Configurar a postura da VPN Linux com o ISE 3.3

Contents
Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Diagrama de Rede
Configurações no FMC/FTD
Configurações no ISE
Configurações no Ubuntu
Verificar
Troubleshooting
Informações Relacionadas

Introdução

Este documento descreve como configurar a postura da VPN Linux com o Identity Services Engine (ISE) e o Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Client
- VPN de acesso remoto no Firepower Threat Defense (FTD)
- Identity services engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Ubuntu 22,04
- Cisco Secure Client 5.1.3.62
- Defesa contra ameaças do Cisco Firepower (FTD) 7.4.1
- Cisco Firepower Management Center (FMC) 7.4.1
- Cisco Identity Services Engine (ISE) 3.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Topologia

Configurações no FMC/FTD

Etapa 1. A conectividade entre o cliente, o FTD, o FMC e o ISE foi configurada com êxito. Como enroll.cisco.com é usado para endpoints que realizam sondagem para redirecionamento (consulte fluxo de postura CCO documentsISE Posture Style Comparison for Pre and Post 2.2 para obter detalhes). Verifique se a rota para o tráfego para enroll.cisco.com no FTD está configurada corretamente.

Etapa 2. Faça o download do nome cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg do pacote a partir de Download do Software Cisco e certifique-se de que o arquivo esteja bom após o download confirmando que o checksum md5 do arquivo baixado é o mesmo que a página Download do Software Cisco.

Etapa 3. Navegue até Objects > Object Management > VPN > Secure Client File. Clique em Add Secure Client File, forneça o nome, procureFile Name para selecionar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, selecione Secure Client Image na lista suspensa File Type. Em seguida, clique em 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

Etapa 4. Navegue até Objects > Object Management > Network.

Etapa 4.1. Crie um objeto para o servidor DNS. Clique em Add Object, forneça o nome e o endereço IP DNS disponível. Clique em Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects Integration			Deploy Q 💕 🌣 🕢 admin 🕬 SECURE
Distinguished Name DNS Server Group External Attributes File List File List File List Key Chain Network	Network	. Network objects are used in various places, including acces	s control policies, network variables, int	Add Network	C, Filter Add Object mport Object otts, and so on.
	Name			Value	Type Override
	any	New Network Object	0	0.0.0.0/0 ::/0	Group 🖬 Q 🗑 🛤
	any-ipv4			0.0.0/0	Network 월 Q, 🗑 🕅
		Description Description Network Host Range Network Allow Overrides	O FQDN		
			Cancel Save		

FMC_Add_Object_DNS



Observação: o servidor DNS configurado aqui deve ser usado para usuários VPN.

Etapa 4.2. Crie um objeto para ISE PSN. Clique em Add Object, forneça o nome e o endereço IP PSN do ISE disponível. Clique em 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	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 Network	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

Etapa 5. Navegue até Objects > Object Management > VPN > Group Policy. Clique em Add Group Policy. Clique em DNS/WINS e selecione o objeto do servidor DNS no Primary DNS Server. Em seguida, clique em Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects	Integration	Deploy Q 🚱 🌣 🕢 admin -	disto SECURE
 Distinguished Name DNS Server Group 	Group Policy			Add Group Policy Q, Filter	
External Attributes File List Excenter	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 assign	s the group policy or it is obtained from the current connection profile.	
Geolocation	Name				
Interface	DftGrpPolicy	Add Group Policy	Ø		/i
Network PKI Policy List Port Port Port Prefix List Route Map SLA Monitor Time Range SLA Monitor Time Zone URL Variable Set VLAN Tag VVPN Certificate Map Couton Attribute		Name:* posture_gp Description: General Secun VPN Protocols IP Address Pools Banner DNS/MINS Split Tunneling	a Client Advanced		
KEV1 IPsec Proposal IKEV1 Policy IKEV2 IPsec Proposal IKEV2 Policy Secure Client Customizatio					
Secure Client File			Cancel	Displaying 1 - 2 of 2 rows 1 < Page 1	of 1 > > C

FMC_Add_Group_Policy



Observação: verifique se o servidor DNS usado na política de grupo VPN pode resolver o FQDN e o enroll.cisco.com do portal de provisionamento do cliente ISE.

Etapa 6. Navegue até Objects > Object Management > Access List > Extended. Clique em Add Extended Access List.

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🔕	admin ~ deale SECURE
 AAA Server RADIUS Server Group Single Sign-on Server Access List 	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 addresses. You use these objects when configuring particular features, such as route maps.	Add Extended Access List Q, Filt	er ports. Supports IPv4 and IPv6
Extended	Name	Value	Override

FMC_Add_Redirect_ACL

Etapa 6.1. Forneça o nome da ACL de redirecionamento. Esse nome deve ser o mesmo do perfil de autorização do ISE. Clique em Add.

New Extended Access List Object

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

Allow Overrides

FMC_Add_Redirect_ACL_Part_1

Etapa 6.2. Bloqueie o tráfego DNS, o tráfego para o endereço IP PSN do ISE e os servidores de remediação para excluí-los do redirecionamento. Permita o restante do tráfego. Isso aciona o redirecionamento. Clique em Save.

Add Extended Access List Entry			G
Action: Block Logging: Default Log Level: Informational			
Log Interval: 300 Sec. Network Port 1 Application 1 Users	 Security 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	Add to Source Add to Destination	Source Networks (0) any	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

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

 $FMC_Add_Redirect_ACL_Part_3$



Passo 7. Navegue até Objects > Object Management > RADIUS Server Group. Clique em Add RADIUS Server Group.

Firewall Management Objects / Object Management	Center Overvier	w Analysis	Policies	Devices	Objects	Integration		Deploy	Q	6
✓ AAA Server RADIUS Server Group Single Sign-on Server ✓ Access List	RADIUS Server RADIUS Server Group of	er Group	or more referen	ces to RADIU	JS Servers. Ti	nese AAA servers are used to authenticate users logging in through Remote Access VPN conne	ections.	Add RADIUS Serv	ver Grou	P
Extended	Name						Value			

 $FMC_Add_New_Radius_Server_Group$

Etapa 7.1. Forneça o nome, chequeEnable authorize only, chequeEnable interim account update, chequeEnable dynamic authorization.

