Konfiguration des Linux VPN-Status mit ISE 3.3

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konfigurieren
Netzwerkdiagramm
Konfigurationen auf FMC/FTD
Konfigurationen auf der ISE
Konfigurationen unter Ubuntu
Überprüfung
Fehlerbehebung
Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration des Linux VPN-Status mit Identity Services Engine (ISE) und Firepower Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Client
- Remote Access VPN mit Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- 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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Topologie

Konfigurationen auf FMC/FTD

Schritt 1: Die Verbindung zwischen dem Client, FTD, FMC und ISE wurde erfolgreich konfiguriert. Da enroll.cisco.com für Endpunkte verwendet wird, die eine Überprüfung der Umleitung durchführen (weitere Informationen finden Sie in den CCO-<u>Dokumenten zum StatusablaufISE</u> <u>Posture Style Comparison for Pre and Post 2.2</u>). Stellen Sie sicher, dass die Route für den Datenverkehr zu enroll.cisco.com auf FTD richtig konfiguriert ist.

Schritt 2: Laden Sie den Paketnamen cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg von <u>Cisco Software Download</u> herunter, und vergewissern Sie sich, dass die Datei nach dem Download korrekt ist. Bestätigen Sie, dass die MD5-Prüfsumme der heruntergeladenen Datei mit der Cisco Software Download-Seite übereinstimmt.

Schritt 3: Navigieren Sie zu Objects > Object Management > VPN > Secure Client File. Klicken Sie aufAdd Secure Client File, geben Sie den Namen ein, File Name wählen Sie aus, cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg und wählen Sie Secure Client Image in der Dropdown-Liste ausFile Type. Klicken Sie dann auf 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

Schritt 4: Navigieren Sie zu Objects > Object Management > Network.

Schritt 4.1: Erstellen eines Objekts für den DNS-Server Klicken Sie aufAdd Object, geben Sie den Namen und die verfügbare DNS-IP-Adresse an. Klicken Sie auf .Save

Firewall Management Objects / Object Management	Center Overview Analysis Policies	Devices Objects Integration			Deploy Q 💕 🌣 🔞 ad	nin 🗸 🖓 da SECURE
Distinguished Name DNS Server Group External Attributes File List	Network A network object represents one or more IP addresses	. Network objects are used in various places, including acces	a control policies, network variables,	Add N	etwork Add Object Add Object Import Object Add Group	ed Objects
Geolocation	Namo			Value	Type Overri	de
Interface	any	New Network Object	?	0.0.0.0/0 ::/0	Group	¶ <u>a</u> Q ≣ A6
Key Chain Network	any-ipv4			0.0.0.0/0	Network	¶aq≣#6
		DNS Description Network Host Range Network Allow Overrides	O FQDN			
			Cancel			

FMC_Add_Object_DNS



Hinweis: Der hier konfigurierte DNS-Server muss für VPN-Benutzer verwendet werden.

Schritt 4.2: Erstellen eines Objekts für ISE PSN Klicken Sie aufAdd Object, geben Sie den Namen und die verfügbare ISE PSN-IP-Adresse an. Klicken Sie auf .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 Geolocation	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	
	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			

$FMC_Add_Object_ISE$

Schritt 5: Navigieren Sie zu Objects > Object Management > VPN > Group Policy. Klicken Sie auf .Add Group Policy Klicken Sie aufDNS/WINS, und wählen Sie das Objekt des DNS-Servers in ausPrimary DNS Server. Klicken Sie dann auf Save.

Firewall Management	t Center Overview	Analysis Policies	Devices Objects	Integration		Deploy Q 🧬	🗘 📵 admin 🗸 dish SECURE
Distinguished Name DNS Server Group	Group Policy					Add Group Policy	Q, Filter
External Attributes	A Group Policy is a set of att	ribute and value pairs, stor	ed in a group policy object, that	define the remote access VPN experience.The	RADIUS authorization server assigns	the group policy or it is obtained from the current conne	ction profile.
File List							
> FlexConfig	Name						
Geolocation	P.0.0 P1		Add Crown Dollar				45
Interface	DittorpPolicy		Add Group Polic	/	0		/1
Key Chain			Mamort				/1
Network			nosture on				
/ PN			postare_gp				
Policy List			Description:				
Deader List							
Route Map							
Security Intelligence			General Secur	e Client Advanced			
Sinkhole			VPN Protocols	Primary DNS Server:			
SLA Monitor			ID Address Dools	DNS, +			
Time Range			Bases	Secondary DNS Server:			
Time Zone			Danner	· +			
Tunnel Zone			DNS/WINS	Primary WINS Server:			
URL			Split Tunneling	· +			
Variable Set				Secondary WINS Server			
VLAN Tag				· +			
V VPN				DHCP Network Scope:			
Certificate Map				• +			
Custom Attribute				Only network object with ipv4 address is allowed	(Ex: 10.72.3.5)		
Group Policy				Default Domain:			
IKEv1 IPsec Proposal							
IKEv1 Palicy							
IKEv2 IPsec Proposal							
IKEv2 Policy							
Secure Client Oustomizatio					Cancel		
Secure Client File					Cancer	Displaying 1 - 2 of 2	trows IC < Page 1 of 1 > >I C

FMC_Add_Group_Policy



Hinweis: Stellen Sie sicher, dass der in der VPN-Gruppenrichtlinie verwendete DNS-Server den ISE-Clientbereitstellungsportal-FQDN und enroll.cisco.com auflösen kann.

Schritt 6: Navigieren Sie zu Objects > Object Management > Access List > Extended. Klicken Sie auf .Add Extended Access List

Firewall Management Objects / Object Management	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 💕 🌣 🕑	admin ~ dub SECURE
✓ AAA Server RADIUS Server Group Single Sign-on Server	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. Filte	r ports. Supports IPv4 and IPv6
Access List Extended	addresses, rok dar inser digects when congruing particular needros, such as roure maps. Name Value		Override

FMC_Add_Redirect_ACL

Schritt 6.1: Geben Sie den Namen der Umleitungszugriffskontrollliste an. Dieser Name muss mit dem im ISE-Autorisierungsprofil

übereinstimmen. Klicken Sie auf .Add

New Exte	nded Ace	cess List Object							Ø
Name redirect									
Entries (0)									
									Add
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
No record	s to display								
_									
Allow Ov	errides								
								Cancel	Save

FMC_Add_Redirect_ACL_Teil_1

Schritt 6.2: Blockieren Sie DNS-Datenverkehr, Datenverkehr zur ISE PSN-IP-Adresse und zu den Wiederherstellungsservern, um diese von der Umleitung auszuschließen. Den restlichen Verkehr zulassen. Dies löst eine Umleitung aus. Klicken Sie auf .Save

Cancel

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

FMC_Add_Redirect_ACL_Teil_2

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 On	Allow verrides	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	11

Cancel Save

 $FMC_Add_Redirect_ACL_Teil_3$



Hinweis: In diesem Beispiel für die Umleitungszugriffskontrollliste wird das Ziel-FTP als Beispiel für den Wiederherstellungsserver

Schritt 7. Navigieren Sie zu Objects > Object Management > RADIUS Server Group. Klicken Sie auf .Add RADIUS Server Group

Firewall Managemen	t Center	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	6
AAA Server RADIUS Server Group Single Sign-on Server Access List	RADIUS RADIUS Serve	Server G	Group ts contain one	or more refere	ences to RADI	US Servers. Ti	nese AAA servers are used to authenticate users logging in through Remote Access VPN conne	Anctions.	dd RADIUS Serv	ver Grou	up
Extended	Name							Value			

FMC_Add_New_Radius_Server_Gruppe

Schritt 7.1: Geben Sie einen Namen ein, prüfen Sie Enable authorize only, prüfen Sie Enable interim account update, prüfen Sie Enable dynamic authorization.

