ISE 3.3を使用したLinux VPNポスチャの設定

内容	
<u>はじめに</u>	
<u>前提条件</u>	
<u>要件</u>	
<u>使用するコンポーネント</u>	
<u>設定</u>	
<u>ネットワーク図</u>	
<u>FMC/FTDでの設定</u>	
<u>ISEでの設定</u>	
<u>Ubuntuでの設定</u>	
<u>確認</u>	
<u>トラブルシュート</u>	
関連情報	

はじめに

このドキュメントでは、Identity Services Engine(ISE)およびFirepower Threat Defense(FTD)で Linux VPNポスチャを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Cisco Secure クライアント
- ・ Firepower Threat Defense(FTD)のリモートアクセスVPN
- Identity Services Engine (ISE)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Ubuntu 22.04
- ・ Cisco Secureクライアント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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

設定

ネットワーク図



トポロジ

FMC/FTDでの設定

ステップ1:クライアント、FTD、FMC、およびISE間の接続が正常に設定されました。as enroll.cisco.comは、リダイレクトのプローブを行うエンドポイントに使用されます(詳細について は、『ポスチャフローCCOドキュメント:2.2前後のISEポスチャスタイル比較』を参照してくださ い)。FTDでenroll.cisco.comへのトラフィックのルートが正しく設定されていることを確認します 。

ステップ2: <u>Cisco Software Download</u>からパッケージ名cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkgをダ ウンロードし、ダウンロードしたファイルのmd5チェックサムがCisco Software Downloadページと同じであることを確認して、ダ ウンロード後にファイルの状態が良好であることを確認します。

ステップ3: Objects > Object Management > VPN > Secure Client Fileに移動します。Add Secure Client Fileをクリックし、名前を入力 し、File Nameを参照して選択します。cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg、Secure Client Image inFile Typeドロップ ダウンリストを選択します。次にSaveをクリックします。

Firewall Management Objects / Object Management	t Center Overview Analysis Policie	s Devices Objects Integration		Deploy	Q 🔮 🕸 🛛 admin 🗸	ence SECURE
> Distinguished Name DNS Server Group	Secure Client File			Add Secure	Client File	
External Attributes File List	File objects represent files used for remote access V	PN policy configurations. They can contain Secure Client profile and image files.				
> 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	±911
Port PortList	linux_image	File Name:*		ux64-5.1.3.62-webdeploy-k9.pkg	Secure Client Image	1/1
Route Map > Security Intelligence		Cisco-secure-client-linux64-5.1.3.62-W	owse			
Sinkhole SLA Monitor		File Type:* Secure Client Image				
Time Kange Time Zone Tunnel Zone		Description:				
URL Variable Set						
VLAN Tag ~ VPN						
Certificate Map Custom Attribute Group Policy		Cano	cel Save			
IKEv1 IPsec Proposal IKEv1 Policy						
IKEv2 IPsec Proposal IKEv2 Policy Secure Client Custominatio						
Secure Client File				Displa	ying 1 - 4 of 4 rows IC < Page 1]of1>>IC

 $FMC_Upload_Secure_Client_{\prec} \rightarrow \rightarrow$

ステップ4: Objects > Object Management > Networkに移動します。

ステップ 4.1 : DNSサーバのオブジェクトを作成します。Add Objectをクリックし、名前と使用可能なDNS IPアドレスを入力しま す。をクリックします。Save

Firewall Management Objects / Object Management	Center Overview	Analysis Policie	es Devices Objects	Integration			Deploy	Q 🗳 🌣 😡 🛛 adm	in ~ dude SECURE
Distinguished Name DNS Server Group External Attributes File List	Network A network object represents	one or more IP address	ies. Network objects are used i	n various places, including acces	s control policies, network vari	iables, intrusion rules, identity rules	Add Network Add Ob s, network discovery rule Add Gn Add Gn	Q, Filter Opject Object oup	ed Objects
 FlexConfig Geolocation Interface 	Namo arry		New Network	Object		0	Value 0.0.0.0/0 ::/0	Type Overrid Group	• 1⊒ Q ≅ M
Key Chain Network	any-ipv4		Name		1		0.0.0/0	Network	¶aq ⊕ #8
			DNS_		J				
			Network Host F	ange Network	O FQDN				
					Cancel	ve			

 $FMC_Add_Object_DNS(オプション)$



注:ここで設定するDNSサーバは、VPNユーザ用です。

ステップ 4.2: ISE PSNのオブジェクトを作成します。Add Objectをクリックし、名前と使用可能なISE PSN IPアドレスを入力しま す。をクリックします。Save