Add RADIUS Server Group	?
Name:*	1
rtpise	
Description:	
Group Accounting Mode:	
Single	
Retry Interval:* (1-10) Seconds	
10	
Realms:	
▼	I
Enable authorize only	
Enable interim account update	
Interval:* (1-120) hours	
24	
Enable dynamic authorization	
Port:* (1024-65535)	
• • •	

Cancel

Etapa 7.2. Clique no Plus ícone para adicionar um novo servidor radius. Forneça o PSNIP Address/Hostname, Key do ISE. Selecione o specific interface para conexão. Selecione o Redirect ACL. Em seguida, clique Savepara salvar o novo servidor radius. Em seguida, cliqueSave novamente para salvar o novo 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) 		IP Address/Hostname:* Configure DNS at Threat Defense Platform Settings to resolve hostname Authentication Port:* (1-65535) 1812 Kev:* Orafine Your	
Merge Downloadable ACL with Cisco AV Pair ACL After Cisco AV Pair ACL Before Cisco AV Pair ACL RADIUS Servers (Maximum 16 servers)	+	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 +	
	Cancel Save	Cancel	Save

FMC_Add_New_Radius_Server_Group_Part_2

Etapa 8. Navegue até Objects > Object Management > Address Pools > IPv4 Pools. Clique em Add IPv4 Pools e forneça o **Name, IPv4 Address Range**e Mask. Em seguida, clique em Save.

Firewall Managen Objects / Object Manage	hent Center Overview Analysis Policies Devices Objects Integration		Deploy Q	6 0	fangni v	ence SECURE
> AAA Server > Access List > Address Pools	IPv4 Pools IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.		Add IPv4 P	Q, Filter		
Phyl Roois Phyl Roois Phyl Roois Asplication Fitters AS Path BFD Template Cipher Suite List Community List DHCP IPv6 Pool Distinguished Name DNS Server Group External Attributes Fie List Park-Config Geolocation Interface Key Chain Network Policy List Port Ports Ports Ports Ports Ports Ports Ports Ports Security Intelligence Sinkhole	Name				Dverride	/¥ /¥
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

Etapa 9. Navegue até Certificate Objects > Object Management > PKI > Cert Enrollment. Clique em Add Cert Enrollment, forneça um nome e selecione Self Signed Certificateem Enrollment Type. Clique na guiaCertificate Parameters e forneça Common Name e Country Code. Em seguida, clique em Save.

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Object	integration	De	eploy Q 💕 🌣 🎯 fangni - 🕬	SECURE
AAA Server Access List Address Pools Application Filters	Cert Enrollment A certificate enrollment object contains the Certification Authority (CA) server in your Private Key Infrastructure (PKI).	formation and enrollment parameters that are	Add required for creating Certificate Signing Requests (CSRs) and obtaining identity Ce	Cert Enrollment Q. Filter	cur in
AS Path	Name			Type Override	
BFD Template Clipher Suite List	Add Cert Enrollment	Ø	Add Cert Enrollment	• Serti /	¥
> Community List	Name*		Namo*	berti	ũ.
DHCP IPv6 Pool	demo_vpn		demo_vpn	Serti	i i
 Distinguished Name DNS Server Group External Attributes 	Description		Description		
File List	CA Information Certificate Parameters Key Revocation		CA Information Certificate Parameters Key Revocation		
> FlexConfig	Ferriment Trace Certificate		laster 2001 - Carto an 2001 in antifanta		
Geolocation	Common Name (CN) is manufatory for self-signed certificate that is used in	Damote Access	Include FQUN: Don't use FQUN in certificate *		
Interface Key Chain	VPN. To configure CN, please navigate to 'Certificate Parameters' tab.	nemole Access	Include Device's IP Address:		
Network	Validation Usage: 🗹 IPsec Client 🗹 SSL Client 🗌 SSL Server		Common Name (CN): demo.example.com		
V PKI			Organization Unit (UU):		
Cert Enrollment			Organization (O):		
External Cert Groups			Locality (L):		
External Certs			State (ST):		
Internal CA Groups			Country Code (C): CN		
Internal CAs			Email (E):		
Internal Cert Groups			Include Device's Serial Number		
Internal Certs					
Trusted CA Groups					
Trusted CAs	Allow Overrides		Allow Overrides		
Policy List					
Port Predix List		ancel Save	Ca	ncel Save	
Route Map					
> Security Intelligence				Unspraying 1 - 3 of 3 rows IC C Page 1 of 1	2 al C

FMC_Add_New_Cert_Enroll

Etapa 10. Navegue até Devices > Certificates. Clique em Add, selecione o nome do FTD em Device, selecione inscrição configurada anteriormente em Cert Enrollment. Clique em Add.

Firewall Managem Devices / Certificates	ent Center	Overview Analysis	Policies Devices Object	integration		Deploy	¢ 🔮 م	fangni s	ence SECURE
Filter									Add
All Certificates	*								
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status				
Add Now Cort	ificato			0				<u> </u>	
Add New Cert	mcate			U	@ CA			± 4	2 C 🖬
Add a new certific	ate to the device	e usina cert enro	ollment object which is used	to	G.CA G.ID			± 1	2 C 🖬
generate CA and i	dentify certificat	e.						<u> </u>	
Device*:					Q CA ID			± 8	2 C 🖬
Posture-FTD-Cf	ML27	•							
Cost Forella cott									
demo und		-							
denio_vpr		• +							
Cert Enrollment De	etails:								
Name:	demo_vpn								
Enrollment Type:	Self-Signed	d							
Enrollment URL:	N/A								
			Cancel	ldd					

FMC_Add_New_Cert_To_FTD

Etapa 11. Navegue até Devices > VPN > Remote Access. Clique em Add.

Etapa 11.1. Forneça o nome e adicione o FTD ao Selected Devices. Clique em Next.

Firewall Management Center Overview	Analysis Policies Devices Objects Integration		Deploy Q 🚱 🌣 🕢 admin 🗸 🔥 SECURE
Firewall Management Center Devices / VFW / Senge Witzer	Analysis Delices Delices Delices Magnation • Secure Client • Access & Certificate • Summary	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 Readm or RADRUS Server Group or SSO to authenticate VPN clients. Secure Client Package Make sure you have Secure Client package for VPN client downloaded or you have the relevant Clico credentials to download it during the witard. Device Interface Interface group to enable VPN access.	Deploy Q <table-cell></table-cell>
			Cancel Back Next

FMC_New_RAVPN_Wizard_1

Etapa 11.2. Selecione o grupo de servidores radius configurado anteriormente no Authentication Server, Authorization Server, Accounting Server. Role a página para baixo.

Einewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🗳 🌣 🕢 admin 🗸 📩 SECURE
Remote Access VPN Policy Wizard	
1 Policy Assignment 2 Connection Profile 3 Secure Client 4 Access & Certificate 5 Summary	
• Palicy Assignment • Access & Centricate • Summary • Palicy Assignment • Access & Centricate • Summary • Palicy Assignment • Access & Centricate • Summary • Palicy Assignment • Access & Centricate • Summary • Palicy Assignment • Access & Centricate • Summary • Palicy Assignment • Access & Centricate • Summary • Palicy Assignment • One Color Profile <td></td>	
(MACH PS)	
Client Address Assignment:	
	Cannal Back Next

$FMC_New_RAVPN_Wizard_2$

Etapa 11.3. Selecione o nome do pool configurado anteriormente em IPv4 Address Pools. Selecione a política de grupo configurada anteriormente em Group Policy. Clique em Next.

Firewall Management Center Overview Analysis P	officies Devices Objects Integration	Deploy Q 🚱 🌣 🕲 admin 🗸 👘 SECURE
Remote Access VPN Policy Wizard		
1 Policy Assignment — Connection Profile 3 Secure Clie	nt 4) Access & Certificate 5) Summary	
	(Realm or RADIUS)	
	Accounting Server: rtpise +	
	(RADIUS)	
	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:* postwe_ap +	
	Edit Group Policy	

Cancel Back Next

FMC_New_RAVPN_Wizard_3

Etapa 11.4. Marque a caixa de seleção da imagem do Linux. Clique em Next.

Firewall Management Center Overview Analysis Powiew VPN / Setup Wizard	Policies Devices Objects I	ntegration		Deploy Q 🚱 🌣 🕢 admin ~ 🖓
Remote Access VPN Policy Wizard				
1 Policy Assignment 2 Connection Profile 3 Secure Clie	ent 4 Access & Certificate -	5 Summary		
	Secure Client Image The VPN gateway can automatically o connection is initiated. Minimize connect	Internet Outside Upper	e Corporate Pessurces	
	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-linux64-5.1.3.62-webd	Linux 🔻	

Cancel Back Next

 $FMC_New_RAVPN_Wizard_4$

Etapa 11.5. Selecione a interface da interface VPN. Selecione a inscrição de certificado inscrita no FTD na etapa 9. Clique em Next.



FMC_New_RAVPN_Wizard_5

Etapa 11.6. Confirme duas vezes as informações relacionadas na página de resumo. Se tudo estiver bem, clique em Finish. Se algo precisar ser modificado, clique em Back.

Cancel Back Next





Etapa 12. Implante a nova configuração no FTD para concluir a configuração da VPN de acesso remoto.

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

Configurações no ISE

Etapa 13. Navegue até Work Centers > Posture > Network Devices. Clique em Add.

=	diale Identity Services	Engine					Work Centers	/ Posture				Q	۵ () 0	9 S
н	Bookmarks	Overview	Network D	evices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings				
-	Dashboard														
ph of	Context Visibility	Net	work De	evices	3										
×	Operations											s	elected 0	otal 4	0 0
0	Policy	Ø Edit	+ Add () Duplicate	🛓 Import 🖞 Export	Generate PAC	0 Delete 🗸							All	~ 7
8.	Administration		Name ^	IP/Mask	Profile Name	Location	Туре		Description						
	Work Contern	0	FTD-CML2		🛝 🟥 Cisco 🕕	All Locations	Firewall								
-	work centers	0	FTD-CML2	1.0	🟥 Cisco 🕕	All Locations	Firewall								
		0	FTD-CML2		🟥 Cisco 🕕	All Locations	Firewall								
0	Interactive Help		8.00	100	🗯 Cisco 🕠	All Locations	Firewall								

ISE_Add_New_Devices

Etapa 13.1. Forneça o Name, IP Addresse role a página para baixo.

= :	dentity Service	es Engine				w	ork Centers / I	Posture		
Щ.	Overview Netwo	ork Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Ⅲ ◎ ペ ●	Network Devices Lis Network Device Name Description	t > New Network D CCS posture-FTD	evice							
A 0 A 1	IP Addres	s 🗸 * IP :	······································	-	¢					
U	Device Profile	👬 Cisco	~	1						
	Model Name Software Versio	n		-						
	Network Device	Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Devic	e	~	Set To Default					

ISE_Add_New_Devices_1

Etapa 13.2. Marque a caixa de seleção de RADIUS Authentication Settings. Forneça o Shared Secret. Clique em Submit.

\equiv $\frac{1}{1000}$ Identity Service	s Engine					۷	Vork Centers / P	osture			Q,	0 û	0 A
J. Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings				
E Dashboard	8	~ RADIUS Authent	ication Settings										
* Operations		RADIUS UDP Setting	5										
E Policy		Shared Secret		Show									
2. Administration		Use Second Shared	Secret ()										
H Work Centers		Secon Secret	d Shared		Show								
Interactive Help		CoA Port 1	100	Set To Defa	uit .								
		RADIUS DTLS Setting	ps 🕕										
		DTLS Required											
		Shared Secret rad	ius/d0s	0									
		Issuer CA of ISE	alast if some load factions if		-								
		Certificates for CoA P	elect il required (opsonal)										
		General Settings											
		🗌 Enable KeyWrap 💿											
		Key Encryption Key		Show									
		Message Authenticator Code Key		Show									
		Key Input Format ASCII () HEXA	DECIMAL										
		 TACACS Authen 	tication Settings										
		 SNMP Settings 											
		 Advanced Trusts 	sec Settings										
											Submit	Care	cel

ISE_Add_New_Devices_2

Etapa 14. Baixe o nomecisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg do pacote em <u>Download do software Cisco</u> e verifique se o arquivo está bom confirmando se a soma de verificação md5 do arquivo baixado é a mesma que a página de Download do

software Cisco. O download do nomecisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg do pacote foi concluído com êxito na Etapa 1.

Etapa 15. Navegue até Work Centers > Posture > Client Provisioning > Resources. Clique em Add. Selecione Agent resources from local disk.

≡	diale Identity Services Engine			Wo	ork Centers	/ Posture			
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ ◎ ※	Client Provisioning Policy Resources Client Provisioning Portal	Resources	🚺 Duplicate 🛛 De	siete				Selec	ated 0 Total 16 🕃
		Agent res	ources from Cisco site			Type \vee	Version	Last Update	Description
-		Agent res	ources from local disk			WinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Pro
-file I		Native Su	pplicant Profile			Native Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
		Agent Cor	nfiguration			Native Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?		Agent Pos	sture Profile			MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Pro
		AMP Enab	ler Profile	5.1.3.062		CiscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure (
		CiscoSecur	eClientDesktopLinux 5.1	1.3.062		CiscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure (
		CiscoSecure	eClientComplianceModu	uleWindows 4.3.4015.819	92	CiscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
		CiscoSecure	eClientComplianceModu	uleLinux 4.3.3139.0		CiscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure (
		CiscoAgent	lessWindows 5.0.03061			CiscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAgent	lessOSX 5.0.03061			CiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTempo	oralAgentWindows 5.0.0	03061		CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
		CiscoTempo	oralAgentOSX 5.0.0306	1		CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE_Upload_Resource

Etapa 15.1. Selecione Cisco Provided Package. Clique Choose File para carregar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Clique em Submit.

