished Name     DNS Server Group     External Attributes     File List	Network A network object represents one or more IP address	is. Network objects are used in various places, including acces	s control policies, network variables, intrusi	Add Network Add Obj Import O Add Gro	Q. Filter     Objects     Objects     orts, and so on.
<ul> <li>FlexConfig</li> <li>Geolocation</li> <li>Interface</li> </ul>	Name any	New Network Object	0	Value 0.0.0.0/0 :/0	Type Override Group 🐴 Q 🗑 🙏
Key Chain Network	any-ipu4	Name	1	0.0.0/0	Network 🖥 Q 🗑 🤼
		Description			
		Network  Host Range Network  Allow Overrides	O FQDN		
			Cancel		

#### FMC\_Add\_Object\_ISE

Étape 5. Accédez à Objects > Object Management > VPN > Group Policy. Cliquez sur Add Group Policy. Cliquez sur DNS/WINS, sélectionnez l'objet du serveur DNS dans Primary DNS Server. Cliquez ensuite sur Save.

Firewall Managemen	nt Center Overview Analysis Polic	es Devices Objects Integration		Deploy Q 🧬 🌣 🛛 admin 🗸 📩
Distinguished Name     DNS Server Group     External Attributes     File List	Group Policy A Group Policy is a set of attribute and value pairs,	stored in a group policy object, that define the remote access VPN	experience.The RADIUS authorization server assigns the group policy or it is ob	Add Group Policy Q. Filter
> FlexConfig Geolocation	Name			
Key Chain Network Policy List Port Port Port Port Port Port Port Por		Name*  posture_gp  Description:  General Secure Client Advanced  VPN Protocols  P Address Pools Banner  DMS/VM/S Split Tunneling Secondary UNIS Server:  DHCP Network Scope:  OHCP Network Scope:  Oht/ network client in the i	v         +           v         +           v         +           v         +           v         +           v         +           v         +           v         +           v         +           v         +           v         +           v         +           v         +	28
IKEVT IP36E Proposal IKEV1 Policy IKEV2 Policy IKEV2 Policy Secure Client Customizatio Secure Client File			Cancel	Displaying 1 - 2 of 2 rows $ A  \leq Page$ 1 of 1 > 1 C

FMC\_Add\_Group\_Policy



**Remarque** : assurez-vous que le serveur DNS utilisé dans la stratégie de groupe VPN peut résoudre le FQDN et le enroll.cisco.com du portail d'approvisionnement du client ISE.

Étape 6. Accédez à Objects > Object Management > Access List > Extended. Cliquez sur Add Extended Access List.

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 💕 🌣 🙆	admin ~ dealer SECURE
<ul> <li>AAA Server</li> <li>RADIUS Server Group</li> <li>Single Sign on Server</li> </ul>	Extended An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-identifies traffic based on destination address or addresses. You use these objects when configuring particular features, such as route maps.	Add Extended Access List Q. Film	ports. Supports IPv4 and IPv6
Access List Extended	Name	Value	Override

FMC\_Add\_Redirect\_ACL

Étape 6.1. Indiquez le nom de la liste de contrôle d'accès de redirection. Ce nom doit être le même que dans le profil d'autorisation ISE. Cliquez

#### sur Add.

#### New Extended Access List Object

Name redirect											
Entries (0)											
									Add		
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT			
No records to display											
Allow Ov	verrides										

#### FMC\_Add\_Redirect\_ACL\_Part\_1

Étape 6.2. Bloquez le trafic DNS, le trafic vers l'adresse IP PSN ISE et les serveurs de conversion pour les exclure de la redirection. Autorisez le reste de la circulation. Cela déclenche la redirection. Cliquez sur Save.

Add Extended Access List Entry				0
Action: Block				
Logging:				
Default				
Log Level:				
Informational •				
Log Interval:				
300 Sec.				
Network Port  Opplication	s 🕕 Security Group Tag			
Available Networks C +		Source Networks (0)	Destination Networks (1)	
Q Search by name or value		any	ISE_PSN	Ì
IPv4-Private-192.168.0.0-16	Add to Source			
IPv4-Private-All-RFC1918				
IPv6-IPv4-Mapped				
IPv6-Link-Local				
IPv6-Private-Unique-Local-Addresses				
IPv6-to-IPv4-Relay-Anycast				
ISE_PSN_				
rtp_ise		Enter an IP address Add	Enter an IP address	Add

FMC\_Add\_Redirect\_ACL\_Part\_2

Cancel Save

Cancel

Name redirect									
Entries (4)									Add
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	any-ipv4	Any	ISE_PSN_	Any	Any	Any	Any	1
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	11
3	Block	Any	Any	FTP	Any	Any	Any	Any	11
4 Allow O	Allow verrides	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	11

Cancel Save

 $FMC\_Add\_Redirect\_ACL\_Part\_3$ 



Remarque : le FTP de destination dans cet exemple de liste de contrôle d'accès de redirection est utilisé comme exemple de serveur

Étape 7. Accédez à Objects > Object Management > RADIUS Server Group. Cliquez sur Add RADIUS Server Group.

þ	Firewall Management Objects / Object Management	t Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	69
~	A Server RADIUS Server Group	RADIUS	Server G	àroup					_ A	Add RADIUS Serv	er Grou	ip.
~ Acc	Single Sign-on Server	RADIUS Serv	er Group object	ts contain one	or more refere	ences to RADI	US Servers. Ti	ese AAA servers are used to authenticate users logging in through Remote Access VPN conne	ctions.			
	Extended	Name							Value			

FMC\_Add\_New\_Radius\_Server\_Group

Étape 7.1. Indiquez le nom, la vérification Enable authorize only, la vérification Enable interim account update, la vérification Enable dynamic authorization.

Name:*	_
rtpise	
Description:	
Group Accounting Mode:	
Single	▼
Retry Interval:* (1-10) Seconds	
10	
Realms:	
	▼
Enable authorize only	
Enable interim account update	
Interval:* (1-120) hours	
24	
Enable dynamic authorization	
Port:* (1024-65535)	
1	1
	Cancel Save

 $FMC\_Add\_New\_Radius\_Server\_Group\_Part\_1$ 

Étape 7.2. Cliquez sur l'Plus icône pour ajouter un nouveau serveur RADIUS. Fournissez le PSN ISE IP Address/Hostname, Key. Sélectionnez le specific interface pour la connexion. Sélectionnez la Redirect ACL. Cliquez ensuite sur Savepour enregistrer le nouveau serveur RADIUS. Cliquez ensuite Save à nouveau sur pour enregistrer le nouveau groupe de serveurs RADIUS.

?

Add RADIUS Server Group	0	New RADIUS Server	0
<ul> <li>Enable authorize only</li> <li>Enable interim account update</li> <li>Interval:* (1-120) hours</li> <li>24</li> <li>Enable dynamic authorization</li> <li>Port:* (1024-65535)</li> <li>1700</li> <li>Merge Downloadable ACL with Cisco AV Pair ACL</li> </ul>		IP Address/Hostname:* Configure DNS at Threat Defense Platform Settings to resolve hostname Authentication Port:* (1-65535) 1812 Kev:*  Confirm Key:*  Accounting Port: (1-65535)	•
After Cisco AV Pair ACL     Before Cisco AV Pair ACL     RADIUS Servers (Maximum 16 servers)	+	1813           Timeout:         (1-300) Seconds           10	
IP Address/Hostname No records to display		Connect using: Routing Specific Interface + Inside_zone + Redirect ACL: redirect \	
Cance	I Save	Cancel	Save

FMC\_Add\_New\_Radius\_Server\_Group\_Part\_2

Étape 8. Accédez à Objects > Object Management > Address Pools > IPv4 Pools. Cliquez sur Add IPv4 Pools et indiquez les **Name, IPv4 Address Range**et Mask. Cliquez ensuite sur Save.