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

FMC_Add_New_Radius_Server_Gruppe_Teil_1

Schritt 7.2: Klicken Sie auf das Plus Symbol, um einen neuen Radius-Server hinzuzufügen. Geben Sie die ISE PSN IP Address/Hostname, Key an. Wählen Sie die specific interface Option zum Herstellen der Verbindung aus. Wählen Sie den Redirect ACL. Klicken Sie dann Saveauf, um den neuen Radius-Server zu speichern. Klicken Sie dann erneut aufSave, um die neue Radius-Server-Gruppe zu speichern.

?

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 Key:* 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_Gruppe_Teil_2

Schritt 8: Navigieren Sie zu Objects > Object Management > Address Pools > IPv4 Pools. Klicken Sie aufAdd IPv4 Pools, und geben Sie das Name, IPv4 Address Rangeund Maskan. Klicken Sie dann auf Save.

Firewall Managerr Objects / Object Manager	ent Center Overview Analysis Policies Devices	Objects Integration		Deploy Q 💕 🌣 🙆	fangni v	enco SECURE
> AAA Server > Access List > Address Pools	IPv4 Pools	nostic interface with clustering, or for VPN remote access profiles.		Add IPv4 Pools Q, Fitte	r	
Prod Pools Prod Pools Application Fitters AS Path BFD Template Cipher Stote List Cipher Stote List DHCP IPv6 Pool Cipher Stote List Community List DHCP IPv6 Pool Cipher Stote List DHCP IPv6 Pool Cipher Stote List Community List DHCP IPv6 Pool Stote Cipher Cipher Cipher Stote Cipher File List Centoria Cesolocation Interface Key Chain Network Pool Pool Pool Pool Pool Stote List Roote Map Scentry Intelligence Sinkhole SLA Monitor Time Range Time Zone	Name of pothers_pool_97_0	Add IPv4 Pool Name* posture_pool Description IPv4 Address Range* 192.168.6.30-192.168.6.100 Format: lpaddr-ipaddr e.g., 10.72.1.1-10.72.1.150 Mask* 255.255.255.0 Iondo Overrides Onfigure device overrides in the address pool object to shared across multiple devices • Override (o)	Cancel		Overnide ©	/1
URL Variable Set				Displaying 1 - 2 of 2 rows	C < Page 1	of 1 > > C

FMC_Add_New_Pool

Schritt 9. Navigieren Sie zu Certificate Objects > Object Management > PKI > Cert Enrollment. Klicken Sie Add Cert Enrollmentauf, geben Sie einen Namen an, und wählen Sie Self Signed Certificateaus Enrollment Type. Klicken Sie auf die Certificate Parameters Registerkarte, und geben Sie Common Name und Country Code an. Klicken Sie dann auf Save.

Firewall Managemen Objects / Object Management	nt Center Overview Analysis Policies Devices	Objects Integration		Deploy Q 💕 🔅 😡 far	ngni 🗸 🔤 diala SECURE
AAA Server Access List Address Pools Application Filters	Cert Enrollment A certificate enrollment object contains the Certification Authority (C your Private Key Infrastructure (PKI).	A) server information and enrollment parameters the	at are required for creating Certificate Signing Requests (CSRs) and obtaining Ider	Add Cert Enrollment Q, Filter	ese activities occur in
AS Path	Name			Type Over	ide
BFD Template Cipher Suite List	Add Cert Enrollment	Θ	Add Cert Enrollment	O Serti	/1
Community List DHCP II-N6 Pool Dis Serier Group External Attributes File List ResConfig Geolocation interface Key Chain Network V PKI Cert Enrollment External Cert Internal Cert	Name* demo_yon Description	on It is used in Remote Access s' tab.	Name* demo_vpn Description Certificate Parameters Key Revocation Include FQDN: Don't use FQDN in certificate Include Device's IP Address: Common Name (CR): demo example.com Organization (DR): Compon Name (CR): demo example.com Organization (DR): Country Code (CI: CN Email (L): Include Device's Serial Number	jeri	/1
Trusted CAs Policy List	Allow Overrides		Allow Overrides		
Port > Prefix List Route Map		Cancel Save		Cancel Save Displaying 1 - 3 of 3 rows IC C Pi	ige 1 of 1 >) C
> Security Intelligence					

FMC_Add_New_Cert_Enrollment

Schritt 10. Navigieren Sie zu Devices > Certificates. Klicken Sie aufAdd, wählen Sie den FTD-Namen unter Device, und wählen Sie die zuvor konfigurierte Registrierung unter Cert Enrollment aus. Klicken Sie auf .Add

Firewall Managerr Devices / Certificates	ent Center Oven	riew Analysis	Policies Devices Objects	Integration		Deploy Q 🔮 🌣 🛛	fangni v once SECURE
Filter All Certificates	¥						Add
Name	Domain En	rollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status		
Add New Cer	tificate			0	G CA LID		A
Add a new certific	ate to the device us	ing cert enr	ollment object which is used	to	© CA		± @ C T
generate CA and	identify certificate.	ing cort on t					•
Posture-FTD-Cl Cert Enrollment*: demo_vpn	ML27	• • +					
Cert Enrollment D	etails:						
Name: Enrollment Type: Enrollment URL:	demo_vpn Self-Signed N/A						
			Cancel	dd			

 $FMC_Add_New_CERT_TO_FTD$

Schritt 11. Navigieren Sie zu Devices > VPN > Remote Access. Klicken Sie auf .Add

Schritt 11.1: Geben Sie den Namen an, und fügen Sie die FTD zu Selected Devices hinzu. Klicken Sie auf .Next

Firewall Management Center Overview	Analysis Policies Devices Objects Integration		Deploy Q 🚱 🌣 🔕 admin 🗸 🕬 SECURE
Firewall Management Center Devices / VMV / Secto Woard Overview Remote Access VPN Policy Wizard Policy Assignment 2 Connection Profile	Analysis Policies Devices Objects Integration 3 Secure Client ④ Access & Certificate ⑤ Summary Targeted Devices and Protocols This wizard will guide you through the required minimal steps to configure the Remote Access VP policy with a new user-defined connection profile. Name:*	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 RADIUS Server Group or SSO to authenticate VPN clients. Secure Client Package Make sure you have Secure Client package for VPN	Deploy Q
	✓ SSL ✓ IPsec-IKEv2	Client downloaded or you have the relevant Cisco credentials to download it during the wizard. Device Interface	
	Targeted Devices: Available Devices Selected Devices Q. Search Posture-FTD-CML22	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.	
	Posture-FTD-CML27 VPN-FTD-Posture-CML: Add		
			Cancel Back Next

FMC_New_RAVPN_Assistent_1

Schritt 11.2: Wählen Sie die zuvor konfigurierte Servergruppe für den Radius im Authentication Server, Authorization Server, Accounting Server. Blättern Sie auf der Seite nach unten.

Firewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 🕼 admin 🗸 🕬 SECURE
Remote Access VPN Policy Wizard	
1) Policy Assignment 3) Connection Profile 3) Secure Client 4) Access & Certificate 5) Summary	
Ramote Secure Client Outside VPN Inside Coporate Resources	
Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the turnel itseft, 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	
This name is configured as a connection alias, it can be used to connect to the VPN gateway	
Authentication, Authorization & Accounting (AAA):	
Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.	
Authentication Method: AAA Only +	
Authentication Server*	
Authorization Server: Trpise (ream or KAUTUS)	
Accounting Server: transit +	
Client Address Assignment:	
	Gancel Back Next

 $FMC_New_RAVPN_Assistent_2$

Schritt 11.3: Wählen Sie den zuvor konfigurierten Poolnamen in IPv4 Address Pools. Wählen Sie die zuvor konfigurierte Gruppenrichtlinie in Group Policyaus. Klicken Sie auf Next.

Firewall Management Center Devices / VPN / Setup Wizard Overview Analysis Policies	Devices Objects Integration	Deploy	۹	¢ 🗘	0	admin 🗸	osce SECURE
Remote Access VPN Policy Wizard							
Policy Assignment Policy Assignment Policy Assignment Policy Assignment Policy Assignment	4 Access & Certificate 5 Summary						
	(Basim or BADELS)						
	Accounting Server: tpise tpis						
	Client Address Assignment:						
	Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.						
	Use AAA Server (Realm or RADIUS only)						
	Use DHCP Servers						
	Use IP Address Pools						
	IPv4 Address Pools: posture_pool						
	IPv6 Address Pools:						
	Group Policy:						
	A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.						
	Group Policy:* posture_ap +						
	Edit Group Policy						

Cancel Back Next

FMC_New_RAVPN_Wizard_3

Schritt 11.4: Aktivieren Sie das Kontrollkästchen des Linux-Abbilds. Klicken Sie auf .Next



Cancel Back Next

FMC_New_RAVPN_Assistent_4

Schritt 11.5: Wählen Sie die Schnittstelle der VPN-Schnittstelle aus. Wählen Sie die Zertifizierung aus, die in Schritt 9 bei FTD registriert wurde. Klicken Sie auf .Next



FMC_New_RAVPN_Assistent_5

Schritt 11.6: Bestätigen Sie die verwandten Informationen auf der Zusammenfassungsseite. Wenn alles in Ordnung ist, klicken Sie auf Finish. Wenn Sie Änderungen vornehmen möchten, klicken Sie auf Back.





Schritt 12: Stellen Sie die neue Konfiguration in FTD bereit, um die Remote Access-VPN-Konfiguration abzuschließen.

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy 2	🚱 🌣 😨 🛛 admin 🗸 🖓 diede SECU	URE
posture_vpn			Q Advanced Deploy Advanced Deploy) Ignore warnings Deploy Can	ncel
			Posture-FTD-CML27	Ready for Deployment ents	s.(1)
Connection Profile Access Interfaces Advanced				:y: No	lone
					+
Name	AAA	Group Policy			
DefaultWEBVPNGroup	Authentiation: None Authorization: None Accounting: None	DftGrpPolicy			
posture_vpn	Authentication: rtpise (RADIUS) Authonization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	posture_gp	1 selected 1 pending	20	

FMC_Bereitstellung_FTD

Konfigurationen auf der ISE

Schritt 13: Navigieren Sie zu Work Centers > Posture > Network Devices. Klicken Sie auf .Add

=	diale Identity Services	Engine					Work Centers	/ Posture				Q	۵	0	٥	۹
Щ	Bookmarks	Overview	Network D	evices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
- 22	Dashboard															
ph of the second	Context Visibility	Net	work De	evices												
×	Operations												Selected (Total	0	٥
0	Policy	Ø Edit	+ Add () Duplicate	🕁 Import 🏠 Export	Generate PAC	🔋 Delete 🗸								All 🗸	γ
8.	Administration		Name \land	IP/Mask	Profile Name	Location	Туре		Description							
	Work Contorn	0	FTD-CML2	100	🗯 Cisco 🕕	All Locations	Firewall									
eili	work Centers	0	FTD-CML2	1.0	📇 Cisco 🕕	All Locations	Firewall									
			FTD+CML2		🟥 Cisco 🕕	All Locations	Firewall									
3	Interactive Help		8.00	1000	🗯 Cisco 🕕	All Locations	Firewall									

ISE_Hinzufügen_Neue_Geräte

Schritt 13.1: Stellen Sie das bereit, Name, IP Addressund blättern Sie auf der Seite nach unten.

≡ :	Identity Servic	es Engine				w	ork Centers / I	Posture		
Щ	Overview Netv	vork Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
Ⅲ 尽 火 ●	Network Devices L Network Dev Name	ist > New Network D ices posture-FTD	evice	_						
A.	IP Addr	ess 🗸 * IP ;	······ / 32	-	¢					
?	Device Profile	👬 Cisco	~	0						
	Model Name		~	_						
	Software Vers	ion	~	-						
	Network Devic	e Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Devic	e	~	Set To Default					

ISE_Hinzufügen_Neue_Geräte_1

Schritt 13.2: Aktivieren Sie das Kontrollkästchen von RADIUS Authentication Settings. Stellen Sie die Shared Secret bereit. Klicken Sie auf .Submit

=	dentity Services	Engine						Vork Centers / P	osture			۵ ۵	0 Q A
щ	Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings			
	Dashboard		~ RADIUS Authent	tication Settings									
뱅	Context Visibility		RADIUS UDP Setting	25									
\propto	Operations		Protocol RA	volus									
0	Policy		Shared Secret		Show								
8.	Administration		Use Second Shared	d Secret 🕕									
đi.	Work Centers		Secor	nd Shared		Show							
			CoA Port 1	700	Set To Defa	uit .							
Q	Interactive Help			- 0									
			DTLS Required	ua 🕣									
			Shared Secret rad	dius/dtls									
			CoA Port 2	1083	Set To Defe	with the second s							
			Issuer CA of ISE	Palast Reserved (astissed)	~ 0								
			Certificates for CoA	select in required (optional)									
			ono name										
			General Settings										
			🗌 Enable KeyWrap 🕓										
			Key Encryption Key		Show								
			Message Authenticator Code Key		Show								
			Key Input Format										
			ASCII () HEXA	ADECIMAL									
			 TACACS Author 	ntication Settings									
			 SNMP Settings 										
			 Advanced Trust: 	are aettings									
												Submit	Cancel

ISE_Hinzufügen_Neue_Geräte_2

Schritt 14: Laden Sie den Paketnamen cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg von Cisco Software Download

herunter, und vergewissern Sie sich, dass die Datei korrekt ist, indem Sie bestätigen, dass die MD5-Prüfsumme der heruntergeladenen Datei mit der Cisco Software Download-Seite übereinstimmt. Der Paketname cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg wurde in Schritt 1 erfolgreich heruntergeladen.

Schritt 15: Navigieren Sie zu Work Centers > Posture > Client Provisioning > Resources. Klicken Sie auf .Add Auswählen Agent resources from local disk.