≡	dentity Services E	ngine		Work Cen	ters / Posture			Q	۵	0	Q	8
三日の火日日の火日日の火日日の火日日の火日の火日の火日の火日の火日の火日の火日の火	Bookmarks Dashboard Context Visibility Operations Policy Administration	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local Agent Resources Fro Category	Disk) Agent Resources From Loc orn Local Disk Cisco Provided Package	al Disk							
A	Work Centers		-	Choose File cisco-secure	eptoy-k9.pkc							
			Submit	Name CiscoSecureClientDesktopLi	Type CiscoSecureClientDe	Version 5.1.3.62	Description Cisco Secure Client for Ii					

ISE_Upload_Resources_1



Observação: repita a Etapa 14. para carregar cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg.

Etapa 16. Navegue até Work Centers > Posture > Client Provisioning > Resources. Clique em Add. Selecione Agent Posture Profile.

≡	duals Identity Services Engine				Work Cent	ers / Posture			
щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Setting	js	
0⊡	Client Provisioning Policy Resources	Resources							
×	Calent Provisioning Portai							Selected 0 Total 16 🔗	3
0		🖉 Edit 🛛 🕂 Add 🔿	Duplicate 📋 De	elete				all \sim ∇	7
		Agent res	sources from Cisco site	,	Version	Last Update	Description		
		Agent res	sources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii		1
-file		Native Su	pplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S		L
		Agent Co	onfiguration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu		L
?		Agent Po	sture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			L
		AMP Ena	bler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

ISE_Add_Agent_Posture_Profile

Etapa 16.1. Forneça o Name, Server name rules e mantenha o restante como padrão. Clique em Save.

Nome: linux_agent_profile

Regras de nome de servidor: *.example.com

≡ :8	sco Identity	Services Engine			Wa	ork Centers /	Posture			
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ 	Client Provis Resources Client Provis	ioning Policy	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

≡ :	sco Identity Serv	ices Engine			w	ork Centers / F	Posture		
Щ	Overview Ne	twork Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Client Provisioning Resources	Policy	Posture Protocol						
×	Client Provisioning	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
a o			Retransmission Delay	(i) 60	secs		Time (in secon	ds) to wait bef	ore retrying.
ส์เ			Retransmission Limit	1 4			Number of retr	ies allowed for	a message.
?			Discovery host 🕕				Enter any IP ad detects and re- portal.	ldress or FQDN directs that http	I that is routed through a NAD. The NAD p traffic to the Client Provisioning
			Discovery Backup Ser	rver List Choose	1		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 * (•.examp	ole.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 eviously connect max time limit	reach discovery targets (redirection ted PSNs) by sending the discovery t is reached
									Cancel Save

ISE_Add_Agent_Posture_Profile_2

Etapa 17. Navegue até Work Centers > Posture > Client Provisioning > Resources. Clique em Add. Selecione Agent Configuration.

≡ :	liale Identity	Services Engine				Work Cent	ers / Posture				
щ	Overview	Network Devices	Client Prov	Policy Elements	Posture Policy	Policy	Sets Troubleshoo	ot Reports	Settings		
	Client Provis Resources	ioning Policy	Resou	urces							
×	Client Provis	ioning Portal								Selected 0 Total 16	C
			🖉 Edit 🛛 -	🕂 Add 🧄 📋 Duplicate 🛛 📋 D	elete					All 🗸	Y
Ψ.				Agent resources from Cisco site		Version	Last Update	Description			
80			0	Agent resources from local disk	oSecureClientDe	51362	2024/05/08 10:31:28	Cisco Secure Clier	nt for li		
កា			0	Agent resources from local disk		0.1.0.02	2024/03/03 04:01:20				-1
				Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Na	itive S		-1
				Agent Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Clier	nt 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_Configuration

Etapa 17.2. Configure os detalhes:

Selecione Pacote de agentes: CiscoSecureClientDesktopLinux 5.1.3.062

Nome: linux_agent_config

Módulo de conformidade: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Marque a caixa de seleção de VPN, Diagnostic and Reporting Tool

Postura ISE de seleção de perfil: linux_agent_profile

Clique em Submit.

≡ :	identity	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		
10	Resources		* Select Agent Package:	Ci	scoSecureClientDesktopLir	ux 5.1.3.062 V			
*	Client Provis	ioning Portal	* Configuration Name:						
U			linux_agent_config						
80			Description:						
កា				10					
0			Description Value N	otes					
			* Compliance Module CiscoSecu	reClientComplianceModule	Linux 4.3.~				
			Cisco Secure Client	Module Selection					
			ISE Posture 🔽 VPN 🗹						
			Secure Firewall						
			Network Visibility						
			Diagnostic and Reporting 🔽 Tool						
			Profile Selection						
			* ISE Posture linux_ager	nt_profile	×			Su	ibmit Canc

ISE_Add_Agent_Configuration_1

Etapa 18. Navegue até Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Clique Edit no final de qualquer nome de regra. Selecione Insert new policy below.

≡ :8	dentity	Services E	Ingine									v	Vork Ce	enters / Post	ure					
щ	Overview	Network	Devices	Clie	nt Provis	ioning	Policy Elemen	nts	Posture Policy	<i>,</i>	Policy Sets	Troul	bleshoot	Reports	Settings					
部 18 火 単 あ。	Client Provis Resources Client Provis	sioning Policy		CI Defin For A For I Wind Intel For N Mac If yo with	ient I Agent Con Native Sup dows Ager architectu Windows A ARM64 pr u configur out an AR	Provision figuration: v plicant Con it, Mac Ager res. Mac po Agent ARM6 plicies requi e an ARM64 dl64 conditio	ioning Policy to deter ersion of agent, ar figuration: wizard p nt, Mac Temporal a blicies run the sam 4 policies, configu e no Other Condi c client provisioning n. This is because	oli min gent orofi and e pa re S tions g po e an	e what users will recc profile, agent compli le andfor wizard. Dra Mac Agentless polici kckage for both archit ession: OS-Architect a arm64 configuration licy for an OS, ensur endpoint is matched	eive up ance of g and ecture ure EC is. e that seque	pon login and use module, and/or ai drop rules to cha oport ARM64. Win es. QUALS arm64 in t the ARM64 policy entially with the p	r session gent cust nge the dows po he Other is at the plicies lis	n initiation tomizatior order. Ilicies run r Conditio e top of th sted in this	: package. separate packag ns column. ne conditions list, s window.	es for ARM4 ar ahead of polic	nd				
				\sim																
?						Rule Name			Identity Groups		Operating Syst	ems		Other Condition	s		Re	sults		
				8		IOS		H	Any	and	Apple IOS All		and	Condition(s)		t	then Ci	sco-ISE-N	SP	Edit 🐱
				8	2	Android		If	Any	and	Android		and	Condition(s)		t	then Cla	sco-ISE-N	SP	Edit
																		Dup	licate above	
																		Dup	licate below	
																		Inse	ert new policy ab	ove
																		Inse	ert new policy be	low

