Configuración de la condición de VPN de Linux con ISE 3.3

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Diagrama de la red
Configuraciones en FMC/FTD
Configuraciones en ISE
Configuraciones en Ubuntu
Verificación
Troubleshoot
Información Relacionada

Introducción

Este documento describe cómo configurar el estado de la VPN Linux con Identity Services Engine (ISE) y Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cliente seguro de Cisco
- VPN de acceso remoto en Firepower Threat Defence (FTD)
- Identity Services Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- 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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Topología

Configuraciones en FMC/FTD

Paso 1. La conectividad entre el cliente, FTD, FMC e ISE se ha configurado correctamente. Como enroll.cisco.com se utiliza para los terminales que hacen sondeos para redirección (consulte los <u>documentos de</u> CCO sobre el flujo de postura <u>Comparación del estilo de postura ISE para</u> <u>versiones anteriores y posteriores a la 2.2</u> para obtener más información). Asegúrese de que la ruta para el tráfico a enroll.cisco.com en FTD esté configurada correctamente.

Paso 2. Descargue el nombre del paquete cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg de <u>Descarga de Software</u> <u>de Cisco</u> y asegúrese de que el archivo sea bueno después de la descarga confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página de Descarga de Software de Cisco.

Paso 3. Desplácese hasta Objects > Object Management > VPN > Secure Client File. Haga clic en Add Secure Client File, proporcione el nombre, navegue File Name para seleccionar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, seleccione Secure Client Image en la lista desplegableFile Type. A continuación, haga clic en 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

FMC_Upload_Secure_Client_Image

Paso 4. Desplácese hasta Objects > Object Management > Network.

Paso 4.1. Cree un objeto para el servidor DNS. Haga clic en Add Object, indique el nombre y la dirección IP de DNS disponible. Haga clic en Save.

Firewall Managemen Objects / Object Managemen	nt Center Overview Analysis Poli	cies Devices Objects Integration		Deploy	् 💕 🔅 🎯 ədmir	1 - Cisco SECURE
Distinguished Name DNS Server Group External Attributes File List Geolocation Interface Key Chain Network	Network A network object represents one or more IP addre	isses. Network objects are used in various places, including acc	cess control policies, network variables, intrusion rule	Add Network Add Control Add Co	Q, Filter Object Show Unused orts, and so on. Group	J Objects
	Name			Value	Type Override	
	any	New Network Object	0	0.0.0.0/0 ::/0	Group	¶a q ⊕ #
	any-ipv4			0.0.0.0/0	Network	¶a q ⊕ #
		Description Network Host Range Network Allow Overrides	k O FQDN			
			Cancel			

FMC_Add_Object_DNS



Nota: El servidor DNS configurado aquí se debe utilizar para los usuarios de VPN.

Paso 4.2. Cree un objeto para ISE PSN. Haga clic en Add Object, introduzca el nombre y la dirección IP PSN de ISE disponible. Haga clic en Save.

Firewall Management	t Center Overview Analysis Polic	ies Devices Objects Integration		Deploy	९ 💕 🌣 😰 🛛 admin	osce SECURE
Distinguished Name DNS Server Group External Attributes	Network			Add Network Add Ob	Q. Filter	Objects
File List > FlexConfig	A network object represents one or more IP addre	sses. Network objects are used in various places, including acce	ss control policies, network variables, intrusi	on rules, identity rules, network discovery rule Add Gn	Object orts, and so on. oup	
Geolocation	Name	New Network Object	0	Value	Type Override	
Interface	any	New Network Object		0.0.0.0/0 ::/0	Group	¶a. ≣ &
Key Chain	any-ipv4	News		0.0.0.0/0	Network	¶g Q ⊕ 85
		Name	1			
		Description				
		Network				
		Host Range Network	O FQDN			
]			
		Allow Overrides	-			
			Cancel Save			

$FMC_Add_Object_ISE$

Paso 5. Desplácese hasta Objects > Object Management > VPN > Group Policy. Haga clic en Add Group Policy. Haga clic en DNS/WINS, seleccione el objeto del servidor DNS en Primary DNS Server. A continuación, haga clic en Save.

Firewall Management	t Center Overview Analysis Policies I	Devices Objects In	tegration	Deploy Q 🚱 🌣 🕢 admin ~ debis SECURE
Distinguished Name DNS Server Group	Group Policy			Add Group Policy Q, Filter
External Attributes File List Devicements	A Group Policy is a set of attribute and value pairs, stored in	a group policy object, that de	afine the remote access VPN experience. The RADIUS authorization server assigns	the group policy or it is obtained from the current connection profile.
Geolocation	Namo			
Interface	DftGrpPolicy	Add Group Policy	0	/i
Network > PKU Policy List Port > Prefix List Route Map > Security Intelligence SLA Monitor Time Range SLA Monitor Time Zone URL Variable Set VLAN Tag Certificate Map		Name:" posture_gp Description: General Secure C VPN Protocols IP Address Pools Banner DNS/WWS Split Tunneling	Illent Advanced Primary DNS Server: DNS	
Cuatom Attribute Group Policy KKVI Policy KKV2 Policy KKV2 Policy Secure Client Cuatomizatio Secure Client File			Only network object with low4 address is allowed (Dr: 10.72.3.5) Default Domain: Cancel Sove	Displaying 1 - 2 of 2 rows $ I \leq Page$ 1 of 1 > $ I $

FMC_Add_Group_Policy



Nota: asegúrese de que el servidor DNS utilizado en la política de grupo VPN puede resolver el FQDN y enroll.cisco.com del portal de aprovisionamiento de clientes de ISE.

Paso 6. Desplácese hasta Objects > Object Management > Access List > Extended. Haga clic en Add Extended Access List.

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧐 🌣 🕢 admin 🗸 🔥 SECURE
 AAA Server RADIUS Server Group Signala Since on Second 	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 only, Identifies traffic based	Add Extended Access List Q, Filter
Access List Extended	addresses. You use these objects when configuring particular features, such as route maps. Name Value	Override

FMC_Add_Redirect_ACL

Paso 6.1. Proporcione el nombre de la ACL de redirección. Este nombre debe ser el mismo que en el perfil de autorización de ISE. Haga clic en

Add.

New Extended Access List Object

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

FMC_Add_Redirect_ACL_Part_1

Paso 6.2. Bloquee el tráfico DNS, el tráfico a la dirección IP PSN de ISE y los servidores de corrección para excluirlos de la redirección. Permitir el resto del tráfico. Esto activa la redirección. Haga clic en Save.