Firewall Management Objects / Object Management	Center Overview Analysis	Policies Devices Objects Integration		Deploy	y Q 💕 🌣 🛛 admin	 dubi SECUR
> Distinguished Name	Network			Add Network	• Q, Filter	
DNS Server Group External Attributes File List FiexConfig Geolocation	A network object represents one or more IP	addresses. Network objects are used in various places, including acco	iss control policies, network variables, intrusion r	ules, identity rules, network discovery rule Im	Id Object Show Unused orts, and so on.	Objects
	Name			Value	Type Override	
Interface	any	New Network Object	0	0.0.0.0/0 ::/0	Group	14 Q 2 M
Key Chain	any-ipv4			0.0.0.0/0	Network	G Q ⊕ M
TECHNOR		Name	1			
		ISE_PSN_	J			
		Description				
			J			
		Network	0 5000			
		Host O Range O Network				
		Allow Overrides	-			
			Cancel Save			

 $FMC_Add_Object_ISE(オプション)$

ステップ 5: Objects > Object Management > VPN > Group Policyに移動します。をクリックします。Add Group PolicyDNS/WINSをク リックし、Primary DNS ServerでDNSサーバのオブジェクトを選択します。次にSaveをクリックします。

Firewall Managemen Objects / Object Managemen	nt Center Overview Analysis nt	Policies Devices Objects	Integration		Deploy Q 🚱 🌣 🕢 admin 🗸 📩 dada SECU	URE
Distinguished Name DNS Server Group	Group Policy			[Add Group Policy Q, Filter	
> External Attributes	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 as	signs the group policy or it is obtained	rom the current connection profile.	
File List						
> FlexConfig	Name					
Geolocation						
Interface	DfltGrpPolicy	Add Group Policy		0	/ 1	
Key Chain					/ 1	
Network		Name:*				
> ркі		posture_gp				
Policy List		Description:				
Port						
> Prefix List						
Route Map		General Secure	Client Advanced			
> Security Intelligence			Dimes DND Deser			
Sinkhole		VPN Protocols	DNS dever			
SLA Monitor		IP Address Pools	Diro,			
Time Kange		Banner	Secondary DNS Server:			
Time Zone		DNS/WINS	• +			
Tunnel Zone		Split Tunneling	Primary WINS Server:			
URL No.			· +			
Variable Set			Secondary WINS Server:			
			• +			
VPN			DHCP Network Scope:			
Certificate Map			• +			
Custom Attribute			Only network object with Ipv4 address is allowed (Ex: 10.72.3.5)			
Word Policy			Default Domain:			
KEVT Insec Proposal						
IVEV2 IReas Proposal						
IKEV2 Proc Proposal						
Secure Client Oustomizatio				_		
Secure Client File			Cancel		Displaying 1 - 2 of 2 rows $ \langle \langle Page 1 \rangle \rangle$ of 1 $>$ $ $	С

FMC_Add_Group_ポリシー



注:VPNグループポリシーで使用されるDNSサーバがISEクライアントプロビジョニングポータルのFQDNと enroll.cisco.comを解決できることを確認します。

手順 6: Objects > Object Management > Access List > Extendedに移動します。をクリックします。Add Extended Access List

Cirewall Manageme	nt Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🔕 admin 🗸 🖽 SECURE
 AAA Server RADIUS Server Group 	Extended	Add Extended Access List Q, Filter
Single Sign-on Server	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 addresses. You use these objects when configuring particular features, such as route maps.	sed on source and destination address and ports. Supports IPv4 and IPv6
Extended	Name Value	Override

FMC_追加_リダイレクト_ACL

ステップ 6.1: リダイレクトACLの名前を指定します。この名前は、ISE認可プロファイルと同じである必要があります。をクリックします。Add

New Exter	nded Aco	cess List Object							0
Name redirect									
2110100 (0)									Add
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
No record	s to display								
Allow Ov	errides								

*FMC*_追加_リダイレクト_*ACL*_パート_1

ステップ 6.2: DNSトラフィック、ISE PSN IPアドレスへのトラフィック、および修復サーバをブロックして、リダイレクトから 除外します。残りのトラフィックを許可します。これにより、リダイレクトがトリガーされます。をクリックします。Save