≡	dentity Services Engine			Wo	rk Centers /	/ Posture			
Щ	Overview Network Devices	Client Provisionin	g Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
Ⅲ 回 火	Client Provisioning Policy Resources Client Provisioning Portal	Resource	S	oloto				Sele	cted 0 Total 16 😅
U.		Agen	resources from Cisco site		т	ype 🗸 🗸	Version	Last Update	Description
a o		Agent	resources from local disk		١	WinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Pro
-file		Native	Supplicant Profile		1	Native Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
		Agen/	Configuration		1	Native Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?		Agen'	Posture Profile		,	MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Pro-
		AMP	Enabler Profile	5.1.3.062	(CiscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure (
		CiscoSe	cureClientDesktopLinux 5.	1.3.062	0	CiscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure (
		CiscoSe	cureClientComplianceMod	uleWindows 4.3.4015.819	92 0	CiscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
		CiscoSe	cureClientComplianceMod	uleLinux 4.3.3139.0	(CiscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure (
		CiscoAg	entlessWindows 5.0.0306	1	(CiscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAg	entlessOSX 5.0.03061		(CiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTe	mporalAgentWindows 5.0.	03061	(CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
		CiscoTe	mporalAgentOSX 5.0.0306	:1	(CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE_Upload_Ressource

Schritt 15.1: Auswählen Cisco Provided Package. Klicken Sie hierChoose File, um cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg hochzuladen. Klicken Sie auf .Submit

E diale Identity Services Engine	Work Centers / Posture	
Bookmarks Dashboard Client Provisioning Policy Context Visibility Context Visibility Client Provisioning Portal Operations	Agent Resources From Local Disk. > Agent Resources From Local Disk. Agent Resources From Local Disk	
Policy Administration Work Centers	Category Cisco Provided Package Choose File cisco-secureeploy-k9.pkc	
) Interactive Help	Agent Uploaded Resources Name Yype Version Description CiscoSecureClientDesktopLi CiscoSecureClientDe 5.1.3.62 Cisco Secure Client for II Submit Cancel	



Hinweis: Wiederholen Sie Schritt 14, um hochzuladen cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg.

Schritt 16: Navigieren Sie zu Work Centers > Posture > Client Provisioning > Resources. Klicken Sie auf .Add Auswählen Agent Posture Profile.

≡ ;	Indentity Services Engine				Work Cent	ers / Posture			
Щ.	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy S	Sets Troubleshoo	t Reports Setting	S	
-10 -10	Client Provisioning Policy Resources	Resources							
×	Client Provisioning Portal							Selected 0 Total 16	Ø
0		🖉 Edit 🛛 🕂 Add 🔿	Duplicate 📋 D	elete				All 🗸	∇
		Agent re	sources from Cisco site	,	Version	Last Update	Description		
40		Agent re	sources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii		
-file		Native S	upplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S		
		Agent Co	onfiguration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu		
?		Agent Po	osture Profile	ntProfile	Not Applic	2024/05/08 10:37:17			
		AMP End	abler Profile	ntProfile	Not Applic	2024/05/16 15:15:49			

ISE_Add_Agent_Status_Profil

Schritt 16.1: Geben Sie die Name, Server name rules an, und behalten Sie den Rest als Standard bei. Klicken Sie auf .Save

Name: linux_agent_profile

Servernamen-Regeln: *.example.com

- cise	" Identity	Services Engine			Wo	ork Centers / I	Posture			
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
11日 12日 火 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	Client Provisi Resources Client Provisi	oning 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

≡ :8	Identity Services Engin	e	N	/ork Centers / P	osture	
Щ	Overview Network Devic	es Client Provisioning Policy E	lements Posture Policy	Policy Sets	Troubleshoot Reports	Settings
-15	Client Provisioning Policy Resources	Posture Protocol				
×	Client Provisioning Portal	Parameter	Value		Description	
0		PRA retransmission time	120 secs		This is the agent retry peri- communication failure	od if there is a Passive Reassessment
a 0		Retransmission Delay ()	60 secs		Time (in seconds) to wait t	before retrying.
ส์เ		Retransmission Limit ()	4		Number of retries allowed	for a message.
?		Discovery host ()			Enter any IP address or FQ detects and redirects that portal.	DN that is routed through a NAD. The NAD http traffic to the Client Provisioning
		Discovery Backup Server List	Choose		By default, AnyConnect se PSNs sequentially if the PS as the backup list and rest discovery probes.	nds discovery probes to all the Cisco ISE IN is unreachable. Choose specific PSNs rict the nodes to which AnyConnect sends
		Server name rules * ①	*.example.com		A list of wildcarded, comm servers that the agent can	a-separated names that defines the connect to. E.g. " *.cisco.com"
		Call Home List 🕕			A list of IP addresses, that that the agent will try to co endpoint doesn't respond	defines the all the Policy service nodes nnect to if the PSN that authenticated the for some reason.
		Back-off Timer 🕕	30 secs		Agent will continuously try targets and previously con packets till this max time li	to reach discovery targets (redirection nected PSNs) by sending the discovery mit is reached
						Cancel Save

ISE_Add_Agent_Posture_Profile_2

Schritt 17: Navigieren Sie zu Work Centers > Posture > Client Provisioning > Resources. Klicken Sie auf .Add Auswählen Agent Configuration.

≡	dentity Services Engine				Work Cent	ers / Posture				
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy S	Sets Troublesho	ot Reports	Settings		
₽1	Client Provisioning Policy Resources	Resources								
×	Client Provisioning Portal								Selected 0 Total 16	C
		🖉 Edit 🛛 🕂 Add 🔿	📋 Duplicate 🍵 De	lete					$_{\rm All}\sim$	7
U.		Agent re:	sources from Cisco site	3	Version	Last Update	Description			
_		Agent re:	sources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Clien	t for li		
កា		Native St	pplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Nat	tive S		1
		Agent Co	nfiguration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Clien	t Linu		1
?		Agent Po	sture Profile	ntProfile	Not Applic	2024/05/08 10:37:17				1
		AMP Ena	bler Profile	ntProfile	Not Applic	2024/05/16 15:15:49				1

ISE_Add_Agent_Konfiguration

Schritt 17.2: Konfigurieren Sie die Details:

Agent-Paket auswählen: CiscoSecureClientDesktopLinux 5.1.3.062

Name: linux_agent_config

Compliance-Modul: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Aktivieren Sie das Kontrollkästchen von VPN, Diagnostic and Reporting Tool

Profilauswahl ISE-Status: linux_agent_profile

Klicken Sie auf .Submit

≡ :8	isco 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	sioning Policy					•		
B	Resources		* Select Agent Package:	Ci	scoSecureClientDesktopLir	nux 5.1.3.062 🗸 🗸			
×	Client Provis	sioning Portal	* Configuration Name:						
U			linux_agent_config						
80			Description:						
កា				li					
?			Compliance Module CiscoSecu Cisco Secure Client ISE Posture C VPN C Secure Firewall	otes rreClientComplianceModule	Linux 4.3.				
			Posture Network Visibility Diagnostic and Reporting Tool Profile Selection * ISE Posture linux_ager	nt_profile	~			St	ibmit Canc

ISE_Add_Agent_Konfiguration_1

Schritt 18: Navigieren Sie zu Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Klicken Sie Edit auf das Ende eines beliebigen Regelnamens. Auswählen Insert new policy below.

≡ ::	isco Identity	Services E	ingine									w	ork C	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 ackage for both architi ession: OS-Architect a arm64 configuration 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

Schritt 18.1: Konfigurieren Sie die Details:

Regelname: Linux

Betriebssysteme: Linux Alle

Ergebnisse: linux_agent_config

Klicken Sie auf Done und Save.