Firewall Managerr Objects / Object Manager	ent Center Overview Analysis Policies Devices	Objects Integration		Deploy Q 💕 🌣 😰 fangni -	cites SECURE
> AAA Server > Access List > Address Pools	IPv4 Pools	gnostic interface with clustering, or for VPN remote access profiles.		Add IPv4 Pools	
PH4 Rools     PH4 Rools     PH4 Rools     Application Fitters     AS Path     BFD Template     Cipher Suite List     DHCP IPv6 Pool     Otstinguished Name     DHS Server Group     Startal Attibutes     File List     PH4 Rools     File List     RexConfig     Geolocation     Interface     Kery Chain     Network     PH6     Policy List     Port     Port     Suite Map     Security intelligence     Sinkhole     Sinkhole     Sink Monitor     Time Remone	Norme 	Add IPv4 Pool          Name*         posture_pool         Description         IPv4 Address Range*         192.168.6.30-192.168.6.100         Format: Ipaddr-Ipaddr e.g., 10.72.1.1-10.72.1.150         Mask*         255.255.55.0         INO Overrides         Ondigue device overrides in the address pool object to shared across multiple devices         I Override (0)	Cancel	Override	/1
Time Zone Tunnel Zone URL Variable Set				Displaying 1 - 2 of 2 rows  < < Page	of 1 > >1 C

FMC\_Add\_New\_Pool

Étape 9. Accédez à Certificate Objects > Object Management > PKI > Cert Enrollment. Cliquez sur Add Cert Enrollment, indiquez un nom, puis sélectionnez Self Signed Certificatedans Enrollment Type. Cliquez sur l'Certificate Parameters onglet et indiquez Common Name et Country Code. Cliquez ensuite sur Save.

Firewall Management Objects / Object Management	t Center Overview Analysis Policies Devic	es Objects Integration		Deploy Q 🚱 🗘 🕢 fangni
AAA Server     Access List     Address Pools     Angleation Filters	Cert Enrollment A certificate enrollment object contains the Certification Authority your Private Key Infrastructure (PKI).	(CA) server information and enrollment parameters	that are required for creating Certificate Signing Requests (CSRs) and obtaining	Add Cert Enrollment Q, Filter
AS Path BFD Template	Name			Type Override
Cipher Suite List > Community List DHCP IPv6 Pool > Distinguished Name DNS Server Group > External Attributes File List > FlaxConfig Geolocation Interface Key Chain Network > PKI Cert Enrollment External Cert Groups Internal CA Groups Internal CAS Internal CAS	Name*         @emo_spn         Description         CA Information Certificate Parameters Key Revoc         Enrollment Type:         Salt Signed Certificate         VPN: To compare CA, Inservingte to "Certificate Parameters Validation Usage:         Validation Usage:         © Psec Client © SSI Client	ation	PLOU VEIT EITHOMITTERN  Name*  demo_vpin  Description  CA Information Certificate Parameters Key Revocation Include PQDN: Don't use PQDN in certificate Include PqUNca's IP Address: Common Name (CM): Corganization (UN): Corganization (UN): Coganization (UN): C	m     m     m
Trusted CAs Policy List	Allow Overrides		Allow Overrides	
Port Prefix List Route Map Security Intelligence		Cancel Save		Cancel Seve Displaying 1 - 3 of 3 rows I < < Page 1 of 1 >> I C

FMC\_Add\_New\_Cert\_Enroll

Étape 10. Accédez à Devices > Certificates. Cliquez sur Add, sélectionnez le nom FTD sous Device, sélectionnez l'inscription configurée précédente sous Cert Enrollment. Cliquez sur Add.

Firewall Manager Devices / Certificates	nent Center	Overview Analysis	Policies Devices Obje	ects Integration		Deploy Q 💕	¢ 0	fangni v ence SECURE
Filter All Certificates	٠							Add
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status			
Add New Cer	tificate			0				•
Add New Cer	lineate			•	O CA LD			± @ C 🗑
Add a new certifi	cate to the devi	ce usina cert enro	ollment object which is us	ed to	G.CA (LD)			± 2 C T
generate CA and	identify certific	ate.						<u>۵</u>
Device*:					(e) CA			±₽С∎
Posture-FTD-C	ML27	•						
Cort Enrollmont*:								
damo und								
dente pri		•						
Cert Enrollment D	etails:							
Name:	demo_vp	n						
Enrollment Type:	Self-Sign	ed						
Enrollment URL:	N/A							
			Cancel	Add				

FMC\_Add\_New\_Cert\_To\_FTD

Étape 11. Accédez à Devices > VPN > Remote Access. Cliquez sur Add.

Étape 11.1. Saisissez le nom et ajoutez le FTD à Selected Devices. Cliquez sur Next.

Firewall Management Center Overview Devices / VPN / Setup Wizard	Analysis Policies Devices Objects Integration		Deploy Q 💕 🌣 🔕 admin 🗸 🕬 SECURE
Firewall Management Center     Overview     Overview     Connection Profile     Policy Assignment     (2) Connection Profile	Analysis     Policies     Devices     Objects     Integration            • Secure Client       • Access & Certificate       • Summary    Targeted Devices and Protocols  Takenes  Ven Protocols:         • State	Before You Start Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy. Authentication Server Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients. Secure Client Package Make sure you have Secure Client package for VPN Client downloaded it during the wizard. Device Interface Interfaces should be already configured on targeted	Deptoy Q
	Available Devices       Q, Search     Selected Devices       Posture-FTD-CML27     Image: Comparison of the second seco	Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.	Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_1

Étape 11.2. Sélectionnez le groupe de serveurs RADIUS précédemment configuré dans la Authentication Server, Authorization Server, Accounting Server. Faites défiler la page.

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 😡 admin v 👘 SECURE
Remote Access VPN Policy Wizard	
1) Policy Assignment   Connection Profile  Secure Client  Access & Certificate  Summary	
Secure Clerit       Understand         Secure Clerit       Understand         Connection Profile       Connection Profiles         Connection Profile is specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itset, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.         Connection Profile Name:*       Connection Profile Name:*	
This name is configured as a connection alias, it can be used to connect to the VPN gateway	
Authentication, Authorization & Accounting (AAA):	
Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.	
Authentication Method: AAA Only	
Authentication Server:*  Tipise  UCUAL or Health or HAUNUS)  Failback to LOCAL Authentication	
Authorization Server: replace +	
Accounting Server:	
Client Address Assignment:	
	Cancel Back Next

 $FMC\_New\_RAVPN\_Wizard\_2$ 

Étape 11.3. Sélectionnez le nom du pool précédemment configuré dans IPv4 Address Pools. Sélectionnez la stratégie de groupe précédemment configurée dans Group Policy. Cliquez sur Next.

Firewall Management Center Overview Analysis Polici	cies Devices Objects Integration	Deploy Q 🚱 🌣 🕢 admin V 🔐 SECURE
Remote Access VPN Policy Wizard		
1 Policy Assignment  2 Connection Profile  3 Secure Client -	Access & Certificate      S Summary	
	Accounting Server: (9AD/05) + (9AD/05)	
	Client Address Assignment:	
	Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.	
	Use AAA Server (Realm or RADIUS only)	
	Use DHCP Servers	
	Use IP Address Pools	
	IPv4 Address Pools: posture_pool	
	IPv6 Address Pools:	
	Group Policy:	
	A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.	
	Group Policy:* posture_gp +	
	Edit Group Policy	

Cancel Back

 $FMC\_New\_RAVPN\_Wizard\_3$ 

#### Étape 11.4. Cochez la case de l'image Linux. Cliquez sur Next.

Firewall Management Center Overview Analysis Devices / VPN / Setup Wizard	Policies Devices Objects Integration	Deploy Q 🚱 🌣 🛛 admin ~ 🔤
Remote Access VPN Policy Wizard		
1 Policy Assignment 2 Connection Profile 3 Secure Cli	ent 6 Access & Certificate 5 Summary	
	Remote User Client Mermet Outside Upper Inside Corporate Resources	
	The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.	
	Download Secure Client packages from Cisco Software Download Center.	
	Show Re-order buttons +	
	Secure Client File Object Name     Secure Client Package Name     Operating System	
	client_image cisco-secure-client-win-5.1.3.62-webdepio Windows •	
	☑ linux_5_1_3_62 cisco-secure-client-linux64-5.1.3.62-webd Linux ▼	

Cancel Back Next

 $FMC\_New\_RAVPN\_Wizard\_4$ 

Étape 11.5. Sélectionnez l'interface de l'interface VPN. Sélectionnez l'inscription de certificat qui s'est inscrite sur FTD à l'étape 9. Cliquez sur Next.



Cancel Back Next

FMC\_New\_RAVPN\_Wizard\_5

Étape 11.6. Double-confirmez les informations associées sur la page de résumé. Si tout va bien, cliquez sur Finish. Si vous devez modifier quelque chose, cliquez sur Back.