Etapa 18.1. Configure os detalhes:

Nome da regra: Linux

Sistemas Operacionais: Linux All

Resultados: linux_agent_config

Clique em Done e Save.

Overview Network Image: Client Provisioning Policy Resources Client Provisioning Portal Image: Client Provisioning Portal	ntity Services Engine					Work Cen	nters / Posture	9		
Itent Provisioning Policy Resources Client Provisioning Portal Itent Provisioning Portal Itent Provisioning Portal	ew Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
	t Provisioning Policy urces I Provisioning Portal	Client Provisio Define the Client Provisio For Agent Configuration: For Native Supplicant Cor Windows Agent, Mac Age Intel architectures. Mac p For Windows Agent ARM Mac ARM64 policies requil If you configure an ARM6 without an ARM64 conditi	sioning Policy ning Policy to determine version of agent, agent p figuration: wizard profile ant, Mac Temporal and M oblicies run the same pac 64 policies, configure Se iré e no Other Conditions, i d'ellent provisioning poli ion. This is because an e	what users will receip profile, agent complia and/or wizard. Drag ac Agentless policies kage for both archite ssion: OS-Architectu arm64 configurations or for an OS, ensure indpoint is matched s	ve upon login and use nce module, and/or a and drop rules to cha support ARM64. Win ctures. e EQUALS arm64 in 1 that the ARM64 polic; equentially with the p	r session initiation: gent customization p nge the order. dows policies run so he Other Conditions r is at the top of the olicies listed in this y	package. eparate packages f s column. conditions list, ahe window.	for ARM4 and ead of policies		
		Rule Nam	e If If	Identity Groups Any Any	Operating Syst	ems O and Co and Co	ther Conditions ondition(s) ondition(s)	then then	Results Cisco-ISE-NSP Cisco-ISE-NSP	Edit V Edit V

ISE_Add_New_Provisioning_Policy_1

≡	diale Identity Services Engine	Work Centers / Posture	
Щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
표 명 왕	Cenditions V Anti-Malware Anti-Spyware Anti-Virus Application	C View ⊘ Edit + Add □ Duplicate	Selected 0 Total 385 ② @ 서미
8.	Compound	Name Description File name Condition Type	
	Dictionary Compound	pc_XP64_K82797052_MS13 Cisco Predefined Check SYSTEM_PROGRAMS\C Cisco-Defined	0
nii	Dictionary Simple	pc_W8_64_x/83124275_MS Cisco Predefined Check SYSTEM_ROOT\sysnativ Cisco-Defined	
	External DataSource	pc_Vista_K02893284_MS13 Cisco Predefined Check: SYSTEM_321/magehip.dll Cisco+Defined	
?	File	pc_W81_64_K83033889_M Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Firewall	pc_Vista64_KBI25902_MS0 Cisco Predefined Check: SYSTEM_ROOT\winsxs\a Cisco-Defined	
	Hardware Attributes	pc_W10_64_1709_KB45803 Clsco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Registry	pc_XP_K82653956_MS12+0 Clsco Predefined Check: SYSTEM_32\Wintrust.dll Cisco-Defined	
	Script	pc_WIL_XI02092074_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+ Cisco Predefined Check: SYSTEM_32\Win32k.sys Cisco-Defined	
	Remediations >	pc_W10_K83081436_MS15 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_M5 Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Authorization Profiles	pc_W8_64_K82992611_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Downloadable ACLs	pc_W7_K83078601_MS15 Cisco Predefined Check: SYSTEM_32\Win32k.sys Cisco-Defined	

Etapa 19. Navegue até Work Centers > Posture > Policy Elements > Conditions > File. Clique em Add.

Etapa 19.1. Configure os detalhes:

Nome: linux_demo_file_exist

ISE_Add_New_File_Condition

Sistemas Operacionais: Linux All

Tipo de arquivo: FileExistence

Caminho do arquivo: home, Desktop/test.txt

Operador de Arquivo: Existe

Clique em 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 水 し あ。 第1 ②	Conditions Anti-Malware Anti-Malware Anti-Virus Application Compound Dictionary Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall Hardware Attributes Path Maragement: Registry Script Service USB	File Conditions List > New File Condition File Condition Name * Invxx_demo_file_exist Description * Operating System Linux Ali Compliance Module Any version * File Type FileExistence * File Path home * File Operator Exists	Desktop/tes	ıt.txt	}			Submit	Cancel
	Remediations > Requirements Allowed Protocols Authorization Profiles Downloadable ACLs								

 $ISE_Add_New_File_Condition_1$

Etapa 20. Navegue até Work Centers > Posture > Policy Elements > Requirements. Clique Edit no final de qualquer nome de regra. Selecione Insert new Requirement.