≡	cisco	Identity	Services Engine					1				Wor	k C	enters / Postur	re			
Щ	0	verview	Network Devices	Clie	nt Prov	isioning	Policy Element	s	Posture Polic	у	Policy Sets	Troubles	shoo	ot Reports	Settings			
王 同 火 日		Client Provis Resources Client Provis	ioning Policy	Defi For For Min Inte For	ne the Cl Agent Co Native Su dows Age I architec Windows	Provisor onfiguration: v upplicant Con ant, Mac Age tures. Mac pr Agent ARM6	ioning Policy to determ ersion of agent, age figuration: wizard pr nt, Mac Temporal ar blicles run the same 4 policies, configure	nine ent p rofile nd N pace	cy what users will reci- profile, agent compl e and/or wizard. Dra Aac Agentless policie ckage for both archit ckage for both architect	eive uj liance leg and es sup tecture ture E0	pon login and use module, and/or ag drop rules to cha port ARM64. Win ss. 2UALS arm64 in ti	session init ent customi nge the orde dows policie ne Other Co	tiatio izatio er. s rur nditio	n: n package. n separate packages ons column.	s for ARM4 and			
-AI				Mac If yo with	ARM64 ou configu out an Al	policies requi ure an ARM64 RM64 conditi	re no Other Conditio I client provisioning on. This is because	ons pol an e	arm64 configuration icy for an OS, ensure endpoint is matched	ns. e that I sequi	the ARM64 policy entially with the po	is at the top licies listed	o of t in th	the conditions list, al lis window.	head of policies			
?						Rule Name	•		Identity Groups		Operating Syste	ems		Other Conditions			Results	
				:		IOS		jf.	Any	and	Apple IOS All		and	Condition(s)		then	Cisco-ISE-NSP	Edit 🗸
				_		Android		lf.	Any	and	Android		and	Condition(s)		then	Cisco-ISE-NSP	Edit 🗸
				-		Linux		H.	Any	and	Linux All		and	Condition(s)		then	linux_agent_config	Edit \vee

ISE_Hinzufügen_Neu_Bereitstellung_Richtlinie_1

= :	Indentity Services Engine	Work Centers / Posture	
Щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
11 13 火	Conditions V Anti-Malvare Anti-Spyware Anti-Virus		Selected 0 Total 385 🙆 🔕
	Application	Name Description File name Condition Type	
#0	Dictionary Compound	pc_XP64_KII2797002_M513 Cisco Predefined Check: SYSTEM_PROGRAMS\C Cisco-Defined	8
mil	Dictionary Simple	pc_W8_64_KB3124275_MS Clsco Predefined Check: SYSTEM_ROOT\sysnativ Clsco-Defined	
	External DataSource	pc_Vista_K02803294_M\$13 Cisco Predefined Check: SYSTEM_32\tmagehlp.dll Cisco+Defined	
(?)	File	pc_W81_64_K83033889_M Cisco Predefined Check: SYSTEM_ROOT/sysnativ Cisco-Defined	
	Firewall	pc_Vista64_K8925902_MS0 Cisco Predefined Check: SYSTEM_ROOT\winsxs\a Cisco-Defined	
	Patch Management	pc_W10_64_1709_K845803 Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Registry	pc_XP_KB2653956_MS12+0 Cisco Predefined Check: SYSTEM_32\Wintrust.dll Cisco+Defined	
	Script	pc_W8_K82892074_M513 Cisco Predefined Check: SYSTEM_32\Scrun.dll Cisco-Defined	
	Service	pc_W10_64_1909_K850139 Cisco Predefined Check: SYSTEM_ROOT\SysWO Cisco-Defined	
	038	pc_W7_K82681578_MS12+ Cisco Predefined Check: SYSTEM_32(Win32k.sys Cisco-Defined	
	Remediations >	pc_W10_K83081436_MS15 Cisco Predefined Check: SYSTEM_32\Edgehtml.dll Cisco-Defined	
	Requirements	pc_W81_64_K83042553_M Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Allowed Protocols	pc_W8_64_X82727528_MS 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_KR3078601_MS15 Cisco Predefined Check SYSTEM_32\Win32k.sys Cisco-Defined	

Schritt 19: Navigieren Sie zu Work Centers > Posture > Policy Elements > Conditions > File. Klicken Sie auf .Add

ISE_Add_New_File_Condition

Schritt 19.1: Konfigurieren Sie die Details:

Name: linux_demo_file_exist

Betriebssysteme: Linux Alle

Dateityp: FileExistence

Dateipfad: home, Desktop/test.txt

Dateioperator: existiert

Klicken Sie auf .Submit

≡	dialle Identity Services Engine					Work Cen	iters / Post	ure		
н	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
	Conditions V Anti-Malware Anti-Spyware Application Compound Dictionary Simple Dictionary Simple Disk Encrystoin External DataSource File Firewall Mandware Attributes Pariowal Script Script Service	File Condition File Condition Name * Description * Operating System Compliance Module / * File Type * File Path * File Operator	File Condition	Uesktop/	logi.txt	_}			Submit	Cancel
	Remediations >									
	Requirements Allowed Protocols Authorization Profiles Downloadable ACLs									

 $ISE_Hinzufügen_Neue_Datei_Bedingung_1$

Schritt 20: Navigieren Sie zu Work Centers > Posture > Policy Elements > Requirements. Klicken Sie Edit auf das Ende eines beliebigen Regelnamens. Auswählen Insert new Requirement.