Étape 12. Déployez la nouvelle configuration sur FTD pour terminer la configuration VPN d'accès à distance.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy R. 6	C O admin ~ chills SECURE
posture_vpn			Q Advanced Deploy	ore warnings Deploy Cancel
			Posture-FTD-CML27	eady for Deployment ents.(1)
Connection Profile Access Interfaces Advanced				ty: None
				+
Namo	AAA	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authonization: None Accounting: None	DftGrpPolicy		
posture_vpn	Authentication: rtpise (RADIUS) Authonization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	E posture_gp	1 selected 0 1 pending	20

FMC\_Deploy\_FTD

#### Configurations sur ISE

Étape 13. Accédez à Work Centers > Posture > Network Devices. Cliquez sur Add.

≡	dentity Services	Engine					Work Centers	Posture				۹	۵	0	Q	۹
н	Bookmarks	Overview	Network D	evices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
	Dashboard															
명	Context Visibility	Net	work De	evices												
×	Operations												Selected (	Total	Ø	٥
0	Policy	Ø Edit	+ Add (	) Duplicate	🕁 Import 🖞 Export	Generate PAC	O Delete 🗸								AII V	V
80	Administration		Name ^	IP/Mask	Profile Name	Location	Туре		Description							
	Work Centers	0	FTD-CML2		🗰 Cisco 🕕	All Locations	Firewall									
-		0	FTD-CML2	1.0	🟥 Cisco 🕕	All Locations	Firewall									
			FTD+CML2		🗯 Cisco 🕕	All Locations	Firewall									
0	Interactive Help		8.00	1000	🗯 Cisco 🕕	All Locations	Firewall									

ISE\_Add\_New\_Devices

Étape 13.1. Fournissez le Name, IP Addresset faites défiler la page vers le bas.

≡ ;;	line Identity Servi	ces Engine				w	ork Centers / I	Posture		
Щ	Overview Net	work Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Network Devices	List > New Network D	Device							
× 0	Name	posture-FTD		_						
80	Description			-						
កា	IP Add	ress 🗸 * IP :	u		¢					
?	Device Profile	e 👬 Cisco	~	()						
	Model Name		~							
	Software Vers	sion	~	-						
	Network Devi	ce Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Devic	e	~	Set To Default					

ISE\_Add\_New\_Devices\_1

Étape 13.2. Cochez la case de RADIUS Authentication Settings. Fournissez le Shared Secret. Cliquez sur Submit.

$\equiv \frac{1}{1000}$ Identity Services	Engine					•	/ork Centers / P	osture			۵ ۵ (	D O A
J. Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings			
E: Dashboard		~ RADIUS Authent	tication Settings									
16 Context Visibility		RADIUS UDP Setting	15									
% Operations		Protocol RA	DIUS									
Policy		Shared Secret		Show								
		Use Second Shared	Secret ()									
ALL CONTRACTOR		Secre	10 oneneu 1		Show							
③ Interactive Help		CoA Port 1	700	Set To Defa	a.							
		RADIUS DTLS Setting	gs 🛈									
		DTLS Required										
		Shared Secret rad	lius/dtls									
		CoA Port 2	083	Set To Defa	a							
		Issuer CA of ISE Certificates for CoA 5	ielect if required (optional)	~ <u>0</u>								
		DNS Name										
		General Settings										
		🗌 Enable KeyWrap 🕕	)									
		Key Encryption Key		Show								
		Message Authenticator Code Key		Show								
		Key Input Format ASCII O HEXA	DECIMAL									
		V TACACS Author	tication Settings									
		<ul> <li>SNMP Settings</li> </ul>										
		<ul> <li>Advanced Trust</li> </ul>	Sec Settings									
											Submit	Cancel

ISE\_Add\_New\_Devices\_2

Étape 14. Téléchargez le nom cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg du package à partir de <u>Téléchargement</u> <u>de logiciel Cisco</u> et assurez-vous que le fichier est correct en confirmant que la somme de contrôle md5 du fichier téléchargé est identique à la page Téléchargement de logiciel Cisco. Le nom du package cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg a été téléchargé à l'étape 1.

Étape 15. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent resources from local disk.

≡	diada Identity Services Engine			Wo	rk Centers /	Posture			
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
■ 18 火	Client Provisioning Policy Resources Client Provisioning Portal	Resources	🚺 Duplicate 🏾 🔋 De	leto				Selec	ted 0 Total 16 🔗 All V 🖓
		Agent res	ources from Cisco site		Т	vpe v	Version	Last Update	Description
-		Agent res	ources from local disk		v	VinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Prov
-ili		Native Su	oplicant Profile		N	lative Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
		Agent Cor	figuration		N	lative Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?		Agent Pos	ture Profile		N	MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Pro
		AMP Enab	ler Profile	5.1.3.062	c	iscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure (
		CiscoSecure	ClientDesktopLinux 5.1	.3.062	c	iscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure C
		CiscoSecure	eClientComplianceModu	leWindows 4.3.4015.819	2 C	iscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
		CiscoSecure	ClientComplianceModu	leLinux 4.3.3139.0	c	iscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure (
		CiscoAgent	essWindows 5.0.03061		C	iscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAgenti	lessOSX 5.0.03061		C	iscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTempo	oralAgentWindows 5.0.0	3061	C	iscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
		CiscoTempo	oralAgentOSX 5.0.03061	1	c	iscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

Ressource\_Téléchargement\_ISE

Étape 15.1. Sélectionnez Cisco Provided Package. Cliquez sur Choose File cette option pour télécharger cisco-secure-client-linux64-5.1.3.62webdeploy-k9.pkg. Cliquez sur Submit.

= -duales cisco	Identity Services E	ngine		Work Centers / Posture Q 🖉	9 Q   A
비 Bookm III Dashbi III Contes 옷 Operat II Policy	narks Hoard xt Visibility tions Histration	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local Agent Resources Fro Category	cal Disk > Agent Resources From Local Disk From Local Disk Cisco Provided Package 🗸 🖓	
H Work C	Centers			Choose File cisco-secureeploy-k9 pkc	
⑦ Interac	ctive Help		Submit	✓ Agent Uploaded Resources           Name         ^         Type         Version         Description           CiscoSecureClientDesktopLi         CiscoSecureClientDe         5.1.3.62         Cisco Secure Client for II	

ISE\_Upload\_Resources\_1



Remarque : répétez l'étape 14. pour télécharger cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

Étape 16. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent Posture Profile.

≡ :	Indentity Services Engine				Work Cent	ers / Posture			
Щ	Overview Network Devices	Client Provisioni	Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Setting	S	
	Client Provisioning Policy Resources	Resource	es						
×	Client Provisioning Portal							Selected 0 Total 16	Ø
		🖉 Edit 🛛 🕂 Add	A Duplicate 🛛 D	elete				All 🗸	$\nabla$
		Ager	nt resources from Cisco site	,	Version	Last Update	Description		
40		Ager	nt resources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii		
ា		Natio	ve Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S		
		Ager	nt Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu		
?		Ager	nt Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			
			Enabler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

Profil\_Posture\_Agent\_Ajout\_ISE

Étape 16.1. Fournissez le Name, Server name rules et conservez le reste par défaut. Cliquez sur Save.

#### Nom : linux\_agent\_profile

#### Règles de nom de serveur : \*.example.com

= do	👷 Identity	Services Engine			Wa	ork Centers /	Posture			
щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ 18 火 ● ▲0	Client Provis Resources Client Provis	oning Policy	ISE Posture Agent Profile Set Agent Posture Profil Name * linux_agent_profile Description:	e						
(?)			Agent Behavior Parameter Enable debug log		Value No ~	D	escription nables the debug log	on the agent		

ISE\_Add\_Agent\_Posture\_Profile\_1

≣ "	sco Identity	Services Engine			w	ork Centers / F	Posture		
FI.	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provis Resources	ioning Policy	Posture Protocol						
×	Client Provis	ioning Portal	Parameter	Value			Description		
0			PRA retransmission ti	me 120	secs		This is the age communication	nt retry period n failure	if there is a Passive Reassessment
<b>a</b>			Retransmission Delay	() 60	secs		Time (in secon	ds) to wait bef	lore retrying.
ส์เ			Retransmission Limit	① <u>4</u>			Number of retr	ies allowed for	r a message.
?			Discovery host ①				Enter any IP ac detects and re portal.	Idress or FQDN directs that htt	N that is routed through a NAD. The NAD p traffic to the Client Provisioning
			Discovery Backup Ser	ver List Choose	9		By default, An PSNs sequenti as the backup discovery prob	Connect sends ally if the PSN list and restrict es.	s discovery probes to all the Cisco ISE is unreachable. Choose specific PSNs t the nodes to which AnyConnect sends
			Server name rules * (	) •.examp	ple.com		A list of wildca servers that th	rded, comma- e agent can co	separated names that defines the nnect to. E.g. "*.cisco.com"
			Call Home List 🕕				A list of IP add that the agent endpoint does	iresses, that de will try to conn n't respond for	fines the all the Policy service nodes tect to if the PSN that authenticated the some reason.
			Back-off Timer ①	30	secs		Agent will cont targets and pro packets till this	tinuously try to eviously connects max time limit	reach discovery targets (redirection cted PSNs) by sending the discovery t is reached
									Cancel

ISE\_Add\_Agent\_Posture\_Profile\_2

Étape 17. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent Configuration.