marks board ext Visibility ations y	Overview Conditions Anti-Mahe Anti-Spyn Anti-Virus	Network Devices	Client Provisioning	Policy	Elements	Posture i	Policy Policy Sets	Tro	ubleshoot	Reports S	ettings								
board ext Visibility ations y	Conditions Anti-Mahe Anti-Spye Anti-Virus	vare vare																	
ations y	Anti-Spyw Anti-Virus	are									Guide Me								
у	Anti-Virus		Requirements																
	Applicatio	n	Name		Operating Sys	tem	Compliance Module		Posture Type		Conditions		Remediations Actions						
nistration	Compound		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 🖂					
	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					
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					
	Disk Encry	ption	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit					
active 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 🗸					
	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 9					
	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	AnyAMDefRemediationWin	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 9					
	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	USØ_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_Requirem ent_Win	for	Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Win	then	Select Remediations	Edit 🤟					
	Downloadable ACLs	Downloadable ACLs	Downoadable ACLs	CONTROLEGIC ALLS	Dominicatione AGLS		DOWNOUGBOIL AULS	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	t 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	t for	Mac OSX	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 🤟					
	xctive Help	active Help External D File Pack Ma Registry Service USB Remediation Requirement Allowed Prot Authorization Downloadabit	active Help Ethnal Disdove File File File File File File File Fil	External DisdSporce Avy, AV, Ivstallation, Mec File Avy, AV, Cetholico, Mec File Avy, AS, Definition, Mec Hardware Antributes Avy, AS, Definition, Mec Hardware Antributes Avy, AS, Definition, Mec Begintry Avy, AS, Definition, Mec Service Avy, AM, Destallation, Wei USB Avy, AM, Definition, Mec Remediations Avy, AM, Definition, Mec Avy, AM, Definition, Mec Avy, AM, Definition, Mec Notes: Avy, AM, Definition, Mec Definition, Mec USB Avy, AM, Definition, Mec More Protocols Outrion, Statistics, Lin USB Author Protocols Definiti, AppVin, Requirem ert, Mac Definition, AppVin, Requirem ert, Mac Definition, Lin Definition, AppVin, Requirem ert, Mac Definition, Lin Definition, Statistics, Lin Definition, Statistics, Lin Definition, AppVin, Requirem ert, Mac Definition, Statistics, Lin Definition, AppVin, Requirem ert, Mac Definition, Statistics, Attributert, Mac Remediation Actions in Statistics Definition, Statistics in Statistin	External DasSource File File File File File File File Fil	Extranal DisalSource Avg.,MJ, Mastaliation, Mac. fir. Mac. OSX File Avg.,MJ, Catholiton, Mac. fir. Mac. OSX Hardware Antributes Avg.,MJ, Catholiton, Mac. fir. Mac. OSX Patch Management Avg.,MJ, Catholiton, Mac. fir. Mac. OSX Brightry Scinicia Avg.,MJ, Catholiton, Mac. fir. Mac. OSX Scinicia Avg.,MJ, Catholiton, Mac. fir. Mac. OSX USB Avg.,MJ, Definition, Mac. fir. Mac. OSX Avg.,MJ, Definition, Lin. fir. Derion, Applyin, Begurem. fir. Moreal Protocols Orfault, Applyin, Begurem. fir. Definit, Applyin, Begurem. fir. Mac. OSX Barbardation Actions in filtered based on the operating system fir. Barbardation Actions in filtered based on the operating system fir. Barbardation Actions in filtered based on the operatin	External DataBouce Avy, AV, Installation, Adv for Mac 05X using File Herdware Attributes Avy, AV, Installation, Adv for Mac 05X using Avy, AV, Definition, Mac for Mac 05X using Avy, AV, Machine, Line for for Mac 05X using Avy, AV, Machine, Line for for Windows All using Avy, AV, Machine, Line for for Windows All using Avy, AV, Availabilian, Atoms ave for Windows All using Definit, Applyin, Regurierem for Mac 05X	External bisisforce File File Any,AX_Jostalisticn_MAc Nr Mac OSX using 3.x or exterior Network Hordware Artifuites Any,AX_Jostalisticn_MAc Nr Mac OSX using 3.x or exterior Any,AX_Jostalisticn_MAc Nr Mac OSX using 4.x or tare Operation Attors Nr Mac OSX us	Extrand DasSource File File File File File Hardware Attributes Arry, All_Statistics, Mat. 6th Mat. COSX using 3.x or earlier using Arry, All_Statistics, Mat. 6th Mat. COSX using 3.x or earlier using Arry, All_Statistics, Mat. 6th Mat. COSX using 3.x or earlier using Arry, All_Statistics, Mat. 6th Mat. COSX using 3.x or earlier using Arry, All_Statistics, Mat. 6th Mat. COSX using 3.x or earlier using Arry, All_Statistics, Mat. 6th Mat. COSX using 3.x or earlier using Arry, All_Statistics, Mat. 6th Mat. COSX using 4.x or tater using Arry, All_Institution, Mat. 6th Mat. COSX using 4.x or tater using Arry, All_Institution, Mat. 6th Mat. COSX using 4.x or tater using Arry, All_Institution, Infer Ibnux All using 4.x or tater using Arry, All_Institution, Infer Ibnux All using 4.x or tater using Iblue <td< td=""><td>Extrand DasSporce Pile Arr_AV_instaliation_Mat N Mac OSX usin 3.x or earlier usin Apert Marg_AV_instaliation_Mate N Mac OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 4.x or later usin Apert Mater Arr_AV_instaliation_Mate N Matc OSX usin 4.x or later usin Apert Mater Arr_AV_instaliation_Infer No Matc OSX usin 4.x or later usin Apert Mater Dataux_iApplituleurin_infer No Matc OSX using 4.x or later using Apert</td><td>External DisaBource File Avy, MX, Installation, Mae for Mae OSX using A.x.or earlier using Apert memory File May AMX, Distribution, Mae for Mae OSX using A.x.or earlier using Apert memory Parto M. Managament Registry Sorice Avy, AX, Distribution, Mae for Mae OSX using A.x.or earlier using Apert memory Sorice Using Avy, AX, Distribution, Mae for Mae OSX using A.x.or tater using Apert memory Avy, AX, Distribution, Mae for Mae OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mae OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mac OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mac OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mac OSX <t< td=""><td>External Distilization Ary_AU_Installation_Max Nr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Norwall Hudsare Artifubres Ary_AU_Installation_Max Nr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Norwall Hudsare Artifubres Ary_AU_Installation_Max fr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Ary_AU_Installation_Max fr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Service Usine Avy_AU_Installation_Max fr Mac OSX usine Apert mett AVY_aumax_mit Ary_AU_Installation_Max fr Mac OSX usine A.x or later usine Apert mett AVY_aumax_mit Ary_AU_AU_Installation_Max fr Mac OSX usine A.x or later usine Apert mett AVY_aumax_mit_mit Ary_AU_AU_Installation_Max fr Mac OSX usine A.x or later usine <</td><td>Extrand DataSource File Normal points of the second secon</td><td>External Disabases Fig. External Disabases Fig. Max.2, AllIntelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation Mix Mix COSC uing 3. or earlier uing Apr.4 med Mix_Stappendic Mix Mix Apr.4 Mix Mix COSC uing 3. or earlier uing Apr.4 med Mix Apr.4 med Mix Apr.4 Mix Mix Mix Mix Mix Mix Mix Mix Mix Mix</td></t<></td></td<>	Extrand DasSporce Pile Arr_AV_instaliation_Mat N Mac OSX usin 3.x or earlier usin Apert Marg_AV_instaliation_Mate N Mac OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 3.x or earlier usin Apert Arr_AV_instaliation_Mate N Matc OSX usin 4.x or later usin Apert Mater Arr_AV_instaliation_Mate N Matc OSX usin 4.x or later usin Apert Mater Arr_AV_instaliation_Infer No Matc OSX usin 4.x or later usin Apert Mater Dataux_iApplituleurin_infer No Matc OSX using 4.x or later using Apert	External DisaBource File Avy, MX, Installation, Mae for Mae OSX using A.x.or earlier using Apert memory File May AMX, Distribution, Mae for Mae OSX using A.x.or earlier using Apert memory Parto M. Managament Registry Sorice Avy, AX, Distribution, Mae for Mae OSX using A.x.or earlier using Apert memory Sorice Using Avy, AX, Distribution, Mae for Mae OSX using A.x.or tater using Apert memory Avy, AX, Distribution, Mae for Mae OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mae OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mac OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mac OSX using A.x.or tater using Apert memory Avy, AM, Distribution, Mae for Mac OSX <t< td=""><td>External Distilization Ary_AU_Installation_Max Nr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Norwall Hudsare Artifubres Ary_AU_Installation_Max Nr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Norwall Hudsare Artifubres Ary_AU_Installation_Max fr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Ary_AU_Installation_Max fr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Service Usine Avy_AU_Installation_Max fr Mac OSX usine Apert mett AVY_aumax_mit Ary_AU_Installation_Max fr Mac OSX usine A.x or later usine Apert mett AVY_aumax_mit Ary_AU_AU_Installation_Max fr Mac OSX usine A.x or later usine Apert mett AVY_aumax_mit_mit Ary_AU_AU_Installation_Max fr Mac OSX usine A.x or later usine <</td><td>Extrand DataSource File Normal points of the second secon</td><td>External Disabases Fig. External Disabases Fig. Max.2, AllIntelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation Mix Mix COSC uing 3. or earlier uing Apr.4 med Mix_Stappendic Mix Mix Apr.4 Mix Mix COSC uing 3. or earlier uing Apr.4 med Mix Apr.4 med Mix Apr.4 Mix Mix Mix Mix Mix Mix Mix Mix Mix Mix</td></t<>	External Distilization Ary_AU_Installation_Max Nr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Norwall Hudsare Artifubres Ary_AU_Installation_Max Nr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Norwall Hudsare Artifubres Ary_AU_Installation_Max fr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Ary_AU_Installation_Max fr Mac OSX usine 3.x or earlier usine Apert mett AVY_auaumet_mit Service Usine Avy_AU_Installation_Max fr Mac OSX usine Apert mett AVY_aumax_mit Ary_AU_Installation_Max fr Mac OSX usine A.x or later usine Apert mett AVY_aumax_mit Ary_AU_AU_Installation_Max fr Mac OSX usine A.x or later usine Apert mett AVY_aumax_mit_mit Ary_AU_AU_Installation_Max fr Mac OSX usine A.x or later usine <	Extrand DataSource File Normal points of the second secon	External Disabases Fig. External Disabases Fig. Max.2, AllIntelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation_Max fig. Mix COSC uing 3. or earlier uing Apr.4 med Max.2, Mix_Intelliation Mix Mix COSC uing 3. or earlier uing Apr.4 med Mix_Stappendic Mix Mix Apr.4 Mix Mix COSC uing 3. or earlier uing Apr.4 med Mix Apr.4 med Mix Apr.4 Mix					