Add Extended Access List Entry

Action: Block		
Logging: Default		
Log Level: Informational		
Log Interval: 300 Sec. Network Port 3 Application 3 Users 3 Security	y Group Tag	
Available Networks C Q. Search by name or value IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast ISE_PSN_	rce tination	Destination Networks (1) ISE_PSN
rtp_ise	Enter an IP address	Add Enter an IP address Add

FMC_Add_Redirect_ACL_Part_2

Cancel Save

Cancel

0

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

 $FMC_Add_Redirect_ACL_Part_3$



Paso 7. Desplácese hasta Objects > Object Management > RADIUS Server Group. Haga clic en Add RADIUS Server Group.

Firewall Management Objects / Object Management	Center Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	60
 AAA Server RADIUS Server Group Single Sign-on Server Access List 	RADIUS Server	Group	or more refere	nces to RADI	JS Servers. Ti	nese AAA servers are used to authenticate users logging in through Remote Access VPN conn	actions.	Add RADIUS Ser	rver Gro	up
Extended	Name						Value			

FMC_Add_New_Radius_Server_Group

Paso 7.1. Proporcione el nombre, la comprobación Enable authorize only, la comprobación Enable interim account update, la comprobación 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
	Cancel

 $FMC_Add_New_Radius_Server_Group_Part_1$

Paso 7.2. Haga clic en el Plus icono para agregar un nuevo servidor RADIUS. Proporcione el ISE PSN IP Address/Hostname, Key. Seleccione el specific interface para conectarse. Seleccione el Redirect ACL. A continuación, haga clic Savepara guardar el nuevo servidor RADIUS. A continuación, haga clic Save de nuevo para guardar el nuevo grupo de servidores RADIUS.

?

Add RADIUS Server Group	0	New RADIUS Server	0
 Enable authorize only Enable interim account update Interval:* (1-120) hours 24 Enable dynamic authorization Port:* (1024-65535) 1700 Merge Downloadable ACL with Cisco AV Pair ACL After Cisco AV Pair ACL After Cisco AV Pair ACL RADIUS Servers (Maximum 16 servers) 		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) 1813 Timeout: (1-300) Seconds 10	
IP Address/Hostname No records to display.		Connect using: Routing Specific Interface + inside_zone + Redirect ACL: redirect +	
Cance	el Save	Cancel	Save

FMC_Add_New_Radius_Server_Group_Part_2

Paso 8. Desplácese hasta Objects > Object Management > Address Pools > IPv4 Pools. Haga clic en Add IPv4 Pools y proporcione el **Name**, **IPv4 Address Range**y Mask. A continuación, haga clic en Save.

Firewall Manage Objects / Object Manage	ment Center Overview Analysis Policies D	evices Objects Integration		Deploy Q 💕 🌣 😰 fi	ingni v dudi SECURE
> AAA Server > Access List > Address Pools IPv4 Pools	IPv4 Pools	ement/diagnostic interface with clustering, or for VPN remote access profiles.		Add IPv4 Pools Q, Filter	
BY4 Pools FV4 Pools Application Filters AS Path BFD Template Cipher Suits List Community List Distinguished Name DNS Server Group Distinguished Name DNS Server Group External Attributes File List Flex List Poil Poid Sinkhole	Hame al postara_pool_97_0	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* 255.255.255.0 INIOn Overrides Configure device overrides in the address pool object to avoid VP address conflicts in case of object to shared across multiple devices Yourdide (0)		0 vr 0 1 1 1 1 1 1 1 1 1 1 1 1 1	ride
SLA Monitor Time Range Time Zone Tunnel Zone URL Variable Set			Cancel Save	Displaying 1 - 2 of 2 rows < < 1	Page 1 of 1 > >1 C

FMC_Add_New_Pool

Paso 9. Desplácese hasta Certificate Objects > Object Management > PKI > Cert Enrollment. Haga clic en Add Cert Enrollment, proporcione un nombre y seleccione Self Signed Certificateen Enrollment Type. Haga clic en la Certificate Parameters ficha y proporcione Common Name y Country Code. A continuación, haga clic en Save.

Firewall Management Objects / Object Management	t Center Overview Analysis Policies Devices	s Objects Integration		Deploy Q 🚱 🌣 🕢 fangni - 🖓 distribution SECURE
AAA Server Access List Address Pools Application Filters	Cert Enrollment A certificate enrollment object contains the Certification Authority (your Private Key Infrastructure (PKI).	CA) server information and enrollment parameter	ts that are required for creating Certificate Signing Requests (CSRs) and obtaining	Add Cert Enrollment Q. Filter
AS Path BFD Template Cipher Suite List	Name Add Cert Enrollment	ø	Add Cert Enrollment	Type Override
Community List DHCP IPv6 Pool DHCP IPv6 Pool DHS Server Group DHS Server Group File List File List File List File Config Geolocation Internal Cont External Cont Groups External Cont Internal Cost I	Name* demo_vph Description CA Information Certificate Parameters Key Revocation Enrollment Types: Salt Slowed Certificate Image: Common Name (CN) is mandatory for self-signed certificate the VPN. To configure CN, please navigate to 'Certificate Parameters Validation Usage: Image: Please Client I SSL Client _ SSL	tion at is used in Remote Access rs' tab. Server	Name* demo, vpn Description CA Information Certificate Parameters Key Revocation Include FQON: Don't use FQON in certificate Include FQON: Common Name (DN): demo.example.com Organization Unit (OU): Locality (L): State (ST): Country Code (C): CN Emar(10: Include Device's Serial Number	
Policy List	Allow Overrides		Allow Overrides	
Port > Prefix List Route Map		Cancel Save		Cancel Save Displaying 1 - 3 of 3 rows I << Page 1 of 1 >> I C

FMC_Add_New_Cert_Enroll

Paso 10. Desplácese hasta Devices > Certificates. Haga clic en Add, seleccione el nombre de FTD en Device, seleccione la inscripción configurada anterior en Cert Enrollment. Haga clic en Add.

Firewall Manage Devices / Certificates	ment Center	Overview Analysis	s Policies Devices	Objects Integration		Deploy Q	🚱 🔄 👩 🕴 fangni 🗸 👘 🕯 SECURI
Filter All Certificates	•						Add
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status		
Add New Ce	rtificate			0			<u> </u>
					O CA (LD)		± ₽ C ∎
Add a new certif	cate to the dev	vice using cert enr	ollment object which	is used to	G.CA (LD)		± 2 C T
generate CA and	identify certifi	cate.	onnent object which	13 4364 10			
Device*:					(O CA (, ID)		± 2 C T
Posture-FTD-0	CML 27	•					
Cert Enrollment*							
demo_vpn		• +					
Cert Enrollment I	Details:						
Name:	demo v	na					
Enrollment Type:	Self-Sig	ned					
Enrollment URL:	N/A						
			Cancel	Add			

FMC_Add_New_Cert_To_FTD

Paso 11. Desplácese hasta Devices > VPN > Remote Access. Haga clic en Add.