≡ :	Identity Services I	Engine				Work Cente	ers / Posture				
щ	Overview Network	Devices Client P	rovisioning Po	olicy Elements	Posture Policy	Policy S	Sets Troublesho	ot Reports S	Settings		
	Client Provisioning Policy Resources	Res	ources								
×	Client Provisioning Portal									Selected 0 Total 16	g
		🖉 Edit	+ Add \land 👘 🖸	Duplicate 🛛 🍵 Dele	ite					aii $\sim$	$\nabla$
Ψ.			Agent resources	from Cisco site		Version	Last Update	Description			
a.			Agent resources	from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client	for li		
-fi		0	Nativo Supplican	t Profile	o Supplicent Dro	Not Applie	2016/10/07 04:01:12	Dra configured Noti			-1
			Native Supplication	( PTOTILE	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Nati	ve 5		-1
			Agent Configurat	son	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client	Linu		_
(?)			Agent Posture Pr	rofile	ntProfile	Not Applic	2024/05/08 10:37:17				- 1
			AMP Enabler Pro	file	ntProfile	Not Applic	2024/05/16 15:15:49				

ISE\_Add\_Agent\_Configuration

Étape 17.2. Configurez les détails :

Package Select Agent : CiscoSecureClientDesktopLinux 5.1.3.062

Nom : linux\_agent\_config

Module de conformité : CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Cochez la case de VPN, Diagnostic and Reporting Tool

Position ISE de sélection de profil : linux\_agent\_profile

#### Cliquez sur Submit.

≡ :	indentity	Services Engine					Work Cent	ers / Postu	re
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provis	ioning Policy					1		
1d	Resources		* Select Agent Package:	Ci	scoSecureClientDesktopLin	ux 5.1.3.062 V			
*	Client Provis	ioning Portal	* Configuration Name:						
0			linux_agent_config						
80			Description:						
-fli				le le					
0			Description Value N	otes					
			* Compliance Module CiscoSecu	reClientComplianceModule	Linux 4.3. ~				
			Cisco Secure Client	Module Selection					
			ISE Posture 🛛 VPN 🗹						
			Secure Firewall Dosture						
			Network Disibility						
			Diagnostic and Reporting 🗹 Tool						
			Profile Selection						
			* ISE Posture linux_agen	at_profile	~			Su	ibmit Cance

ISE\_Add\_Agent\_Configuration\_1

Étape 18. Accédez à Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Cliquez Edit à la fin du nom d'une règle. Sélectionnez Insert new policy below.

= -	diale Identity	Services	Engine									Wo	ork Ce	enters / Postu	e					
щ	Overview	Network	Devices	Clie	ent Provi	sioning	Policy Elemen	its	Posture Policy	,	Policy Sets	Trouble	eshoot	Reports	Settings					
111 131 141 141 141 141 141 141 141 141	Client Provi Resources Client Provi	isioning Policy	]	C Defi For For Intel For Mac If you	lient Agent Cor Native Suy dows Age 1 architect Windows 2 ARM64 p bu configui nout an AR	Provision figuration: v pplicant Con nt, Mac Age ures. Mac pu Agent ARM6 iolicies require an ARM64 conditi	ioning Policy to deter ersion of agent, as figuration: wizard p nt, Mac Temporal a blicies run the sam 4 policies, configu e no Other Condil c client provisioning n. This is because	miningent profi	cy e what users will recc profile, agent compli le and/or wizard. Dra Mac Agentiess policie cxage for both archit ession: OS-Architect a arm64 configuration licy for an OS, ensure endpoint is matched	eive up ance g and ecture ure E0 s. e that seque	pon login and use module, and/or ag drop rules to chan port ARM64. Wini 39. 2UALS arm64 in ti the ARM64 policy entially with the po	session in ent custor age the or tows polic to Other C is at the b licies liste	nitiation mization der. ies run condition op of th d in this	: package. separate packages ns column. ie conditions list, al s window.	for ARM4 and read of policies					
				$\sim$																
?						Rule Name	•		Identity Groups		Operating Syste	ms		Other Conditions			Resul	ts		
				8		IOS		H	Any	and	Apple IOS All		and	Condition(s)		then	Cisco-	ISE-NSP	Edit 🗸	
				8		Android		If	Any	and	Android		and	Condition(s)		then	Cisco-	ISE-NSP	Editis	
																	1	Duplicate above Duplicate below Insert new policy ab	low	

Étape 18.1. Configurez les détails :

Nom de la règle : Linux

Systèmes d'exploitation : Linux All

Résultats : linux\_agent\_config

Cliquez sur Done et Save.

= :	indentity	Services Engine							Wo	ork C	enters / Postu	ire				
Щ	Overview	Network Devices	Client Pro	visioning	Policy Elements	Post	ture Policy	Policy Se	ts Trouble	eshoo	t Reports	Settings				
11日 1日 火 日 よ。	Client Provis Resources Client Provis	ioning Policy	Client Define the 0 For Agent 0 For Native 5 Windows Af Intel archite For Window Mac ARM64 If you config without an A	Client Provision Configuration: 1 Supplicant Cor gent, Mac Age cctures. Mac p rs Agent ARM6 4 policies requ gure an ARM64 ARM64 conditi	sioning Policy to determine version of agent, agent Inguration: wizard profili- ent, Mac Temporal and I oblicas run the same pa B4 policies, configure S irite no Other Conditions 4 delient provisioning po ion. This is because an	e what us profile, a le and/or Mac Agen ickage for iession: O s arm64 ci licy for an endpoint	ers will receive gent complianc wizard. Drag an titless policies si both architecture onfigurations. 0 S, ensure the is matched seq	upon login ar a module, and d drop rules upport ARM6- res. EQUALS armi t the ARM64 uentially with	d user session i l/or agent custo io change the or b. Windows polic 64 in the Other C policy is at the t the policies liste	initiation mizatio rder, cies run Conditio top of t ed in th	n: in package. in separate package ons column. the conditions list, a is window.	s for ARM4 and ahead of policies				
0				Rule Nam IOS Android Linux	e it it	Identity Any Any Any	Groups and and and	Operating Apple IOS A Android Linux All	Systems	and and and	Other Conditions Condition(s) Condition(s) Condition(s)	1	then then then	Results Cisco-ISE-NSP Cisco-ISE-NSP linux_agent_config	E	dit v dit v dit v

ISE\_Add\_New\_Provisioning\_Policy\_1

=	dealer Identity Services Engine	Work Centers / Posture	
Щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
王 ふ 火 日	Cenditions Anti-Malware Anti-Spyware Anti-Virus Application	C Vew ⊘ Edt + Add □ Duplicate	Selected 0 Total 385 <i>②</i> ۞ 제 ~ ♡
80	Compound	Name Description File name Condition Type	
35	Dictionary Compound	pc_XP84_K82797052_MS13 Cisco Predefined Check: SYSTEM_PROGRAMS\C Cisco-Defined	
-	Disk Encryption	pc_W8_64_xB3124275_MS Clsco Predefined Check: SYSTEM_ROOT(sysnativ Clsco-Defined	
	External DataSource	pc_Vista_K62893294_MS13 Cisco Predefined Check: SYSTEM_32\Imagehip.dll Cisco-Defined	
(?)	File	pc_W81_64_K83033889_M Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Firewall	pc_Vista64_K8925902_MS0 Cisco Predefined Check: SYSTEM_ROOT\winsxs\a Cisco-Defined	
	Hardware Attributes	pc_W10_64_1709_K845803 Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Registry	pc_XP_K82653956_MS12+0 Clsco Predefined Check: SYSTEM_32\Wintrust.dll Cisco-Defined	
	Script	pc_W8_x82892074_MS13 Cisco Predefined Check: SYSTEM_32\Scrrun.dll Cisco-Defined	
	Service	pc_W10_64_1909_K850139 Cisco Predefined Check: SYSTEM_ROOT\SysWO Cisco-Defined	
	USB	pc_W7_K02681578_MS12+ Cisco Predefined Check: SYSTEM_32\Win32k.sys Cisco-Defined	
	Remediations >	pc_W10_K83081436_MS15 Clsco Predefined Check: SYSTEM_32\Edgehtml.dll Clsco-Defined	
	Besultements	pc_W81_64_K83042553_M Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Allowed Protocols	pc_W8_64_K82727528_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Authorization Profiles	pc_W8_64_KB2002611_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Downloadable ACLs	pc_W7_K83078601_M515 Cisco Predefined Check: SYSTEM_32\Win32k.sys Cisco-Defined	

Étape 19. Accédez à Work Centers > Posture > Policy Elements > Conditions > File. Cliquez sur Add.