ISE_Add_New_Posture_Requirement

Etapa 20.1. Configure os detalhes:

Nome: Test_exist_linux

Sistemas Operacionais: Linux All

Módulo de conformidade: 4.x ou posterior

Tipo de postura: Agente

Condições: linux_demo_file_exist

Clique em Done e 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 Darest
						Save

ISE_Add_New_Posture_Requirement_1



Observação: até agora, somente scripts de shell são suportados para agentes Linux como correção.

Etapa 21. Navegue até Work Centers > Posture > Policy Elements > Authorization Profiles. Clique em Add.

Etapa 21.1. Configure os detalhes:

Nome: unknown_redirect

Marque a caixa de seleção de Web Redirection(CWA,MDM,NSP,CPP)

Selecionar Client Provisioning(Posture)

ACL: redirecionar

Valor: Portal de provisionamento do cliente (padrão)

≡ :	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-Virus Application 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 Network Device Profile # Cisco Service Template Track Movement ① Agentless Posture ① Passive Identity Tracking
	Registry Script Service USB Remediations Requirements Allowed Protocols Authorization Profiles Develoardable ACI =	Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) Client Provisioning (Posture) ACL redirect Static IP/Host name/FQDN Suppress Profiler CoA for endpoints in Logical Profile

ISE_Add_New_Authorization_Profile_Redirect_1



Observação: esse redirecionamento de nome de ACL deve corresponder ao nome de ACL correspondente configurado no FTD.

Etapa 21.2. Repita o Add para criar outros dois perfis de autorização para endpoints não compatíveis e compatíveis com os detalhes.

Nome: non_compliance_profile

Nome DACL: DENY_ALL_IPv4_TRAFFIC

Nome: compliance_profile

Nome DACL: PERMIT_ALL_IPv4_TRAFFIC



Observação: a DACL para endpoints compatíveis ou não compatíveis precisa ser configurada de acordo com os requisitos reais.

Etapa 22. Navegue até Work Centers > Posture > Posture Policy. Clique Edit no final de qualquer regra. Selecione Insert new policy.

date Mandley Pandage	- Feeler						- 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	then	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

Etapa 22.1. Configure os detalhes:

Nome da regra: Demo_test_exist_linux

Grupos de Identidade: Qualquer

Sistemas Operacionais: Linux All

Módulo de conformidade: 4.x ou posterior

Tipo de postura: Agente

Requisitos: Test_exist_linux

Clique em Done e 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	 Default_Firewall_Require ment_Mac 	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	ł	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	 Default_Hardware_Attrib utes_Requirement_Mac_ temporal 	Edit 🐱
	Policy Options	Default_Hardware_Attributes_P olicy_Win	H.	Any	and	Windows All	an	4.x or later	and	Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Win 	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	 Default_Hardware_Attrib utes_Requirement_Win_t emporal 	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

Etapa 23. Navegue até Work Centers > Posture > Policy Sets. Clique para Insert new row above.