Paso 11.1. Proporcione el nombre y añada el FTD a Selected Devices. Haga clic en Next.

Firewall Management Center Overview Devices / VPN / Secup Wizard	Analysis Policies Devices Objects Integration		Deploy Q 💞 🌣 🔕 admin 🗸 🕬 SECURE
Firewall Management Center Devices / VPW / Serue Waxed Connection Profile Policy Assignment O Connection Profile	Analysis Decices Objects Megradion • Decice Client • Access & Certificate • Summary	Celefore You Start Mediate Start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy, Authentication Server Configure LOCAL or Readin or RADULS 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 witard. Device Interface 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.	Deploy Q <table-cell></table-cell>
			Cancel Back Next

FMC_New_RAVPN_Wizard_1

Paso 11.2. Seleccione el grupo de servidores RADIUS configurado anteriormente en la Authentication Server, Authorization Server, Accounting Server. Desplácese hacia abajo en la página.

Einewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🗳 🌣 🕢 admin V 🖽 SEC
Remote Access VPN Policy Wizard	
1 Policy Assignment (2) Connection Profile 3 Secure Client 4 Access & Certificate (5) Summary	
Remote User Secure Client Cutation Vision Corporate Nerve Resources	
Consector Brofile:	
Connection Profiles specify the turnel group policies for a VPN connection. These policies pertain to creating the turnel testef, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies. Connection Profile Name:* posture_vpn	
Authentication, Authentication & Accounting (AAA): Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN	
connections.	
Authentication Server*	
Authorization Server: (toke •) +	
Accounting Server:	
Client Address Assignment:	
	Canada Back Mara

$FMC_New_RAVPN_Wizard_2$

Paso 11.3. Seleccione el nombre de conjunto configurado anteriormente en IPv4 Address Pools. Seleccione la política de grupo configurada anteriormente en Group Policy. Haga clic en Next.

Firewall Management Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 🚱 🌣 🚱 admin 🗸 🕬 SECURE
Remote Access VPN Policy Wizard Output Output	Access & Certificate (5) Summary	
	(Recounting Server: (RADUS) + (RADUS)	
	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 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	
	Group Policy:* posture_ap +	
	Edit Group Policy	



 $FMC_New_RAVPN_Wizard_3$

Paso 11.4. Marque la casilla de la imagen de Linux. Haga clic en Next.

Firewall Management Center Overview Analysis Devices / VPN / Setup Wizard	olicies Devices Objects Integration		Deploy Q, 🚱 🌣 🕢 admin ~ 🔤
Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Profile 3 Secure Cl	t 6 Access & Certificate 5 Summary		
	Secure Client Image The VPN gateway can automatically download the latest Secure Client The VPN gateway can automatically download the latest Secure Client	stide VIN balde Corporate Device Resources	
	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	-webdeplo Windows *	
	Inux_5_1_3_62 cisco-secure-client-linux64-5.1.2	i.62-webd Linux *	

Cancel Back Next

 $FMC_New_RAVPN_Wizard_4$

Paso 11.5. Seleccione la interfaz de la interfaz VPN. Seleccione la inscripción de certificados que se inscribió en el FTD en el paso 9. Haga clic en Next.



Cancel Back Next

FMC_New_RAVPN_Wizard_5

Paso 11.6. Confirme la información relacionada en la página de resumen. Si todo está bien, haga clic en Finish. Si necesita modificar algo, haga clic en Back.





Paso 12. Implemente la nueva configuración en FTD para completar la configuración de VPN de acceso remoto.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy	🚱 🕸 🕲 admin 🗸 🐝 SEC	CURE
posture_vpn			Q. Advanced Deploy	. Ignore warnings Deploy Car	ancel
			Posture-FTD-CML27	Ready for Deployment	<u>(s.(1)</u>
Connection Profile Access Interfaces Advanced				ty: ne	None
					+
Name	AAA	Group Policy			
DefaultWEBVPNGroup	Authentication: None Authonization: None Accounting: None	DfttGrpPolicy			
posture_vpn	Authentication: rtpise (RADIUS) Authonization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	posture_gp	1 selected 0 1 pending	₽ 0	

FMC_Deploy_FTD

Configuraciones en ISE

Paso 13. Desplácese hasta Work Centers > Posture > Network Devices. Haga clic en Add.

=	diale Identity Services	Engine					Work Centers	Posture				Q	۵	0	Q	۹
н	Bookmarks	Overview	Network Devi	ces	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
-	Dashboard															
ь	Context Visibility	Net	work Dev	rices												
×	Operations											s	elected 0	Total 4	Ø	٥
0	Policy	Ø Edit	+ Add D D	uplicate	🗄 Import 🖞 Export 🕚	Generate PAC	Delete 🗸							1	All V	V
8.	Administration		Name \land IF	/Mask	Profile Name	Location	Type		Description							
1.	Work Centers	0	FTD-CML2		. 🟥 Cisco 🕕	All Locations	Firewall									
	Work Centers	0	FTD-CML2	line and a	. 🟥 Cisco 🕕	All Locations	Firewall									
		0	FTD-CML2		🗯 Cisco 🕕	All Locations	Firewall									
3	Interactive Help		8.000		🗯 Cisco 🕕	All Locations	Firewall									

ISE_Add_New_Devices

Paso 13.1. Proporcione el Name, IP Addressy desplácese hacia abajo por la página.

≡ du	dentity Service	es Engine				w	ork Centers / I	Posture		
н	Overview Netwo	ork Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Ⅲ 回 火 ●	Network Devices Lis Network Devic Name Description	> New Network D es posture-FTD	evice	_						
20 Al	IP Addres	s 🗸 * IP :	/ 32	2	¢					
?	Device Profile	👬 Cisco	~	0						
	Model Name		、 、	/						
	Software Versio	n	``````````````````````````````````````	·						
	Network Device	Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Device	8	~	Set To Default					

ISE_Add_New_Devices_1

Paso 13.2. Marque la casilla de verificación de RADIUS Authentication Settings. Proporcione el Shared Secret. Haga clic en Submit.