Étape 19.1. Configurez les détails :

Nom : linux\_demo\_file\_existing

ISE\_Add\_New\_File\_Condition

Systèmes d'exploitation : Linux All

Type de fichier : FileExistence

Chemin d'accès au fichier : home, Desktop/test.txt

Opérateur de fichier : existe

Cliquez sur Submit.

≡	doub. Identity Services Engine				Work Cer	nters / Post	ture	
н	Overview Network Devices	Client Provisioning Policy E	ements Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
	Conditions Anti-Malware Anti-Sipware Anti-Yuus Application Compound Dictionary Compound Dictionary Compound Dictionary Simple Disk Encryption Exernation Disk Encryption Disk Encryption Pise Firemall Hardware Attributes Pitch Management Registry Script Script Script	File Conditions List > New File Condition File Condition Name * Inux_demo, Description * Operating System Linu Compliance Module Any version * File Type FileExistence * File Path home * File Operator Exists	All	p/tost.txt	]			Submit
	Remediations > Requirements Allowed Protocols Authorization Profiles Downloadable ACLs							

 $ISE\_Add\_New\_File\_Condition\_1$ 

Étape 20. Accédez à Work Centers > Posture > Policy Elements > Requirements. Cliquez Edit à la fin du nom d'une règle. Sélectionnez Insert new Requirement.

=	dender Identity Services E	ingine							Work	Centers / Po	osture					
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	Elements	Posture	Policy Policy Sets	Tro	ubleshoot	Reports \$	ettings				
5 1	Dashboard Context Visibility	Conditions Anti-Malw	~									Guide Me				
×	Operations	Anti-Spyw	are	Requirements												
0	Policy	Anti-Virus		Name		Operating Sys	tem	Compliance Module		Posture Type		Conditions		Remediations Actions	_	
	Administration	Compound	5	Any_AV_Installation_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_inst	then	Message Text Only	Edit 😔	
-	Automatication	Dictionary	Compound	Any_AV_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_def	then	AnyAVDefRemediationWin	Edit	Duplicate
nî)	Work Centers	Dictionary	Simple	Any_AS_Installation_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_inst	then	Message Text Only	Edit	Insert ner
		Disk Encry External D	ption	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit	Delete
1	Interactive Help	File		Any_AV_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_inst	then	Message Text Only	Edit 👻	1
		Firewall		Any_AV_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_def	then	AnyAVDefRemediationMac	Edit 🤟	
		Hardware	Attributes	Any_AS_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_inst	then	Message Text Only	Edit 🤟	
		Patch Mar	agement	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_def	then	AnyASDefRemediationMac	Edit 🛩	
		Registry		Any_AM_Installation_Win	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_inst	then	Message Text Only	Edit 🗵	
		Service		Any_AM_Definition_Win	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_def	then	AnyAMDerRemediationWin	Edit 😔	
		US8		Any_AM_Installation_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_inst	then	Message Text Only	Edit 😔	
				Any_AM_Definition_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_def	then	AnyAMDefRemediationMac	Edit 😣	
		Remediation	• >	Any_AM_Installation_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_inst	then	Select Remediations	Edit 🗵	
		Requirements		Any_AM_Definition_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_def	then	Select Remediations	Edit 9	
		Allowed Prot	ocols	US8_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	USB_Block	Edit 🤟	
		Authorization Downloadabl	Profiles e ACLs	Default_AppVis_Requirem ent_Win	n for	Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Win	then	Select Remediations	Edit 🤟	
				Default_AppVis_Requirem ent_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Mac	then	Select Remediations	Edit 😔	
				Default_Hardware_Attribu es_Requirement_Win	it for	Windows All	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 👻	
				Default_Hardware_Attribu es_Requirement_Mac	it for	Mac OSX	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 🤟	

ISE\_Add\_New\_Posture\_Requirement

Étape 20.1. Configurez les détails :

Nom : Test\_existing\_linux

Systèmes d'exploitation : Linux All

Module de conformité : version 4.x ou ultérieure

Type de posture : Agent

Conditions : linux\_demo\_file\_existing

Cliquez sur Done et Save.

≡ ;	Indentity Services Engine			Work Centers / Posture		
	Overview Network Devices	Client Provisioning Policy Elem	ments Posture Policy Policy Sets Tr	oubleshoot Reports Sett	tings	
<u> </u>						
	Conditions ~					~ 0
11	Anti-Malware			Guide Me		
*	Anti-Spyware	Requirements				
	Anti-Virus	Name Ope	erating System Compliance Module	Posture Type 0	Conditions Remediations Action	
•	Application		• •			
a.	Compound Dictionary Compound	Test_exist_linux for Linux	xx All using 4.x or later using	Agent met if	inux_demo_file_ex then Select Remediations ist	Edit 🗸
-51	Dictionary Simple	Any_AV_Installation_Win for Wind	dows All using 3.x or earlier using	Agent met if J	ANY_av_win_inst then Message Text Only	Edit 🛩
	Disk Encryption	Any_AV_Definition_Win for Wind	dows All using 3.x or earlier using	Agent met if /	ANY_av_win_def then AnyAVDefRemediationWi	Edit 🛩
0	External DataSource	Any_AS_Installation_Win for Wind	dows All using 3.x or earlier using	Agent met if /	ANY_as_win_inst then Message Text Only	Edit 🛩
	File	Any_AS_Definition_Win for Wind	dows All using 3.x or earlier using	Agent met if A	ANY_as_win_def then AnyASDefRemediationWi	Edit 🗸
	Firewall	Any_AV_Installation_Mac for Mac	OSX using 3.x or earlier using	Agent met if A	ANY_av_mac_inst then Message Text Only	Edit ~
	Patch Management	Any_AV_Definition_Mac for Mac	COSX using 3.x or earlier using	Agent met if J	ANY_av_mac_def then AnyAVDefRemediationMa	e Edit ~
	Registry	Any_AS_Installation_Mac for Mac	: OSX using 3.x or earlier using	Agent met if /	ANY_as_mac_inst then Message Text Only	Edit 👻
	Script	Any_AS_Definition_Mac for Mac	: OSX using 3.x or earlier using	Agent met if J	ANY_as_mac_def then AnyASDefRemediationMa	c Edit ↔
	Service	Any_AM_Installation_Win for Wind	dows All using 4.x or later using	Agent met if /	ANY_am_win_inst then Message Text Only	Edit v
	USB	Any AM Definition Win for Wind	dows All using 4.x or later using	Agent met if A	ANY am win def then AnyAMDefRemediationW	n Edit v
		Any AM Installation Mac for Mac	OSX using 4.x or later using	Agent met if A	ANY am mac inst then Message Text Only	Edit v
	Remediations	Any AM Definition Mac for Mac	DSX using 4.x or later using	Agent met if J	ANY am mac def then AnyAMDefRemediationM	
	Requirements	had been been been been been been been bee	and and the second	- Alexandre - A	an partane and representation of the	Eur v
	Allowed Protocols	Note:				
	Authorization Profiles	Remediation Action is filtered based on the op Remediation Actions are not applicable for App	perating system and stealth mode selection. oplication Conditions (configured using the Provision By Category	or Provision By Everything options), Hardwa	re Conditions, and External Data source conditions.	
	COMPROBIDIE PLOCS	Remediations Actions are not applicable for Ag	Agentiess Posture type.			
						Cause Darest
						Save

ISE\_Add\_New\_Posture\_Requirement\_1



Remarque : actuellement, seuls les scripts shell sont pris en charge pour les agents Linux en tant que correction.