				Posture	Centers / I	Wor							Engine	dentity Servic													
		tings	rts Setti	Reports	oubleshoot	ets T	Policy Policy Se	Posture P	Elements	Policy	Client Provisioning	Network Devices	Overview	Bookmarks	н												
		Guide Me	C					-					Conditions Anti-Mah	Dashboard Context Visibility													
											Requirements	yware	Anti-Spy	Operations	*												
Actions	Remediations Actions	Conditions	c	pe	Posture Typ		Compliance Module	stem	Operating Sy		Name	lon	Applicatio	Policy	0												
V Edit -	Message Text Only	ANY_av_win_inst then	met if Al		Agent	using	3.x or earlier	using	Windows All	in for	Any_AV_Installation_Win	nd	Compour	Administration	a .,												
ationWin Edit Duplicate	AnyAVDefRemediation/Win	ANY_av_win_def then	met if Al		Agent	using	3.x or earlier	using	Windows All	for	Any_AV_Definition_Win	ry Compound	Dictionary	Work Contern													
ly Edit Insert new Req	Message Text Only	ANY_as_win_inst then	met if Al		Agent	using	3.x or earlier	using	Windows All	in for	Any_AS_Installation_Win	ry Simple	Dictionary	Work Centers	nili												
ationWin Edit Delete	AnyASDefRemediationWin	ANY_as_win_def then	met if Al		Agent	using	3.x or earlier	using	Windows All	for	Any_AS_Definition_Win	DataSource	External D														
V Edit V	Message Text Only	ANY_av_mac_inst then	met if Al		Agent	using	3.x or earlier	using	Mac OSX	ec for	Any_AV_Installation_Mac		File	Interactive Help	2												
ationMac Edit v	AnyAVDefRemediationMac	ANY_av_mac_def then	met if Al		Agent	using	3.x or earlier	using	Mac OSX	s for	Any_AV_Definition_Mac		Firewall														
V Edit -	Message Text Only	ANY_as_mac_inst then	met if Al		Agent	using	3.x or earlier	gnieu	Mac OSX	ac for	Any_AS_Installation_Mac	Handware Attributes		Herdware Attributes Patch Management Registry	Hardware												
ationMac Edit -	AnyASDefRemediationMac	ANY_as_mac_def then	met if Al		Agent	using	3.x or earlier	using	Mac OSX	c for	Any_AS_Definition_Mac	Patch Management Registry Script Service USB	Patch Ma														
V Edit	Message Text Only	ANY_am_win_inst then	met if Al		Agent	using	4.x or later	using	Windows All	fin for	Any_AM_Installation_Wir		Script														
iationWin Edit ~	AnyAMDefRemediationWin	ANY_am_win_def then	met if Al		Agent	using	4.x or later	using	Windows All	n for	Any_AM_Definition_Win		Service US8	Service US8	Service US8	Service	Service	Service	Service	Service	Service	Service	Service	Service	Service		
ly Edit	Message Text Only	ANY_am_mac_inst then	met if Al		Agent	using	4.x or later	using	Mac OSX	lac for	Any_AM_Installation_Ma					US8											
lationMad Edit v	AnyAMDefRemediationMac	ANY_am_mac_def then	met if Al		Agent	using	4.x or later	using	Mac OSX	e for	Any_AM_Definition_Mac																
pns Edit v	Select Remediations	ANY_am_lin_inst then	met if Al		Agent	using	4.x or later	using	Linux All	in for	Any_AM_Installation_Lin	ins >	Remediation														
ona Edit v	Select Remediations	ANY_am_lin_def then	met if Al		Agent	using	4.x or later	using	Linux All	for	Any_AM_Definition_Lin	vts	Requirement														
Edit 🤟	USB_Block	USB_Check then	met if U		Agent	using	4.x or later	using	Windows All	for	USB_Block	Allowed Protocols Authorization Profiles Downloadable ACLs	Allowed Protocols	Allowed Protocols	Allowed Protocols	Allowed Protocols	Allowed Protocols	Allowed Protocols	Allowed Protocols	Requirements Allowed Protocols	Allowed Pro						
ons Edit o	Select Remediations	Default_AppVis_Co then ndition_Win	met if De		Agent	using	4.x or later	using	Windows All	em for	Default_AppVis_Requirer ent_Win		Authorizatio														
ons Edit 🤟	Select Remediations	Default_AppVis_Co then ndition_Mac	met if De		Agent	using	4.x or later	using	Mac OSX	em for	Default_AppVis_Requirer ent_Mac	Downloadable ACLs															
ons Edit -	Select Remediations	Hardware_Attribute then s_Check	met if Hi s,		Agent	using	4.x or later	using	Windows All	but for	Default_Hardware_Attrib es_Requirement_Win																
ons Edit v	Select Remediations	Hardware_Attribute then s_Check	met if Hi s,		Agent	using	4.x or later	using	Mac OSX	but for	Default_Hardware_Attrib es_Requirement_Mac																
	Select Remediation Select Remediation Select Remediation Select Remediation	Default_AppVIs_Co then ndlion_Win Co then ndlion_Mac bench Co then ndlion_Mac bench Co then s_Check then s_Check then are Conditions, and External	met if Dr net if Dr net if Pr net if Hi s, met if Hi s,	iverything optio	Agent Agent Agent Agent or Provision By E	using using using using By Categor	4.x or later 4.x or later 4.x or later 4.x or later 4.x or later unode selection. gued using the Provision	using using using using tem and stealth	Windows All Mac OSX Windows All Mac OSX the operating sy for Application C	em for em for but for but for d based on applicable	Default, AppVis, Bequire erc, Win Default, AppVis, Bequire erc, Min Bestaut, Hordwere, Ambrid ers, Bequirement, Wa Default, Hindwere, Ambrid Begurement, Mac	Authorization Profiles Downloadable ACLs															

ISE_Hinzufügen_Neu_Status_Anforderung

Schritt 20.1: Konfigurieren Sie die Details:

Name: Test_exist_linux

Betriebssysteme: Linux Alle

Compliance-Modul: 4.x oder spätere Version

Statustyp: Agent

Bedingungen: linux_demo_file_exist

Klicken Sie auf Done und Save.

= :	Indentity Services Engine			Work Centers / Posture			
н	Overview Network Devices	Client Provisioning Policy Elements Posture P	Policy Policy Sets Tr	oubleshoot Reports S	ettings		
11 15	Conditions v			Guide Me			~ Q
*	Anti-Spyware Anti-Virus	Requirements					
0	Application	Name Operating System	Compliance Module	Posture Type	Conditions Rem	nediations Actions	
80	Compound	Test_exist_linux for Linux All using	4.x or later using	Agent met if	linux_demo_file_ex then Selec ist	ct Remediations Edit v	
al.	Dictionary Compound Dictionary Simple	Any_AV_Installation_Win for Windows All using	3.x or earlier using	Agent met if	ANY_av_win_inst then Mess	sage Text Only Edit 🗸	
	Disk Encryption	Any_AV_Definition_Win for Windows All using	3.x or earlier using	Agent met if	ANY_av_win_def then AnyA	WDefRemediationWin Edit ~	
(?)	External DataSource	Any_AS_Installation_Win for Windows All using	3.x or earlier using	Agent met if	ANY_as_win_inst then Mess	sage Text Only Edit ~	
	File	Any_AS_Definition_Win for Windows All using	3.x or earlier using	Agent met if	ANY_as_win_def then AnyA	ASDefRemediationWin Edit v	
	Firewall Hardware Attributes	Any_AV_Installation_Mac for Mac OSX using	3.x or earlier using	Agent met if	ANY_av_mac_inst then Mess	sage Text Only Edit ~	
	Patch Management	Any_AV_Definition_Mac for Mac OSX using	3.x or earlier using	Agent met if	ANY_av_mac_def then AnyA	WDefRemediationMac Edit ~	
	Registry	Any_A\$_Installation_Mac for Mac OSX using	3.x or earlier using	Agent met if	ANY_as_mac_inst then Mess	sage Text Only Edit 🗸	
	Script	Any_AS_Definition_Mac for Mac OSX using	3.x or earlier using	Agent met if	ANY_as_mac_def then AnyA	ASDefRemediationMac Edit v	
	Service	Any_AM_Installation_Win for Windows All using	4.x or later using	Agent met if	ANY_am_win_inst then Mess	sage Text Only Edit 🗸	
	USB	Any_AM_Definition_Win for Windows All using	4.x or later using	Agent met if	ANY_am_win_def then AnyA	MDefRemediationWin Edit ~	
	Remediations >	Any_AM_Installation_Mac for Mac OSX using	4.x or later using	Agent met if	ANY_am_mac_inst then Mess	sage Text Only Edit ~	
	Requirements	Any_AM_Definition_Mac for Mac OSX using	4.x or later using	Agent met if	ANY_am_mac_def then AnyAi	MDefRemediationMac Edit v	
	Allowed Protocols Authorization Profiles Downloadable ACLs	Note: Remediation Action is fittered based on the operating system and steaht Remediation Actions are not applicable for Application Conditions (confi Remediations Actions are not applicable for Agentiess Posture type.	h mode selection. Igured using the Provision By Category	or Provision By Everything options), Hard	dware Conditions, and External Data so	surce conditions.	ave

ISE_Hinzufügen_Neu_Status_Anforderung_1



Hinweis: Ab sofort werden nur Shell-Skripts für Linux-Agenten als Problembehebung unterstützt.

Schritt 21: Navigieren Sie zu Work Centers > Posture > Policy Elements > Authorization Profiles. Klicken Sie auf .Add

Schritt 21.1: Konfigurieren Sie die Details:

Name: unknown_redirect

Aktivieren Sie das Kontrollkästchen von Web Redirection(CWA,MDM,NSP,CPP)

Auswählen Client Provisioning(Posture)

ACL: umleiten

Wert: Client Provisioning Portal (Standard)

≡ :	lindentity Services Engine	Work Centers / Posture
Щ	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings
11日 11日 11日 11日 11日 11日 11日 11日	Conditions Anti-Malware Anti-Spyware Anti-Virus Application Compound Dictionary Compound Dictionary Simple Disk Encryption External DataSource File Firewall Hardware Attributes	Authorization Profile * Name unknown_redirect Description * Access Type ACCESS_ACCEPT ~ Network Device Profile # Cisco ~ ⊕ Service Template Track Movement ① Agentiess Posture ① Passive Identity Tracking
	Patch Management Registry Script Service US8 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



Hinweis: Diese ACL-Namensweiterleitung muss mit dem entsprechenden, für FTD konfigurierten ACL-Namen übereinstimmen.