Restaurura Overview Network Berking Delicy Elements Pesture Policy Noticy Settings Protocol RADUUS Authentication Settings Protocol RADUS Work Center Second Baned Batteractive Help RADUS OTLS Settings Other Settings Protocol Batteractive Help RADUS OTLS Settings Other Settings Protocol Batteractive Help RADUS OTLS Settings Other Settings Batteractive Help RADUS OTLS Settings Cok Port 100 Batteractive Help RADUS OTLS Settings Cok Port 100 Set To Delevit Batteractive Help RADUS OTLS Settings Cok Port 100 Batteractive Help	
E Dashbased Context Visibility RADIUS UDP Settings Poticy Administration Work Centers Work Centers Stard Section Second Shand Ock Peril 1200 Set So Delawit Second Shand CoA Peril 2083 Set So Delawit Rubuse CoA Peril 2083 Set So Delawit Second Shand Second Shand Second Shand Second Shand Second Shand Second Shand CoA Peril 2083 Set So Delawit Kay Explore Kay Explore Kay Explore Second Shand Second Shand CoA Peril 2083 Set So Delawit Second Shand CoA Peril 2083 Set So Delawit Kay Explore Kay Explore Kay Explore <p< th=""><th>Posture Policy Policy Sets Troubleshoot Reports Settings</th></p<>	Posture Policy Policy Sets Troubleshoot Reports Settings
Protections Protections Protections Protections Administration Image Secret Image Secret	
Och Pori 1300 Set 10 Default RADIUS DTLS Settings • OTLS Required • Shared Secret required (optional) • Och Port 2083 Set 10 Default Univer CA of ISE • • Oth S Name • • Orienticalities for Cock Setect if required (optional) • Oth S Name • • Otherer Division Show Kay Encryption Key Show Show Kay biologistic Coles Show • Vision Forcestic • HEADERCEMAL. • Atcharctication Settings • • > TACACCS Authentication Settings •	Show
 Steam securitys Advanced TrustSec Settings 	

ISE_Add_New_Devices_2

Paso 14. Descargue el nombre del paquete cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg de Descarga de Software de Cisco y asegúrese de que el archivo sea bueno confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página

de Descarga de Software de Cisco. El nombre del paquete cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg se ha descargado correctamente en el paso 1.

Paso 15. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent resources from local disk.

≡	diale Identity Services Engine			Wo	rk Centers /	Posture			
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
11 12 火	Client Provisioning Policy Resources Client Provisioning Portal	Resources	🚺 Duplicate 🌒 De	leto				Selec	cted 0 Total 16 🕃 All \lor ∇
		Agent res	ources from Cisco site		Т	ype \checkmark	Version	Last Update	Description
-		Agent res	ources from local disk		v	VinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Prov
-file		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	SiscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure (
		CiscoSecur	ClientDesktopLinux 5.1	.3.062	c	SiscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure (
		CiscoSecur	ClientComplianceModu	leWindows 4.3.4015.819	2 0	SiscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
		CiscoSecur	ClientComplianceModu	leLinux 4.3.3139.0	c	SiscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure (
		CiscoAgent	essWindows 5.0.03061		c	SiscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAgent	essOSX 5.0.03061		c	SiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTempo	oralAgentWindows 5.0.0	3061	c	SiscoTemporalAgent	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

ISE_Upload_Resource

Paso 15.1. Seleccione Cisco Provided Package. Haga clic Choose File para cargar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Haga clic en Submit.

≡	dentity Services E	ngine		Work Centers / Posture	۹	۵	0	0 X
月 日 回 火	Bookmarks Dashboard Context Visibility Operations	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Loca Agent Resources Fr	I Disk 2 Agent Resources From Local Disk form Local Disk				
0 4.	Policy Administration Work Centers		Category	Cisco Provided Package				
•	Interactive Help		Submit	Agent Uploaded Resources Name Agent Uploaded Resources Description GiscoSecureClientDesktopLi CiscoSecureClientDe S.1.3.62 Cisco Secure Client for II Cancel				



Nota: Repita el paso 14 para cargar cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg.

Paso 16. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent Posture Profile.

≡ :	isto Identity S	ervices Engine				Work Cent	ers / Posture		
Щ	Overview	Network Devices	Client Prov	isioning Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Setti	ngs
-1-1 0-1-1	Client Provision Resources	ing Policy	Reso	urces					
×	Client Provision	ing Portai							Selected 0 Total 16 📿
0			C Edit	+ Add A 🗋 Duplicate 🍵 De	elete				All \vee ∇
				Agent resources from Cisco site	,	Version	Last Update	Description	
			0	Agent resources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii.	
्ताः				Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S	
				Agent Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu.	
?				Agent Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17		
				AMP Enabler Profile	ntProfile	Not Applic	2024/05/16 15:15:49		

ISE_Add_Agent_Posture_Profile

Paso 16.1. Proporcione el Name, Server name rules y mantenga el resto como predeterminado. Haga clic en Save.

Nombre: linux_agent_profile

Reglas de nombre de servidor: *.example.com

≡ :#	dentity	Services Engine			Wa	ork Centers / I	Posture			
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ ◎ ※ ● ▲。	Client Provis Resources Client Provis	ioning Policy Ioning Portal	ISE Posture Agent Profile Set Agent Posture Profil Name * linux_agent_profile Description:	e						
?			Agent Behavior Parameter Enable debug log		Value No V	D	escription nables the debug log	on the agent		

ISE_Add_Agent_Posture_Profile_1

≡ :¦	Identity Services	Engine		V	Vork Centers / F	Posture		
FI.	Overview Network	Devices Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
-15	Client Provisioning Policy Resources	Posture Protoco	I					
2	Client Provisioning Portal	Parameter	Value			Description		
0		PRA retransmission	time 120	secs		This is the age communication	nt retry period n failure	if there is a Passive Reassessment
80		Retransmission Dela	y 🕕 60	secs		Time (in secon	ds) to wait bef	ore retrying.
สีเ		Retransmission Limi	t 🕕 🛛 🛓			Number of retr	ies allowed for	a message.
?		Discovery host 🕕				Enter any IP ad detects and ree portal.	Idress or FQDN directs that http	i that is routed through a NAD. The NAD p traffic to the Client Provisioning
		Discovery Backup S	erver List Choose			By default, Any 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 *	·.exampl	e.com		A list of wildca servers that the	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	resses, that de will try to conn n't respond for	fines the all the Policy service nodes ect to if the PSN that authenticated the some reason.
		Back-off Timer ①	30	secs		Agent will cont targets and pre packets till this	tinuously try to aviously connect max time limit	reach discovery targets (redirection cted PSNs) by sending the discovery t is reached
								Cancel

ISE_Add_Agent_Posture_Profile_2

Paso 17. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent Configuration.

≡ ::	see Identity	Services Engine				Work Cent	ers / Posture			
Щ	Overview	Network Devices	Client Prov	Policy Elements	Posture Policy	/ Policy	Sets Troublesho	ot Reports S	Settings	
10 10	Client Provis Resources	ioning Policy	Reso	urces						
×	Client Provis	ioning Portal							Selected 0	Fotal 16 📿
			🖉 Edit 🐳	+ Add 🔨 🗋 Duplicate 🛛 📋 C	Delete					$\forall V = \nabla V$
Ψ				Agent resources from Circo site		Version	Last Update	Description		
80				Agent resources from local disk	oSecureClientDe	51362	2024/05/08 10:31:28	Cisco Secure Client	for li	1
តា				Agent resources from local disk	obecureonentoe	0.1.0.02	2024/03/00 10.51.20			
			0	Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Nativ	/e S	
				Agent Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client	Linu	
?				Agent Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			- 1
				AMP Enabler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

ISE_Add_Agent_Configuration

Paso 17.2. Configure los detalles:

Seleccionar paquete de agente: CiscoSecureClientDesktopLinux 5.1.3.062

Nombre: linux_agent_config

Módulo de cumplimiento: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Marque la casilla de verificación de VPN, Diagnostic and Reporting Tool

Posición de ISE para la selección de perfiles: linux_agent_profile

Haga clic en Submit.