Étape 21. Accédez à Work Centers > Posture > Policy Elements > Authorization Profiles. Cliquez sur Add.

Étape 21.1. Configurez les détails :

Nom : unknown\_redirect

Cochez la case de Web Redirection(CWA,MDM,NSP,CPP)

Sélectionner Client Provisioning(Posture)

ACL : redirection

#### Valeur : Client Provisioning Portal (par défaut)

≡ :	dialle Identity Services Engine	Work Centers / Posture
Щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
≣ 	Conditions Anti-Malware Anti-Spyware Anti-Spyware Anti-Virus Application Compound Dictionary Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall Hardware Attributes Patch Management	Authorization Profile   * Name   unknown_redirect   Description   * Access Type   ACCESS_ACCEPT   * Access Type   ACCESS_ACCEPT   Network Device Profile   # Cisco   Bervice Template   Track Movement   Image: I
	Registry Script Service US8 Remediations Requirements Allowed Protocols Authorization Profiles Downloadable ACLs	<ul> <li>Common Tasks</li> <li>Voice Domain Permission</li> <li>Web Redirection (CWA, MDM, NSP, CPP)</li> <li>Client Provisioning (Posture)</li> <li>ACL redirect</li> <li>Value Client Provisioning Portal (def: ~</li> <li>Static IP/Host name/FQDN</li> <li>Suppress Profiler CoA for endpoints in Logical Profile</li> </ul>

ISE\_Add\_New\_Authorization\_Profile\_Redirect\_1



**Remarque** : cette redirection de nom de liste de contrôle d'accès doit correspondre au nom de liste de contrôle d'accès correspondant configuré sur FTD.

Étape 21.2. Répétez l' Add pour créer deux autres profils d'autorisation pour les terminaux non conformes et conformes avec les détails.

Nom : non\_compliance\_profile

Nom DACL : DENY\_ALL\_IPv4\_TRAFFIC

Nom : compliance\_profile

Nom DACL : PERMIT\_ALL\_IPv4\_TRAFFIC



**Remarque** : la liste de contrôle d'accès pour les terminaux conformes ou non conformes doit être configurée en fonction des exigences réelles.

Étape 22. Accédez à Work Centers > Posture > Posture Policy. Cliquez sur Edit à la fin des règles. Sélectionnez Insert new policy.

						8-8		Г										~		_		_
Identity Services	Engine							L	Work Centers /	Pos	ture							Q	4	0	φ	L.
J Bookmarks	Overview	r Ne	twork Devices	Client Provisioning P	olicy Elements	Posture Poli	cy Policy S	Sets	Troubleshoot	R	teports Settings											
E Dashboard		_			L																	
10 Context Visibility		Post	ure Policy	Guide Me																		
% Operations		Define the	e Posture Policy by c	onfiguring rules based on operat	ting system and/or othe	conditions.													~			-
Policy		~																				
L_ Administration		Status	Policy Options	Rule Name	Identity Groups	Operat	ing Systems	(	Compliance Module		Posture Type		Other Conditions	Re	quirements	_	-					
			Policy Options	Default_AntiMalware_Policy_Ma c	If Any	and Mac 05	×	and 4	k.x. or later	and	Agent	and	then	e An	_AM_Installation_Ma	Edit v						
			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	ii Any	and Mac 05	×	and a	Lx or later	and	Temporal Agent	and	the	An 6_1	_AM_installation_Ma emporal	Edit	Duptcate Insert new policy					
③ Interactive Help			Policy Options	Default_AntiMalware_Policy_Win	ii Any	and Window	s All	ind 4	Lx or later	and	Agent	and	the	- An	AM_Installation_Wi	Edi	04419					
			Policy Options	Default_AntiMalware_Policy_Win_temporal	ii Any	and Window	s Al	and 4	La. or later	and	Temporal Agent	and	then	. An	, AM_Installation_Wi emporal	Edit						
			Policy Options	Default_AppVis_Policy_Mac	ii Any	and Mac OS	×	and 4	Lx or later	and	Agent	and	then	Def	ault_AppVis_Require rt_Mac	Edt -						
			Policy Options	Default_AppVis_Policy_Mac_temporal	II Any	and Mac OS	×	ind a	La or later	and	Temporal Agent	and	then	Def	ault_AppVis_Require nt_Mac_temporal	Edt y						
			Policy Options	Default_AppVis_Policy_Win	ii Any	and Window	a All	and 4	i.x.or later	and	Agent	and	then	Def	ault_AppVIs_Require nt_Win	Edit 9						
			Policy Options	Default_AppVIs_Policy_Win_te mporal	ii Any	and Window	s Al	ind 4	La or later	and	Temporal Agent	and	the	Def	ault_AppVis_Require nt_Win_temporal	Edit -						
			Policy Options	Default_Firewall_Policy_Mac	ii Any	and Mac OS	x	and 4	Lx or later	and	Agent	and	Det	Del me	ault_Firewall_Require rt_Mac	Edt y						
			Policy Options	Default_Firewall_Policy_Mac_te mporal	ii Any	and Mac OS	×	and 4	Lx or later	and	Temporal Agent	and	the	Def	ault_Firewall_Require nt_Mac_temporal	Edt -						
			Policy Options	Default_Firewall_Policy_Win	IF Any	and Window	s Al	and 4	i.x or later	and	Agent	and	then	Def	auit_Firewall_Require nt_Win	Edit 9						
			Pulicy Options	Default_Firewall_Policy_Win_te mporal	ir Any	and Window	s Alt	and 4	Lx or later	and	Temporal Agent	and	the	Def	ault_Firewall_Require nt_Win_temporal	Edt v						
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	II Any	and Med 05	×	and 4	Lx or later	and	Agent	and	the	Def ute	auit_Hardware_Attrib s_Requirement_Mac	Edt v						
			Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	ii Any	and Mac OS	x .	and 4	k.x. or later	and	Temporal Agent	and	then	Def ute	ault_Hardware_Attrib s_Requirement_Mac_ poral	Edit v						
			Policy Options	Default_Hardware_Attributes_P olicy_Win	II Any	and Window	s At	and 4	Lx or later	and	Agent	and	then	Def	ault_Hardware_Attrib s_Requirement_Win	Edt -						
		-	·····	-					- ii tali		*				and the second second							

Politique\_Nouvelle\_Posture\_Ajout\_ISE

Étape 22.1. Configurez les détails :

Nom de la règle : Demo\_test\_existing\_linux

Groupes d'identités : Tous

Systèmes d'exploitation : Linux All

Module de conformité : version 4.x ou ultérieure

Type de posture : Agent

Configuration requise : Test\_existing\_linux

Cliquez sur Done et Save.

Post	ture Policy	Guide Me	iting :	system and/o	r other con	ditions.							2	~
~														
	Policy Options	Default_Firewall_Policy_Mac	H.	Any	and	Mac OSX	an	4.x or later	and	Agent	and	the	<ul> <li>Default_Firewall_Require ment_Mac</li> </ul>	Edit 👻
	Policy Options	Default_Firewall_Policy_Mac_te mporal	1	Any	and	Mac OSX	an	4.x or later	and	Temporal Agent	and	the	n Default_Firewall_Require ment_Mac_temporal	Edit 🤟
	Policy Options	Default_Firewall_Policy_Win	H	Any	and	Windows All	an	4.x or later	and	Agent	and	the	n Default_Firewall_Require ment_Win	Edit ~
	Policy Options	Default_Firewall_Policy_Win_temporal	H	Any	and	Windows All	an	4.x or later	and	Temporal Agent	and	the	n Default_Firewall_Require ment_Win_temporal	Edit 🤟
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	H	Any	and	Mac OSX	an	4.x or later	and	Agent	and	the	n Default_Hardware_Attrib utes_Requirement_Mac	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	1	Any	and	Mac OSX	an	4.x or later	and	Temporal Agent	and	the	<ul> <li>Default_Hardware_Attrib utes_Requirement_Mac_ temporal</li> </ul>	Edit 🐱
	Policy Options	Default_Hardware_Attributes_P olicy_Win	H.	Any	and	Windows All	an	4.x or later	and	Agent	and	the	<ul> <li>Default_Hardware_Attrib utes_Requirement_Win</li> </ul>	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	18	Any	and	Windows All	ani	4.x or later	and	Temporal Agent	and	the	<ul> <li>Default_Hardware_Attrib utes_Requirement_Win_t emporal</li> </ul>	Edit 😔
	Policy Options	Default_US8_Block_Policy_Win	if.	Any	and	Windows All	ani	4.x or later	and	Agent	and	the	n USB_Block	Edit 😔
-	Policy Options	Default_USB_Block_Policy_Win	11	Any	and	Windows All	an	4.x or later	80	Temporal Agent	and	the	n USB_Block_temporal	Edit 🗸