≡ deader Identity Services	ingine	Work Centers / Posture	A @ @ \$ A
JI Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy	y Sets Troubleshoot Reports	Settings
Dashboard	Policy Sets		Reset Policyset Hitcourts Save
ℜ Operations	• Status Policy Set Name Description Conditions		Allowed Protocols / Server Sequence Hits Actions View
Policy	Q. Search		
Administration	Default Default Default		Default Network Access 🥒 + 🔹 🚳 🗲
③ Interactive Help			Insert new row above
			Reset

ISE_Add_New_Policy_Set

Etapa 23.1. Configure os detalhes:

Nome do Conjunto de Políticas: Postura de Firewall

Condições: Endereço IP do dispositivo de acesso à rede IGUALs [Endereço IP FTD]

Clique Save .

=	dentity Services	Engine							Work Centers /	Posture					¢	<u>م</u> د	۲	۹ ۱	۹
н	Bookmarks	Overview	Networl	k Devices	Client Provisioni	ng Policy Elemen	ts Posture Policy	Policy Sets	Troubleshoot	Reports	Settings								
10 10	Dashboard Context Visibility	ρ	olicy Sets										Reset	Reset	Policyset P	Recounts		Save	
*	Operations		🕑 Status	Policy Set !	iame Desc	cription	Conditions						Allowed Protoco	ls / Server	Sequence	Hits	Actions	View	
0	Policy		Q Searc	h															
8.	Administration		•	Firewall Posts	74		Network Access Device I	P Address EQUALS					Default Network	Access	2+	,	٥	>	
ភា	Work Centers			Default	Defa	ult policy set							Default Network	Access			0	>	
۲	Interactive Help																		
																Reset		Save	
																	_		_

ISE_Add_New_Policy_Set_1

Etapa 23.2. Clique > para inserir o conjunto de políticas. Crie novas regras de autorização para status compatível, não compatível e desconhecido de postura. Clique em Save.

Compatível com compliance_profile

Não Compatível com non_compliance_profile

Desconhecido com 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

Configurações no Ubuntu

Etapa 24. Faça login no cliente Ubuntu via GUI. Abra o navegador para fazer login no portal VPN. Neste exemplo, é demo.example.com.

demo.example.com/+CSCOE×			COEX	+			-	đ	×
$\leftarrow \rightarrow$	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

Etapa 25. Clique em 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

O nome do arquivo baixado é cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu_Browser_VPN_Download_2

Etapa 26. Baixe o certificado VPN pelo navegador e renomeie o arquivo como <certificate>.crt. Este é o exemplo do uso do firefox para baixar o 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

Etapa 27. Abra o terminal no cliente Ubuntu. Navegue até path home/user/Downloads/ para instalar o 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\$

Etapa 28. Confie no certificado do portal VPN no 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

Etapa 29. Abra o Cisco Secure Client no cliente Ubuntu e conecte a VPN ao demo.example.com com êxito.

		Cisco Secure	Client		-		×					
AnyCon	AnyConnect VPN About About											
		ייןיי cisc	 0									
Connect to:	demo.exa	ample.com			~		₽					
Group:	posture_v	pn				,	~					
Username:	isetest											
Password:	••••											

	Se Disconnect				
Connected to demo.example.com.					

 $Ubuntu_Secure_Client_Connected$

Etapa 30. Abra o navegador para acessar qualquer site que dispare o redirecionamento para o portal CPP do ISE. Baixe o certificado do portal CPP do ISE e renomeie o arquivo como <certificate>.crt. Este é um exemplo do uso do Firefox para download.



```
Ubuntu_Browser_CPP_Cert_Download
```

Etapa 30.1. Confie no certificado do portal ISE CPP no 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.
```

Etapa 31. Clique Start no portal CPP do ISE.

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

Ubuntu_Browser_CPP_Start

Etapa 32. Click here to download and install Agent.

Device Security Check × +		- • ×							
$\leftarrow \rightarrow$ C https://demo	pise.example.com :::8443/portal/ClientProvisionStart.action?from=CL 🏠	\boxtimes							
You must log in to this network before	ore you can access the Internet.	×							
alialia 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									
Θ	+ 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

Etapa 33. Abra o terminal no cliente Ubuntu. Navegue até o caminho home/user/Downloads/ para instalar o módulo de postura.

<#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.
```

Etapa 34. Na interface do usuário do cliente Ubuntu, saia do Cisco Secure Client e abra-o novamente. O módulo de postura do ISE foi instalado e executado com êxito.



Ubuntu_Secure_Client_ISE_Posture_Installed

Etapa 35. Abra o terminal no cliente Ubuntu. Navegue até o caminho home/user/Desktop, crie um test.txt arquivo para atender à condição de arquivo configurada no ISE.

<#root>

user@ubuntu22-desktop:~\$

cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Conecte a VPN a demo.example.com no cliente Ubuntu.



*	Disconnect
Connected to demo.example.com	

 $Verify_Ubuntu_Secure_Client_Connected$

Etapa 2. Verifique o status da postura do ISE no cliente Ubuntu.



Verify_Ubuntu_Secure_Client_Compliant

Etapa 3.	Verifique o	registro em	tempo real	do Radius	no ISE.	Navegue a	até Operations	s > RADIUS	Live Log.
----------	-------------	-------------	------------	-----------	---------	-----------	----------------	------------	-----------

=	dentity Services Engine			Оре	rations / RADIUS			Q & @ Q A
Ц	Live Logs Live Sessions							
цц 0	Misconfigured Supplicants 🕕	Miscor	Misconfigured Network Devices 🕕		RADIUS Drops		Client Stopped Responding ①	Repeat Counter ①
*	0		0		0		0	0
U							Refresh Show	Within
a.							Never v Latest 20 re	cords 🗸 Last 24 hours 🗸
đ	ට් 🖆 Reset Repeat Counts ර	🗅 Export To 🗸						Filter 🗸 🐵
	Time	Status Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy A	uthorization Policy
?			Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy
	May 29, 2024 09:08:48.798 PM	٥	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default Fi	irewall 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	irewall Posture >> Unknown

Verify_ISE_LiveLog

Etapa 4. Navegue até a CLI do FTD via SSH ou 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

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para fluxo de postura e solução de problemas do Cisco Secure Client e ISE, consulte os <u>documentos</u> do CCO<u>Comparação de estilo de postura</u> do ISE para pré e pós-2.2 e <u>Solução de problemas de gerenciamento de sessão e postura do ISE</u>.

Informações Relacionadas

<u>Compatibilidade do componente de rede do Cisco Identity Services Engine, versão 3.3</u>

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.3
- Suporte técnico e downloads da Cisco

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.