=	cisco	dentity	Services Engine					Work Cent	ers / Postu	re
Щ	c	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
55		Client Provisi	ioning Policy					1		
14		Resources		* Select Agent Package:	Cit	scoSecureClientDesktopLir	ux 5.1.3.062 V	J		
х		Client Provisi	ioning Portal	* Configuration Name:						
U				linux_agent_config						
80				Description:						
alı.					le					
(?)				Description Value N	otes					
				* Compliance Module	reClientComplianceModulel	Linux 4.3. ~				
				Cisco Secure Client	Module Selection					
				ISE Posture						
				Secure Firewall						
				Network Visibility						
				Diagnostic and Reporting 🗹 Tool						
				Profile Selection						
				* ISE Posture linux_ager	nt_profile	~			Su	ibmit Cance

ISE_Add_Agent_Configuration_1

Paso 18. Desplácese hasta Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Haga clic Edit al final de cualquier nombre de regla. Seleccione Insert new policy below.

≡ ::	isco Identity	Services E	ingine									w	ork Ce	enters / Postur	e				
щ	Overview	Network I	Devices	Clie	nt Provis	sioning	Policy Elemen	nts	Posture Polic	V	Policy Sets	Troubl	eshoo	t Reports	Settings				
11日 1日 火 日 品。	Client Provis Resources Client Provis	ioning Policy		CI Defir For A For N Wind Intel For M Mac If you with	ient f Agent Coni Vative Sup Jows Agen architectu Windows A ARM64 pr u configur out an ARI	Provision figuration: v plicant Con Mt, Mac Agei rres. Mac po Agent ARM6 policies requi e an ARM64	ioning Policy to deter ersion of agent, ar figuration: wizard p nt, Mac Temporal a blicles run the sam 4 policies, configu e no Other Condi c client provisionin n. This is because	min gent profi and e pa re S tion: g pc e an	e what users will recu profile, agent compl le and/or wizard. Dra Mac Agentless polici bession: OS-Architect a arm64 configuratior licy for an OS, ensur endpoint is matched	eive u g and g and secture cure E0 is, e that seque	pon login and use module, and/or ay drop rules to cha oport ARM64. Win es. QUALS arm64 in t the ARM64 policy entially with the policy	r session i gent custo nge the or dows polit he Other O r is at the i plicies liste	initiation mization rder. cies run Conditio top of ti ed in thi	n n package. separate packages ins column. he conditions list, at s window.	for ARM4 and read of policies				
				\sim															
?						Rule Name	,		Identity Groups		Operating Syst	ems		Other Conditions			Result	ts	
						IOS		H	Any	and	Apple IOS All		and	Condition(s)		then	Cisco-I	ISE-NSP	Edit 😔
				8		Android		If	Any	and	Android		and	Condition(s)		then	Cisco-	ISE-NSP	Edit
																	(Duplicate above Duplicate below Insert new policy at Insert new policy be	slow

Paso 18.1. Configure los detalles:

Nombre de regla: Linux

Sistemas operativos: Linux All

Resultados: linux_agent_config

Haga clic en Done y Save.

=	dentity	/ Services Engine						Work (Centers / Postu	ıre				
Щ	Overview	Network Devices	Client Provisionin	g Policy Elements	Posture Polic	y	Policy Sets	Troublesho	ot Reports	Settings				
田 13 火 10 14 14 14	Client Prov Resources Client Prov	isioning Policy	Client Pro Define the Client Pro For Agent Configurat For Native Supplican Windows Agent, Mac Intel architectures. M For Windows Agent / Mac ARM64 policies If you configure an A without an ARM64 co	visioning Policy to determine ion: version of agent, agen Configuration: wizard prov Agent, Mac Temporal and Iac policies run the same p RRM64 policies, configure 5 require no Other Condition RRM64 elient provisioning p andition. This is because an	icy what users will rec t profile, agent comp le and/or wizard. Dri Mac Agentless pota ackage for both archi Session: OS-Architec s arm64 configuratio loty for an 05, ensu endpoint is matched	ceive u liance ag and ies sup itecture cture E ns. re that d sequi	pon login and use module, and/or a drop rules to cha oport ARM64. Win es. QUALS arm64 in t the ARM64 polic; entially with the p	r session initiati gent customizati nge the order. dows policies ru he Other Condit r is at the top of olicies listed in t	on: on package. In separate package ions column. the conditions list, a his window.	is for ARM4 and ahead of policies				
?			Rule III I IOS III I Andro III I Linux	Name if id if if	Identity Groups Any Any Any	and and and	Operating Syst Apple IOS All Android Linux All	ems and and	Other Conditions Condition(s) Condition(s) Condition(s)	5	then then then	Results Cisco-ISE-NSP Cisco-ISE-NSP linux_agent_config]	Edit V Edit V Edit 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	
三 同 火 町	Conditions V Anti-Malvaire Anti-Spyware Anti-Virus Application	C View 2 Edit + Add D Duplicater C Evident	Selected 0 Total 385 🖉 🔕
8.	Compound	Name Description File name Condition Type	
	Dictionary Compound	pc_XP64_K82797002_MS13 Cisco Predefined Check: SYSTEM_PROGRAMSIC Cisco-Defined	0
mil	Dictionary Simple	pc_W8_64_xB3124275_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	External DataSource	pc_Vista_K82893294_M313 Clsco Predefined Check: SYSTEM_32\/magehlp.dll Cisco-Defined	
?	File	pc_W81_64_K83033889_M Clsco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Firewall	pc_Vista64_K8925902_MS0 Cisco Predefined Check: SYSTEM_ROOT\winaxs\a Cisco-Defined	
	Hardware Attributes	pc_W10_64_1709_KB45803 Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Registry	pc_XP_K82653956_MS12-0 Clsco Predefined Check: SYSTEM_32\Wintrust.dll Clsco-Defined	
	Script	pc_W8_K82892074_MS13 Cisco Predefined Check: SYSTEM_32\Scrun.dll Cisco-Defined	
	Service	pc_W10_64_1909_K850139 Cisco Predefined Check: SYSTEM_ROOT\SysWO Cisco-Defined	
	USB	pc_W7_K02681578_MS12 Clsco Predefined Check: SYSTEM_32(Win32k.sys Clsco-Defined	
	Remediations >	pc_W10_KB3081436_M515 Clsco Predefined Check: SYSTEM_32\Edgehtml.dll Clsco-Defined	
	Requirements	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_K82992611_MS Clsco Predefined Check: SYSTEM_ROOT\sysnativ Clsco-Defined	
	Downloadable ACLs	pc_W7_K83078601_MS15 Cisco Predefined Check: SYSTEM_32\Win32k.sys Cisco-Defined	

Paso 19. Desplácese hasta Work Centers > Posture > Policy Elements > Conditions > File. Haga clic en Add.