ISE\_Add\_New\_Posture\_Policy\_1

#### Étape 23. Accédez à Work Centers > Posture > Policy Sets. Cliquez pour Insert new row above.

$\equiv \frac{-de-de}{casco}$ Identity Services	Engine	Work Centers / Posture	ର <b>ଜ</b> ତ ଜାନ
JI Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy	Sets Troubleshoot Reports Settings	
Dashboard     Id Context Visibility	Policy Sets		Reset Policyset Hitcounts Silve
% Operations	Status Policy Set Name Description Conditions		Allowed Protocols / Server Sequence Hits Actions View
Policy	Q. Search		
Administration	Default     Default     Default     policy set		Default Network Access 🖉 + 🔹 🔅 🗲
③ Interactive Help			Insert new row above
			Reset

ISE\_Add\_New\_Policy\_Set

Étape 23.1. Configurez les détails :

Nom du jeu de stratégies : Position du pare-feu

Conditions : ÉGAL à l'adresse IP du périphérique d'accès réseau [FTD IP Address]

Cliquez sur Save .

=	dentity Services	Engine							Work Centers /	Posture						Q,	\$ @	۵ ۵	1.8	L
н	Bookmarks	Overview	Networ	k Devices	Client Provisionin	ng Policy Elemen	nts Posture Policy	Policy Sets	Troubleshoot	Reports	Settings									
82 18	Dashboard Context Visibility	P	olicy Sets										Reset	Rese	t Policyset	Hitcour	6	Sav	•	
*	Operations		🕣 Status	Policy Set N	iame Desc	ription	Conditions						Allowed Prot	ocols / Serve	r Sequenc	e Hit	Actio	es Vi	ow	
-0	Policy		Q. Searc	h																
2.	Administration		•	Firewall Posts	re		Network Access Device	P Address EQUALS					Default Netw	ork Access	24		0		Γ.	
-1	Work Centers			Default	Defau	it policy set							Default Netw	ork Access	.0.4		0		,	
	Interactive Halo																			
																Res	•	Sav		

ISE\_Add\_New\_Policy\_Set\_1

Étape 23.2. Cliquez sur > pour entrer le jeu de stratégies. Créez de nouvelles règles d'autorisation pour l'état conforme à la position, non conforme et inconnu. Cliquez sur Save.

Conforme à compliance\_profile

Non conforme avec non\_compliance\_profile

#### Inconnu avec unknown\_redirect

≡ dualo	Identity	Servic	es Engine					Work Cen	ters / Postu	ıre					
JU 01	verview	Netwo	ork Devices C	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
== 15		0	Firewall Posture		🖳 Neti	work Access-Device IP Add	ress EQUALS :					De	fault Network Access		e + 0
*	~Auth	entication	Policy(1)												
0	۲	Status	Rule Name	Conditions								Use		Hits	Action
	0	Search													
								+							
?		0	Default									All_User_ID_S	tores 🦉	48	稔
												Options			-
	> Auth	orization	Policy - Local Except	tions											
	> Auth	orization	Policy - Global Excep	ptions											
	✓Auth	orization	Policy(4)												
										Results					
	۲	Status	Rule Name	Conditions						Profiles		Security Groups		Hits	Actions
	0	Search													
		٥	Compliant	E Session-P	ostureStatus EQUALS Co	mpliant				compliant_profile	1 +	Select from list	<i>•</i> +	15	礅
		۲	Non_Compliant	E Session P	ostureStatus EQUALS No	nCompliant				non_compliant_profile	<i></i> +	Select from list	/ +	5	٨
		0	Unknown	E Session-Pr	ostureStatus EQUALS Uni	known				unknown_redirect	0 +	Select from list	2 +	47	$\langle 0 \rangle$

ISE\_Add\_New\_Policy\_Set\_2

#### Configurations sur Ubuntu

Étape 24. Connectez-vous au client Ubuntu via l'interface utilisateur graphique. Ouvrez le navigateur pour vous connecter au portail VPN. Dans cet exemple, il s'agit de demo.example.com.

demo.ex	xam	nple.com/+CS	COEX	+			-	ē	×
$\leftarrow \rightarrow$	è	С	0 🗛	https://demo.example.com/	CSCOE+/logon.html#form_title_text	ដ	$\bigtriangledown$	$\mathbf{F}$	≡

Logon
Group posture_vpn v Username Password
Logon

Ubuntu\_Browser\_VPN\_Login

Étape 25. Cliquez sur Download for Linux.

Cisco	Secu	re Client Inst	allati	:	+															e	ē	×
$\leftarrow$	$\rightarrow$	C	0 &		https:	//dem	o.exa	mple	.com	n/CAC	CHE/	/stc/2	/inde	ex.htm	l	F	80%	ជ	•	$\bigtriangledown$	$\checkmark$	≡
		secure	re Client	t																		
		C		C	Cisc	0 5	Sec X	ure	e C	Clie	en	t D	)ov	vnlc	oad							A
								D	ow	nlo	ad	8	Inst	tall								
							Downlo	ad Cisc	co Sec	cure Cli Downl	lient a	and inst	all it on NUX	i your coi	mputer.							
																	🔁 Ins	structi	ons			

Ubuntu\_Browser\_VPN\_Download\_1

Le nom du fichier téléchargé est cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu\_Browser\_VPN\_Download\_2

Étape 26. Téléchargez le certificat VPN via le navigateur et renommez le fichier en <certificate>.crt. Voici l'exemple d'utilisation de firefox pour télécharger le certificat.

-	demo.examp	ole.com/+CSCOE×	+	$\sim$	E	ē	×
$\leftarrow$	$\rightarrow$ G	O 🔓 https://	/demo. <b>example.com</b> /+CSCOE+/logon.html#form_title_text	${igsidential}$	۲	பி	≡

Page Info — https://demo.example.com/+CS	COE+/logon.html	#form_title_text 😑 💷 🛛
General Media Permissions Security		
Website Identity         Website:       demo.example.com         Owner:       This website does not supply ownership in         Verified by:       C=CN,CN=demo.example.com	formation.	<u>V</u> iew Certificate
Privacy & History Have I visited this website prior to today?	No	
Is this website storing information on my computer?	Yes, cookies	<u>C</u> lear Cookies and Site Data
Have I saved any passwords for this website?	No	Vie <u>w</u> Saved Passwords
Technical Details Connection Encrypted (TLS_AES_128_GCM_SHA256, 12 The page you are viewing was encrypted before being t Encryption makes it difficult for unauthorized people to therefore unlikely that anyone read this page as it trave	8 bit keys, TLS 1.3) ransmitted over the view information t led across the netw	e Internet. raveling between computers. It i rork. Help

Ubuntu\_Browser\_VPN\_Cert\_Download

Étape 27. Ouvrez le terminal sur le client Ubuntu. Accédez à pourpath home/user/Downloads/ installer Cisco Secure Client.

#### <#root>

user@ubuntu22-desktop:~\$

cd Downloads/

```
user@ubuntu22-desktop:~/Downloads$
```

```
ls
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

demo-example-com.crt

```
user@ubuntu22-desktop:~/Downloads$
```

```
chmod +x cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

[sudo] password for user: Installing Cisco Secure Client... Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory Extracting installation files to /tmp/vpn.zaeAZd/vpninst959732303.tgz... Unarchiving installation files to /tmp/vpn.zaeAZd... Starting Cisco Secure Client Agent... Done! Exiting now. user@ubuntu22-desktop:~/Downloads\$

Étape 28. Faites confiance au certificat du portail VPN sur le client Ubuntu.