Schritt 21.2: Wiederholen Sie den Schritt, Add um weitere zwei Autorisierungsprofile für nicht konforme und konforme Endpunkte mit den Details zu erstellen.

Name: nicht_konformes_Profil

DACL-Name: DENY_ALL_IPv4_TRAFFIC

Name: compliant_profile

DACL-Name: PERMIT_ALL_IPv4_TRAFFIC



Hinweis: Die DACL für kompatible oder nicht kompatible Endgeräte muss entsprechend den tatsächlichen Anforderungen konfiguriert werden.

Schritt 22: Navigieren Sie zu Work Centers > Posture > Posture Policy. Klicken Sie Edit am Ende einer Regel auf. Auswählen Insert new policy.

								-		_							
E dect Identity Services	Engine								Work Centers /	Pos	ture					۵ ۵	© ₽
Bookmarks	Overview	v Ne	twork Devices	Client Provisioning	Policy Elements	Postu	re Policy Po	licy Sets	Troubleshoot	R	eports Settings						
Dashboard		_															
Context Visibility		Post	ure Policy	Guide Me													
Coperations		Define the	Posture Policy by c	onfiguring rules based on oper	ating system and/	or other cond	itions.									Ŷ	
Policy		~															
Administration		Status	Policy Options	Rule Name	Identity Gro	oups	Operating System	ns	Compliance Module		Posture Type	Other Conditions		Requirements	_		
Work Centers			Policy Options	Default_AntiMalware_Policy_Ma c	ir Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Any_AM_Installation_Ma	Edit প		
			Policy Options	Default_AntiMalware_Policy_Ma	ir Any	and	Mac OSK	and	4.x or later	and	Temporal Agent	and	then	Any_AM_installation_Ma c_temporal	Duplicate Edit Inset new policy		
D Interactive Help			Policy Options	Default_AntiMalware_Policy_W	ii Any	and	Windows All	and	4.x or later	and	Agent	and	then	Any_AM_Installation_Win	Ed. Luura		
			Policy Options	Default_AntiMalware_Policy_Win_temporal	ii Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Any_AM_Installation_Win_temporal	Edt -		
			Policy Options	Default_AppVis_Policy_Mac	i' Any	and	Mac OSX	and	4.x or later	and	Agent	and	then	Default_AppVis_Require ment_Mac	Edit +		
			Policy Options	Default_AppVis_Policy_Mac_te mporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Mac_temporal	Edit y		
			Policy Options	Default_AppVIa_Policy_Win	i Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_AppVis_Require ment_Win	Edit v		
			Policy Options	Default_AppVis_Policy_Win_te mporal	ii Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then	Default_AppVis_Require ment_Wis_temporal	Edit v		
			Pullcy Options	Default_Firewall_Policy_Mac	ii Any	and	Mac OSX	and	4.x or later	and	Agent	and	then.	Default_Firewall_Require ment_Mac	Edt v		
			Policy Options	Default_Firewall_Policy_Mac_te mporal	ii Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and	then	Default_Firewall_Require ment_Mac_temporal	Edit -		
			Policy Optiona	Default_Firewall_Policy_Win	ir Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_Firewall_Require ment_Win	Edit v		
			Policy Options	Default_Firewall_Policy_Win_te mporal	ir Any	and	Windows All	and	4.x or later	and	Temporal Agent	and	then.	Default_Firewall_Require ment_Win_temporal	Edit v		
			Policy Options	Default_Hardware_Attributes_P olicy_Mac	ii Any	and	Mac OSX	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	i' 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	r Any	and	Windows All	and	4.x or later	and	Agent	and	then	Default_Hardware_Attrib utes_Requirement_Win	Edit 9		
		-	·····	*					* 11 Mali		******						

ISE_Hinzufügen_Neuer_Status_Richtlinie

Schritt 22.1: Konfigurieren Sie die Details:

Regelname: Demo_test_exist_linux

Identitätsgruppen: Alle

Betriebssysteme: Linux Alle

Compliance-Modul: 4.x oder spätere Version

Statustyp: Agent

Voraussetzungen: Test_exist_linux

Klicken Sie auf Done und 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	H	Any	and	Windows All	an	4.x or later	and	Temporal Agent	and	the	n Default_Firewall_Require ment_Win_temporal	Edit 🤟
	Policy Options	Default_Hardware_Attributes_P olicy_Mac	H	Any	and	Mac OSX	an	4.x or later	and	Agent	and	the	n Default_Hardware_Attrib utes_Requirement_Mac	Edit 👻
	Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	1	Any	and	Mac OSX	an	4.x or later	and	Temporal Agent	and	the	 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_Hinzufügen_Neu_Status_Richtlinie_1

Schritt 23: Navigieren Sie zu Work Centers > Posture > Policy Sets. Klicken Sie auf Insert new row above.

≡ deader Identity Services	ingine	Work Centers / Posture	A @ @ Q A
JI Bookmarks	Overview Network Devices Client Provisioning Policy Elements Posture Policy	Troubleshoot Reports	Settings
Dashboard	Policy Sets		Reset Policyset Hitcounts Saw
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 2 + 0 🛞 🗲
③ Interactive Help			Insert new row above
			Resol

ISE_Hinzufügen_Neu_Policy_Set

Schritt 23.1: Konfigurieren Sie die Details:

Richtliniensatzname: Firewall-Status

Bedingungen: IP-Adresse des Netzwerkzugriffsgeräts ENTSPRICHT [FTD-IP-Adresse]

Klicken Sie auf . Save

=	dentity Services	Engine							Work Centers /	Posture					c	۵ ۵	۲	۹ ۱	۹
P.	Bookmarks	Overview	Net	rork Devices	Client Provisionin	g Policy Elements	s Posture Policy	Policy Sets	Troubleshoot	Reports	Settings								
80 (6	Dashboard Context Visibility		Policy Se	ts									Reset	Reset	Policyset H	itcounts		Save	
. 94	Operations		State	itus Policy Set	Name Desc	ription Co	onditions						Allowed Proto	cols / Server	Sequence	Hits	Actions	View	
- 0	Policy		Q, 5	iaich															
.8.	Administration		-	Firewall Por	iture		P Network Access Device	P Address EQUALS					Default Netw	ork Access	2+	7	0	,	
-1	Work Centers			Default	Defaul	It policy set							Default Netw	ork Access	<i>i</i> +	+	0	>	
•	Interactive Help															Reset		Save	

ISE_Hinzufügen_Neue_Richtlinie_Festlegen_1

Schritt 23.2: Klicken Sie >, um den Richtliniensatz einzugeben. Erstellen Sie neue Autorisierungsregeln für den Status "Compliance", "Compliance nicht" und "Unbekannt". Klicken Sie auf .Save