Paso 19.1. Configure los detalles:

Nombre: linux_demo_file_exist

ISE_Add_New_File_Condition

Sistemas operativos: Linux All

Tipo de archivo: FileExistence

Ruta del archivo: inicio, Desktop/test.txt

Operador de archivos: existe

Haga clic en Submit.

≡	dentity Services Engine					Work Cen	ters / Post	ture		
н	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
11日 1日 火 1日 1日 1日 1日 1日 1日 1日 1日 1日 1日	Cenditiens 🗸	File Conditions List > New F File Condition	Tile Condition	 	ost.txt]			Submit	Cancel
	Remediations > Requirements Allowed Protocols Automization Profiles Downloadable ACLs									

 $ISE_Add_New_File_Condition_1$

Paso 20. Desplácese hasta Work Centers > Policy Elements > Requirements. Haga clic Edit al final de cualquier nombre de regla. Seleccione Insert new Requirement.

=	dentity Services E	Engine							Work	Centers / Po	osture					
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	/ Elements	Posture	Policy Policy Sets	Tro	ubleshoot	Reports	Settings				
10	Dashboard Context Visibility	Conditions Anti-Male	~									Guide Me				
×	Operations	Anti-Spyv	ware	Requirements												
0	Policy	Anti-Virus	5	Name		Operating Sys	tem	Compliance Module		Posture Type		Conditions		Remediations Actions		
	Administration	Compoun	d	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 🖂	
-	A CHINE COULD BE COUL	Dictionary	Compound	Any_AV_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_def	then	AnyAVDefRemediation/Win	Edit	Duplicate
- Ali	Work Centers	Dictionary	y 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 new P
		Disk Encry External D	yption DataSource	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit	Delete
3	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	nagement	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_def	then	AnyASDefRemediationMac	Edit 🛩	
		Script		Any_AM_Installation_Wir	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 😔	
		U\$8		Any_AM_Installation_Ma	for	Mac OSX	using	4.x or later	gnieu	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	16 >	Any_AM_Installation_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_inst	then	Select Remediations	Edit 😪	
		Requirement	15	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	tocols	USB_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	USB_Block	Edit 😣	
		Authorization Downloadabl	e ACLs	Default_AppVis_Requirer 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_Requirer ent_Mac	n for	Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Mac	then	Select Remediations	Edit 😔	
				Default_Hardware_Attrib 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_Attrib es_Requirement_Mac	it for	Mac OSX	using	4.x or later	using	Agent	met 2	Hardware_Attribute s_Check	then	Select Remediations	Edit 😔	
				Default_Hardware_Attrib es_Requirement_Mac Note: Remediation Action is filtered Remediation Actions are not a	at for based on	Mac OSX the operating syst for Application Co	using em and stealt iditions (confi	4.x or later h mode selection. gured using the Provision By I	using Category (Agent or Provision By Ever	met if rything options), Ha	Hardware_Attribute s_Check rdware Conditions, and	then	Select Remediations Data source conditions.	Edit 👻	

ISE_Add_New_Posture_Requirement

Paso 20.1. Configure los detalles:

Nombre: Test_exist_linux

Sistemas operativos: Linux All

Módulo de cumplimiento: 4.x o posterior

Tipo de postura: Agente

Condiciones: linux_demo_file_exist

Haga clic en Done y 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	101 Jun 2001 101 101	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 Daset
						Save

ISE_Add_New_Posture_Requirement_1



Nota: A partir de ahora, sólo se admiten scripts de shell para los agentes Linux como solución.

Paso 21. Desplácese hasta Work Centers > Posture > Policy Elements > Authorization Profiles. Haga clic en Add.

Paso 21.1. Configure los detalles:

Nombre: unknown_redirect

Marque la casilla de verificación de Web Redirection(CWA,MDM,NSP,CPP)

Seleccionar Client Provisioning(Posture)

ACL: redirección

Valor: Client Provisioning Portal (predeterminado)

≡ :	Indentity Services Engine	Work Centers / Posture
Щ.	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
11 13 10 10 10 10 10 10 10 10 10 10 10 10 10	Conditions Anti-Malware Anti-Spyware Anti-Virus Application Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall Hardware Attributes Patch Management	* Name unknown_redirect Description * Access Type Access_Accept * Access Type Access_accept * Cisco * Access Type Access_accept *
	Registry Script Service USB Remediations Requirements Allowed Protocols Authorization Profiles Downloadable ACLs	 Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) Client Provisioning (Posture) ACL redirect Value Client Provisioning Portal (def: ~ Static IP/Host name/FQDN Suppress Profiler CoA for endpoints in Logical Profile

ISE_Add_New_Authorization_Profile_Redirect_1



Nota: Esta redirección de nombre de ACL debe coincidir con el nombre de ACL correspondiente configurado en FTD.

Paso 21.2. Repita el Add para crear otros dos perfiles de autorización para terminales no conformes y conformes con los detalles.

Nombre: non_compliance_profile

Nombre de DACL: DENY_ALL_IPv4_TRAFFIC

Nombre: compliance_profile

Nombre de DACL: PERMIT_ALL_IPv4_TRAFFIC



Nota: La DACL para terminales conformes o no conformes debe configurarse según los requisitos reales.