#### <#root>

user@ubuntu22-desktop:~\$

cd Downloads/

user@ubuntu22-desktop:~/Downloads\$

ls

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

demo-example-com.crt

user@ubuntu22-desktop:~/Downloads\$

openssl verify demo-example-com.crt

CN = demo.example.com, C = CN
error 18 at 0 depth lookup: self-signed certificate
Error demo-example-com.crt:

verification failed

user@ubuntu22-desktop:~/Downloads\$

sudo cp demo-example-com.crt /usr/local/share/ca-certificates/

user@ubuntu22-desktop:~/Downloads\$

sudo update-ca-certificates

Updating certificates in /etc/ssl/certs... rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL

#### 1 added

```
, O removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

user@ubuntu22-desktop:~/Downloads\$

openssl verify demo-example-com.crt

demo-example-com.crt: OK

Étape 29. Ouvrez Cisco Secure Client sur le client Ubuntu et connectez le VPN à demo.example.com avec succès.

		Cisco Secure	Client		•	×
AnyCon	nect VPN	ics	About			
		ıı ııı cısc	11 0			
Connect to:	demo.exa	ample.com			~	₽
Group:	posture_v	pn				~
Username:	isetest					
Password:	*****					



 $Ubuntu\_Secure\_Client\_Connected$ 

Étape 30. Ouvrez le navigateur pour accéder à tout site Web déclenchant la redirection vers le portail CPP ISE. Téléchargez le certificat à partir du portail CPP ISE et renommez le fichier <certificate>.crt. Voici un exemple d'utilisation de Firefox pour le téléchargement.



Ubuntu\_Browser\_CPP\_Cert\_Download

Étape 30.1. Faites confiance au certificat du portail CPP ISE sur le client Ubuntu.

#### <#root>

user@ubuntu22-desktop:~/Downloads\$ ls cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh demo-example-com.crt

ise-cert.crt

user@ubuntu22-desktop:~/Downloads\$

sudo cp ise-cert.crt /usr/local/share/ca-certificates/

user@ubuntu22-desktop:~/Downloads\$

```
sudo update-ca-certificates
```

Updating certificates in /etc/ssl/certs... rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL

1 added

```
, O removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

Étape 31. Cliquez Start sur le portail CPP ISE.

Device Security Check × +	-	ø	×				
← → C () A https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08 ☆		$\bigtriangledown$	≡				
Our must log in to this network before you can access the Internet.							
Client Provisioning Portal							
Device Security Check Your computer requires security software to be installed before you can connect to the network.							

Ubuntu\_Browser\_CPP\_Start

Étape 32. Click here to download and install Agent.

Device Security Che	k × +		- 0	×				
$\leftarrow \   \rightarrow \   G$	https://demoise.e	example.com :::8443/portal/ClientProvisionStart.action?from=CL 🏠	${igodot}$	≡				
You must log in to	his network before yo	ou can access the Internet.		$\times$				
cisco.		Client Provisioning Portal						
Device Security Check Your computer requires security software to be installed before you can connect to the network. Unable to detect Posture Agent								
•	+ This is my first time here							
<ol> <li>You must install Agent to check your device before accessing the network. <u>Click here to download and install Agent</u></li> <li>After installation, Agent will automatically scan your device before allowing you access to the network.</li> <li>You have 20 minutes to install and for the system scan to complete.</li> </ol>								
Note: With some browsers, when you click Download, the script is directly saved in the configured Downloads folder in your system. Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.								
You have 20 minutes to install and for the compliance check to complete								
θ		+ Remind me what to do next						

Ubuntu\_Browser\_CPP\_Download\_Posture

Étape 33. Ouvrez le terminal sur le client Ubuntu. Accédez au chemin home/user/Downloads/ d'installation du module de posture.

#### <#root>

user@ubuntu22-desktop:~/Downloads\$ ls

cisco-secure-client-ise-network-assistant-linux64-5.1.3.62\_demoise.example.com\_8443\_0NcLgcMURfyZmR6HoLmL

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt
ise-cert.crt
user@ubuntu22-desktop:~/Downloads$
chmod +x cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfy
user@ubuntu22-desktop:~/Downloads$
user@ubuntu22-desktop:~/Downloads$
user@ubuntu22-desktop:~/Downloads$
./cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6Hol
Cisco Network Setup Assistant
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
Cisco ISE Network Setup Assistant started. Version - 5.1.3.62
Trusted and Secure Connection
You are connected to
demoise.example.com
whose identity has been certified. Your connection to this website is encrypted.
Downloading Cisco Secure Client...
Downloading remote package...
Running Cisco Secure Client - Downloader...
Installation is completed.
```

Étape 34. Sur l'interface utilisateur du client Ubuntu, quittez le client sécurisé Cisco et rouvrez-le. Le module de posture ISE est installé et s'exécute correctement.



Ubuntu\_Secure\_Client\_ISE\_Posture\_Installed

Étape 35. Ouvrez le terminal sur le client Ubuntu. Accédez à path home/user/Desktop, créez un fichiertest.txt pour répondre à la condition de fichier configurée sur ISE.

#### <#root>

user@ubuntu22-desktop:~\$

#### cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

#### Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Connectez le VPN à demo.example.com sur le client Ubuntu.



Seconnect 2010					
Connected to demo.example.com.					

Vérifier\_Ubuntu\_Secure\_Client\_Connected

Étape 2. Vérifiez l'état de la position ISE sur le client Ubuntu.



Vérifier\_Ubuntu\_Secure\_Client\_Compliant

#### Étape 3. Cochez Radius Live Log sur ISE. Accédez à Operations > RADIUS Live Log.

≡	dentity Services Engine		Oper	ations / RADIUS	Q & @ Q   A			
н	Live Logs Live Sessions							
14	Misconfigured Supplicants 🕕 Misconfig		igured Network Devices 🕕 RADIUS De		RADIUS Drops		Client Stopped Responding 🕕	Repeat Counter ①
*	0		0		0		0	0
U							Refresh Show	Within
80							Never v Latest 20 rec	cords 🗸 Last 24 hours 🗸
di.	ට් 🖆 Reset Repeat Counts ර	🗅 Export To 🗸						Filter 🗸 🛞
	Time	Status Details	Identity E	ndpoint ID	Endpoint Profile	Posture Status	Authentication Policy Au	uthorization Policy
?			Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy A	uthorization Policy
	May 29, 2024 09:08:48.798 PM	٥	isetest 52	2:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default Fire	rewall Posture >> Compliant
	May 29, 2024 09:08:48.798 PM		5:	2:54:00:17:6B:FA		Compliant	Firewall Posture Fir	rewall Posture >> Compliant
	May 29, 2024 09:08:13.570 PM	a a	isetest 52	2:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default Fir	rewall Posture >> Unknown

Vérifier\_ISE\_LiveLog

Étape 4. Accédez à FTD CLI via SSH ou la console.

#### <#root>

>

>

```
system support diagnostic-cli
```

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available commands.

ftdv741>

enable

Password: ftdv741# ftdv741#

show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
```

```
Username : isetest Index : 33
Assigned IP : 192.168.6.30 Public IP : 192.168.10.13
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 51596 Bytes Rx : 17606
Pkts Tx : 107 Pkts Rx : 136
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : posture_gp Tunnel Group : posture_vpn
Login Time : 14:02:25 UTC Fri May 31 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb007182000210006659d871
Security Grp : none Tunnel Zone : 0
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 33.1
Public IP : 192.168.10.13
Encryption : none Hashing : none
TCP Src Port : 59180 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : linux-64
Client OS Ver: Ubuntu 22.04 LTS 22.04 (Jammy Jellyfish)
```

Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 6364 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 33.2 Assigned IP :192.168.6.30 Public IP : 192.168.10.13 Encryption : AES-GCM-128 Hashing : SHA256 Ciphersuite : TLS\_AES\_128\_GCM\_SHA256 Encapsulation: TLSv1.3 TCP Src Port : 59182 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Linux\_64 Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 6364 Bytes Rx : 498 Pkts Tx : 1 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3 DTLS-Tunnel: Tunnel ID : 33.3 Assigned IP :192.168.6.30 Public IP : 192.168.10.13 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 56078 UDP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Linux\_64 Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62 Bytes Tx : 38868 Bytes Rx : 17108 Pkts Tx : 105 Pkts Rx : 130 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

#### Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour le flux de posture et le dépannage de Cisco Secure Client et ISE, consultez les <u>documents</u> CCO<u>Comparaison des styles de posture ISE</u> pour les versions antérieures et postérieures à 2.2 et <u>Dépannage de la gestion et de la posture des sessions ISE</u>.

Informations connexes

<u>Compatibilité des composants réseau de Cisco Identity Services Engine, version 3.3</u>

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.3
- <u>Assistance technique de Cisco et téléchargements</u>

### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.