Konformität mit compliance_profile

Nicht konform mit nicht konformem Profil

Unbekannt mit unknown_redirect

≡	disco Iden	ntity S	Servic	es Engine					Work Cent	ers / Postu	re						
н	Overvie	w v	Netwo	ork Devices Client	t Provisioning Policy	Elements F	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
탱			۰	Firewall Posture		P Network	Access-Device IP Addre	ess EQUALS :						Default Netwo	rk Access	0	+ 0
*	~	Authe	ntication	Policy(1)													
0		Ð	Status	Rule Name	Conditions								Use			Hits	Actions
40 		Q	Search														
mil									+								
?				Defects									All_User	ID_Stores	1	-	rêt.
			Ŭ	Delenit.									> Optio	ns		*0	253.
	>	Autho	rization	Policy - Local Exceptions													
	>	Autho	rization	Policy - Global Exceptions	5												
	~	Autho	rization	Policy(4)													
											Results						
		۲	Status	Rule Name	Conditions						Profiles		Security G	roups		Hits	Actions
		Q	Search														
			٥	Compliant	는 Session-PostureStatu	s EQUALS Complia	м				compliant_profile	1 +	Select fro	om list	1	15	<u>ې</u>
			٥	Non_Compliant	b Session PostureStatu	s EQUALS NonCom	pliant				non_compliant_profile	0+	Select fro	am list	Ø +	5	(2)
			0	Unknown	E Session-PostureState	s EQUALS Unknown	1				unknown_redirect	1 +	Select fro	am list	1+	47	©
	CIECO	•		NUMBER STORES IN THE STORES STORES		THE RECEIPTION OF THE RECEIPTI											

ISE_Hinzufügen_Neue_Richtlinie_Festlegen_2

Konfigurationen unter Ubuntu

Schritt 24: Melden Sie sich über die Benutzeroberfläche beim Ubuntu-Client an. Öffnen Sie den Browser, um sich beim VPN-Portal anzumelden. In diesem Beispiel ist dies demo.example.com.

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

Logon
Group posture_vpn v
Username
Password
Logon

Ubuntu-Browser_VPN_Anmeldung

Schritt 25: Klicken Sie auf .Download for Linux

Cisco Secu	re Client Insta	llati	+					ē	×
$\leftarrow \ \rightarrow $	С	0 &	https://demo. example.com /CACHE/stc/2/index.html	F	80%	ជ	\bigtriangledown	1	≡
	Secure	RE Client							
	C		Disco Secure Client Download		9				A
			Download & Install						
			Download Cisco Secure Client and install it on your computer. Download for Linux						
				•) Inst	ructions			

Ubuntu-Browser_VPN_Download_1

Der Name der heruntergeladenen Datei lautet cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu-Browser, VPN, Download 2

Schritt 26: Laden Sie das VPN-Zertifikat über den Browser herunter, und benennen Sie die Datei um in <Zertifikat>.crt. Dies ist das Beispiel, in dem Firefox zum Herunterladen des Zertifikats verwendet wird.

-	demo.example.	com/+CSCOE× +	\sim		đ	×
\leftarrow	\rightarrow C	Ttps://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 information 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, 128 The page you are viewing was encrypted before being tr Encryption makes it difficult for unauthorized people to therefore unlikely that anyone read this page as it travel	8 bit keys, TLS 1.3) ransmitted over the view information t led across the netw	e Internet. raveling between computers. It i rork. Help

 $Ubuntu-Browser_VPN_Zertifikat_Herunterladen$

Schritt 27: Öffnen Sie das Terminal auf dem Ubuntu-Client. Navigieren Sie zu,path home/user/Downloads/ um Cisco Secure Client zu installieren.

<#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
```

user@ubuntu22-desktop:~/Downloads\$

```
sudo ./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\$

Schritt 28: Vertrauen Sie dem VPN-Portalzertifikat auf dem Ubuntu-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\$

```
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

Schritt 29: Öffnen Sie Cisco Secure Client auf dem Ubuntu-Client, und stellen Sie eine Verbindung zwischen VPN und demo.example.com her.

		Cisco Secure (Client		-		×
AnyCon	nect VPN	✓ Statistic	s 🕕	About			
		ıı ııı cısco	l i D				
Connect to:	demo.exa	ample.com			~		\$
Group:	posture_v	pn				`	-
Username:	isetest						
Password:	******						

🗞 Disco	onnect
Connected to demo.example.com.	

 $Ubuntu_Secure_Client_Verbunden$

Schritt 30: Öffnen Sie den Browser, um auf eine Website zuzugreifen, die die Umleitung zum ISE CPP-Portal auslöst. Laden Sie das Zertifikat vom ISE CPP-Portal herunter, und benennen Sie die Datei um in <Zertifikat>.crt. Dies ist ein Beispiel für die Verwendung von Firefox zum Herunterladen.



Ubuntu-Browser_CPP_Zertifizierung_Herunterladen

Schritt 30.1: Vertrauen Sie dem ISE CPP-Portalzertifikat auf dem Ubuntu-Client.

<#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.
```

Schritt 31: Klicken Sie Start auf das ISE CPP-Portal.

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

Schritt 32. Click here to download and install Agent.

Device Security Check ×	+	- 0	×						
\leftarrow \rightarrow C https:/	//demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL 🏠	\bigtriangledown	≡						
You must log in to this net	work before you can access the Internet.		\times						
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									
+ 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		Ď						

Ubuntu-Browser_CPP_Download_Status

Schritt 33: Öffnen Sie das Terminal auf dem Ubuntu-Client. Navigieren Sie zum Pfadhome/user/Downloads/, um das Statusmodul zu installieren.

<#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$
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.
```

Schritt 34: Beenden Sie auf der Benutzeroberfläche des Ubuntu-Clients den Cisco Secure Client, und öffnen Sie ihn erneut. Das ISE-Statusmodul wurde installiert und erfolgreich ausgeführt.



Ubuntu_Secure_Client_ISE_Posture_Installed

Schritt 35: Öffnen Sie das Terminal auf dem Ubuntu-Client. Navigieren Sie zu Pfad home/user/Desktop, und erstellen Sie eine Datei, um die auf der ISE konfigurierte Dateibedingung zu erfüllentest.txt.

<#root>

user@ubuntu22-desktop:~\$

cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Verbinden Sie VPN mit demo.example.com auf dem Ubuntu-Client.

	- • ×							
AnyCon	nect VPN	🗠 Statis	tics	🎯 ISE Posture	About			
cisco								
Connect to: demo.example.com								
Group: posture_vpn ~								
Username:	isetest							
Password:	00000000000							



 $Verify_Ubuntu_Secure_Client_Connected$

Schritt 2: Überprüfen Sie den Status des ISE-Status auf dem Ubuntu-Client.



Verify_Ubuntu_Secure_Client_Compliant

Schritt 3: Aktivieren Sie Radius Live Log auf ISE. Navigieren Sie zu Operations > RADIUS Live Log.

≡	disclosed in the services Engine		Opera	ations / RADIUS			Q & @ & A	
Щ	Live Logs Live Sessions							
::								
цц 0	Misconfigured Supplicants 🕕 Mi		configured Network Devices 🕕		RADIUS Drops		Client Stopped Responding 🕕	Repeat Counter ①
*	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

Schritt 4: Navigieren Sie über SSH oder Konsole zu FTD CLI.

<#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

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Informationen zum Statusablauf und zur Fehlerbehebung bei Cisco Secure Client und der ISE finden Sie in den CCO-<u>DokumentenISE-</u> <u>Statusstilvergleich für Vor- und Nachbereitung 2.2</u> und <u>Fehlerbehebung bei ISE-Sitzungsmanagement und -status.</u>

Zugehörige Informationen

<u>Kompatibilität der Cisco Identity Services Engine mit Netzwerkkomponenten, Version 3.3</u>

- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3
- <u>Technischer Support und Downloads von Cisco</u>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.