Paso 22. Desplácese hasta Work Centers > Posture > Posture Policy. Haga clic Edit al final de las reglas. Seleccione Insert new policy.

date Mandley Pandage	- Fastas						Г	West 6							~			1
ince identity services	s engine						L	Work Centers /	Pos	ture					ų	•	6	2
Bookmarks	Overview	v Ne	twork Devices	Client Provisioning P	olicy Elements	Posture Policy Polic	y Sets	Troubleshoot	R	eports Settings								
Dashboard					L													
Context Visibility		Post	ure Policy	Guide Me														
Operations		Define the	Posture Policy by c	onfiguring rules based on opera	ting system and/or othe	r conditions.										~		
Policy		~																
Administration		Status	Policy Options	Rule Name	Identity Groups	Operating Systems		Compliance Module		Posture Type	Other Conditions		Requirements	_				
Work Centers			Policy Options	Default_AntiMalware_Policy_Ma c	if Any	and Mac OSK	and	4.x or later	and	Agent	and	then	Any_AM_installation_Ma c	Edt 🛩				
			Policy Options	Default_AntiMalware_Policy_Ma c_temporal	ir Any	and Mac OSX	and	4.x or later	and	Temporal Agent	and	0.44	Any_AM_installation_Ma	Duplicate Edit				
Interactive Help			Policy Options	Default_AntiMalware_Policy_Wi	ii Any	and Windows All	and	4.x or later	and	Agent	and	the	Any_AM_Installation_Wi	Edit Creats				
			Policy Options	n Default_AntiMalware_Policy_Wi	if Any	and Windows All	and	4.x or later	and	Temporal Agent	and	then	n Any_AM_Installation_Wi	Edt v				
		-		n_temporal						-			n_temporal					
		0	Policy Options	Denaut_Apparts_Policy_Mac	1 Aug	and Mac OSX	and	6.x or later	ang	Agent	and .	0.44	ment_Mac	Edit 🤟				
			Policy Options	Default_AppVis_Policy_Mac_te mporal	If Any	and Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Mac_temporal	Edt y				
			Policy Options	Default_AppVis_Policy_Win	ii Any	and Windows All	and	4.x or later	and	Agent	and	then	Default_AppVIs_Require ment_Win	Edt -				
			Policy Options	Default_AppVis_Policy_Win_te	ir Any	and Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require	Edt v				
			Policy Options	Default_Firewall_Policy_Mac	it Any	and Mac OSX	and	4.x or later	and	Agent	and	then	Default_Firewalt_Require	Edt v				
			Policy Options	Default Firewall Policy Mar. te	1 Arr	and MarcOSX	and	& a or later	ini	Temporal Agent	and	The	ment_Mac Default_Firewall_Require	50 ×				
		-		mporal									ment_Mac_temporal					
			Policy Options	Default_Firewall_Policy_Win	ir Any	and Windows All	and	4.x or later	and	Agent	and	then	Default_Firewall_Require ment_Win	Edt -				
			Policy Options	Default_Firewall_Policy_Win_te mporal	If Any	and Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_Firewall_Require ment_Win_temporal	Edt v				
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	If Any	and Mac OSK	and	4.x or later	and	Agent	and	ther	Default_Hardware_Attrib utes_Requirement_Mac	Edt v				
			Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	r Any	and Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_Hardware_Attrib utes_Requirement_Mac_ temporal	Edt v				
			Policy Options	Default_Hardware_Attributes_P olicy_Win	ii Any	and Windows All	and	4.x or later	and	Agent	and	the	Default_Hardware_Attrib utes_Requirement_Win	Edt v				
		-		-				* 11 % * 11					-					

ISE_Add_New_Posture_Policy

Paso 22.1. Configure los detalles:

Nombre de regla: Demo_test_exist_linux

Grupos de identidades: Cualquiera

Sistemas operativos: Linux All

Módulo de cumplimiento: 4.x o posterior

Tipo de postura: Agente

Requisitos: Test_exist_linux

Haga clic en Done y Save.

Post	ture Policy	Guide Me configuring rules based on opera	ting syste	m and/or other co	nditi	ons.									~
~															
	Policy Options	Default_Firewall_Policy_Mac	II Any	80	d A	lac OSX	and	4.x or later	- an	d A	pent	and	the	 Default_Firewall_Require ment_Mac 	Edit 🗸
	Policy Options	Default_Firewall_Policy_Mac_te mporal	II Any	an	d A	Aac OSX	and	4.x or later	-24	d Te	imporal Agent	and	the	n Default_Firewall_Require ment_Mac_temporal	Edit 😔
	Policy Options	Default_Firewall_Policy_Win	If Any	an	d N	Nindows All	and	4.x or later	an.	d A	pent	and	the	 Default_Firewall_Require ment_Win 	Edit 😔
	Policy Options	Default_Firewall_Policy_Win_temporal	If Any	an	d V	Windows All	and	4.x or later	- 80	d Te	Imporal Agent	and	the	 Default_Firewall_Require ment_Win_temporal 	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	II Any	an	d N	/ac OSX	and	4.x or later	20	d A	pent	and	the	Default_Hardware_Attrib utes_Requirement_Mac	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	ii Any	an	d N	lac OSX	and	4.x or later	20	d Te	emporal Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Mac_ temporal 	Edit 🐱
	Policy Options	Default_Hardware_Attributes_P olicy_Win	II Any	an	d N	Nindows All	and	4.x or later	- 20	d A	pent	and	the	Default_Hardware_Attrib utes_Requirement_Win	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	II Any	an	d V	Mindows All	and	4.x or later	an	d Te	emporal Agent	and	the	Default_Hardware_Attrib utes_Requirement_Win_t emporal	Edit 😔
	Policy Options	Default_US8_Block_Policy_Win	II Any	an	d V	Windows All	and	4.x or later	an	d A	gent	and	the	US8_Block	Edit ~
	Policy Options	Default_USB_Block_Policy_Win	If Any	an	d V	Windows All	and	4.x or later	20	d Te	emporal Agent	and	the	USB_Block_temporal	Edit 😔

ISE_Add_New_Posture_Policy_1

Paso 23. Desplácese hasta Work Centers > Posture > Policy Sets. Haga clic para Insert new row above.

$\equiv \frac{-de-de}{c_{\rm DECO}}$ Identity Services	ingine	Work Centers / Posture	A @ @ A A
JI Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy	Sets Troubleshoot Reports	Settings
Dashboard	Policy Sets		Inset Reset Policyset Hitcourts Size
% 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
			Read

ISE_Add_New_Policy_Set

Paso 23.1. Configure los detalles:

Nombre del conjunto de políticas: Estado del firewall

Condiciones: Dispositivo de acceso a la red Dirección IP EQUALs [Dirección IP FTD]

Haga clic Save .

=	dentity Services	Engine							Work Centers /	Posture					c	<u>م</u> د	۲	۹ ۱	۹
J.	Bookmarks	Overview	Networl	k Devices	Client Provisioni	ng Policy Eleme	ents Posture Policy	Policy Sets	Troubleshoot	Reports	Settings								
82 13	Dashboard Context Visibility	p	olicy Sets										Reset	Reset	Policyset H	Recounts		Save	
*	Operations		Status	Policy Set M	iame Des	cription	Conditions						Allowed Protoco	ls / Server !	Sequence	Hits	Actions	View	
0	Policy		Q, Searc	h.														_	
2.	Administration		0	Firewall Posts	-		Network Access Device	P Address EQUALS					Default Network	Access	2+	,	٨	>	
-1	Work Centers		0	Default	Defa	ult policy set							Default Network	Access	14	+	0	>	
٢	Interactive Help																_		
																Reset		Save	

ISE_Add_New_Policy_Set_1

Paso 23.2. Haga clic > para introducir el conjunto de políticas. Crear nuevas reglas de autorización para estados conformes al estado, no conformes y desconocidos. Haga clic en Save.

De conformidad con compliance_profile

No conforme con non_compliance_profile

Desconocido con unknown_redirect

Image: Construction Network Devices Client Provisioning Policy Elements Posture Policy Sets Troubleshoot Reports Settings Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Image: Construction Ima	ş	2 + 0
Image: Status Firewait Posture Default Network Access Device IP Address EQUALS : Default Network Access ** -Authentication Policy(1)	5	<u>∕</u> + o
Condition Policy(1) Use		
Status Rule Name Conditions Use		
	Hit	s Action
a Q Search		
+		
(?) All_User_ID_Stores		eAa
> Options		(Q)
>Authorization Policy - Local Exceptions		
>Authorization Policy - Global Exceptions		
VAuthorization Policy(4)		
Results		
Status Rule Name Conditions Profiles Security Groups	Hitz	Action
Q Search		
Compliant & Session PostureStatus EQUALS Compliant	+ 15	礅
Non_Compliant b Session PostureStatus EQUALS NonCompliant (non_compliant_profile)	+ 5	
Unknown E Session-PostureStatus EQUALS Unknown unknown_redirect / + Select from list	+ 47	

ISE_Add_New_Policy_Set_2

Configuraciones en Ubuntu

Paso 24. Inicie sesión en el cliente Ubuntu mediante la GUI. Abra el explorador para iniciar sesión en el portal VPN. En este ejemplo, es 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
Logon

Ubuntu_Browser_VPN_Login

Paso 25. Haga clic en Download for Linux.

Cisco	Secu	re Client Inst	allatic×	:	+															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

El nombre del archivo descargado es cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu_Browser_VPN_Download_2

Paso 26. Descargue el certificado VPN a través del navegador y cambie el nombre del archivo a <certificate>.crt. Este es el ejemplo de cómo usar firefox para descargar el certificado.

-	demo.example	com/+CSCOE× +	\sim	-	Ø	×
\leftarrow	\rightarrow G	O https://demo. example.com /+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. traveling between computers. It vork. Help

Ubuntu_Browser_VPN_Cert_Download

Paso 27. Abra el terminal en el cliente Ubuntu. Desplácese hasta path home/user/Downloads/ para instalar 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\$

Paso 28. Confíe en el certificado del portal VPN en el cliente 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

Paso 29. Abra Cisco Secure Client en el cliente Ubuntu y conecte VPN a demo.example.com correctamente.

		Cisco Secure	Client		•	×
AnyCon	🛙 About					
		יו ויו cisc	 0			
Connect to:	demo.exa	ample.com			~	₽
Group:	posture_v	pn				~)
Username:	isetest					
Password:	******					

	Seconnect 2017				
Connected to demo.example.com.					

 $Ubuntu_Secure_Client_Connected$

Paso 30. Abra el navegador para acceder a cualquier sitio web que active la redirección al portal ISE CPP. Descargue el certificado del portal ISE CPP y cambie el nombre del archivo a <certificate>.crt. Este es un ejemplo del uso de Firefox para la descarga.



Ubuntu_Browser_CPP_Cert_Download

Paso 30.1. Confíe en el certificado del portal CPP de ISE en el cliente 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.
```

Paso 31. Haga clic Start en el portal de ISE CPP.

Device Security Check × +	-	ø	×				
← → C () A https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08 ☆		\bigtriangledown	≡				
Ou 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

Paso 32. Click here to download and install Agent.

Device Security Check × +	- •	×				
← → C https://demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL ☆	\bigtriangledown	≡				
You 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. Unable to detect Posture Agent						
+ This is my first time here						
 You must install Agent to check your device before accessing the network. <u>Click here to download and install Agent</u> After installation, Agent will automatically scan your device before allowing you access to the network. You have 20 minutes to install and for the system scan to complete. 						
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						
+ Remind me what to do next						

Ubuntu_Browser_CPP_Download_Posture

Paso 33. Abra el terminal en el cliente Ubuntu. Vaya a la ruta home/user/Downloads/ para instalar el módulo de estado.

<#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.
```

Paso 34. En la interfaz de usuario del cliente de Ubuntu, salga de Cisco Secure Client y vuelva a abrirlo. El módulo de estado de ISE se ha instalado y se ha ejecutado correctamente.



Ubuntu_Secure_Client_ISE_Posture_Installed

Paso 35. Abra el terminal en el cliente Ubuntu. Navegue hasta rutahome/user/Desktop, cree un test.txt archivo para cumplir con la condición de archivo configurada en ISE.

<#root>

user@ubuntu22-desktop:~\$

cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Conecte VPN a demo.example.com en el cliente Ubuntu.



* Disconnect					
Connected to demo.example.com.					

 $Verify_Ubuntu_Secure_Client_Connected$

Paso 2. Compruebe el estado de ISE en el cliente Ubuntu.



Verify_Ubuntu_Secure_Client_Compliant

Paso 3. Marque Radius Live Log en ISE. Desplácese hasta Operations > RADIUS Live Log.

≡	disclosed in the services Engine			Opera	ations / RADIUS			Q & @ & A	
Щ	Live Logs Live Sessions								
::									
11 O	Misconfigured Supplicants 🕕 Mis		configured Network Devices 🕕		RADIUS Drops 🕕		Client Stopped Responding 🕕	Repeat Counter 🕕	
*	0		0		0		0	0	
U							Refresh Show	Within	
a.							Never v Latest 20 rei	cords v Last 24 hours v	
đ	ට් 🖆 Reset Repeat Counts 🖞) Export To 💛						Filter 🗸 🛞	
	Time	Status Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy A	uthorization Policy	
?		Y	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy /	Authorization Policy	
	May 29, 2024 09:08:48.798 PM	۵	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default Fi	rewall Posture >> Compliant	
	May 29, 2024 09:08:48.798 PM			52:54:00:17:6B:FA		Compliant	Firewall Posture Fi	irewall Posture >> Compliant	
	May 29, 2024 09:08:13.570 PM	a a	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default Fi	rewall Posture >> Unknown	

Verify_ISE_LiveLog

Paso 4. Vaya a FTD CLI mediante SSH o la consola.

<#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

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para ver el flujo de estado y la resolución de problemas de Cisco Secure Client e ISE, consulte los <u>documentos de</u> CCO<u>ISE Posture Style</u> <u>Comparison for Pre and Post 2.2 y Troubleshooting de ISE Session Management and Posture.</u>

Información Relacionada

<u>Compatibilidad de componentes de red de Cisco Identity Services Engine, versión 3.3</u>

- <u>Guía del administrador de Cisco Identity Services Engine, versión 3.3</u>
- <u>Soporte técnico y descargas de Cisco</u>

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).