Cancel Save

Cancel

Action: Black Default Default Log leve: Informational Cog Interval: 300 Sec. Network Port Application Users Security Group Tag Available Networks C Gesterch by name or value IPv4-Private-1192.168.0.0-16 IPv4-Private-1192.168.0.0-16 IPv4-Private-1192.168.0.0-16 IPv4-Private-1192.168.0.0-16 IPv4-Private-11918 IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast IPv6-to-IPv4-Relay-Anycast	Add Extended Access List Entry				0
Default Log Level: Informational Constrained and an anti-action of the second and anti-action of the second anti-	Action: Block				
Log Level: Informational Sec. Network Port Application Users Sec. Available Networks C Available Networks C Add to Source Add to Source Add to Destination IPv6-IPv4-Mapped IPv6-IPv4-Mapped IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast IELPSN	Default				
Log Interval: 300 Sec. Network Port Application Users Security Group Tag Available Networks (° + Source Networks (0) Q Search by name or value IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-IPv4-Relay-Anycast IPv6-to-IPv4-Relay-Anycast ISE_PSN	Log Level: Informational				
Network Port Application Available Networks C Available Networks C C Source Networks (0) Destination Networks (1) IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Private-Unique-Local-Addresses IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast StepSN	Log Interval: 300 Sec.				
Available Networks C + Source Networks (0) Destination Networks (1) 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	Network Port (1) Application (1) Users	Security Group Tag			
Q. Search by name or value IPv4-Private-192.168.0.0-16 IPv4-Private-All-RFC1918 IPv6-IPv4-Mapped IPv6-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast	Available Networks C +		Source Networks (0)	Destination Networks (1)	
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	Q Search by name or value		any	ISE_PSN	Ì
IPv4-Private-AlI-RFC1918 Add to Destination IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast IPv6-to-IPv4-Relay-Anycast IPv6-to-IPv4-Relay-Anycast	IPv4-Private-192.168.0.0-16	Add to Source		L	
IPv6-IPv4-Mapped IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast ISE_PSN	IPv4-Private-All-RFC1918				
IPv6-Link-Local IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast ISE_PSN	IPv6-IPv4-Mapped				
IPv6-Private-Unique-Local-Addresses IPv6-to-IPv4-Relay-Anycast ISE_PSN	IPv6-Link-Local				
IPv6-to-IPv4-Relay-Anycast ISE_PSN_	IPv6-Private-Unique-Local-Addresses				
ISE_PSN_	IPv6-to-IPv4-Relay-Anycast				
	ISE_PSN_				
rtp_ise Enter an IP address Add Enter an IP address Add	rtp_ise		Enter an IP address Add	Enter an IP address	Add

*FMC*_追加_リダイレクト_*ACL*_パート_2

Name									
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	Απγ	Any	Any	11
3	Block	Any	Any	FTP	Any	Any	Any	Any	/1
4 Allow O	Allow verrides	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	/1

Cancel Save

FMC_追加_リダイレクト_ACL_パート_3



注:このリダイレクトACLの例では、宛先FTPが修復サーバの例として使用されています。

手順7: Objects > Object Management > RADIUS Server Groupに移動します。をクリックします。Add RADIUS Server Group

Firewall Management Objects / Object Management	Center Ove	erview Analysis	Policies Devices	Objects Integration	Deploy Q 🚱
V AAA Server RADIUS Server Group Single Sign-on Server	RADIUS Server Grou	rver Group	or more references to RA	DIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connection	Add RADIUS Server Group
Extended	Name			v	latue

 $FMC_Add_New_Radius_ therefore - therefor$

ステップ 7.1:名前、チェック、チェック、チェEnable authorize onlyックEnable interim account update、チェックEnable dynamic authorizationを指定します。

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

FMC_追加_新規_Radius_サーバ_グループ_パート_1

ステップ 7.2:新しいradiusサーバを追加するPlus アイコンをクリックします。ISE PSNを入力しIP Address/Hostname, Keyます。接 続するspecific interfaceを選択します。Redirect ACLを選択します。次に、をクリックSaveして新しいRADIUSサーバを保存します 。次にSaveを再度クリックして、新しいRADIUSサーバグループを保存します。

?

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 Before Cisco AV Pair ACL 	+	IP Address/Hostname:* Configure DNS at Threat Defense Platform Settings to resolve hostname Authentication Port:* (1-65535) 1812 Kev:* Confirm Key:* Accounting Port: (1-65535) 1813 Timeout: (1-300) Seconds 10	o
IP Address/Hostname		Connect using: Routing Specific Interface inside_zone Redirect ACL: redirect + 	
	Cancel Save	Cancel	Save

FMC_追加_新規_Radius_サーバ_グループ_パート_2

ステップ8: Objects > Object Management > Address Pools > IPv4 Poolsに移動します。Add IPv4 Poolsをクリックし、Name, IPv4 Address RangeおよびMaskを入力します。次にSaveをクリックします。

Firewall Managen Objects / Object Manage	ment Center Overview	Analysis Policies	Devices Ot	jects	Integration			Deploy Q	e o	fangn	i ~ circo SECURE
> AAA Server > Access List > Address Pools	IPv4 Pools	4 addresses, it is used for n	nanagement/diagnos	tic interfac	ce with clustering, or for VPN remote access profil	es.		Add IPv4 Poo	45 Q	Filtor	
BP44 Roois Pr46 Roois Pr46 Roois Application Fitens AS Path BFD Template Cipher Suite List DHCP IP46 Rooi Distinguished Name DHCP IP46 Rooi DHCP IP46 Rooi Potol Statemal Attibutes File List Precedent Actional Attibutes File List Precedent Actional Attibutes File List Precedent Actional Attibutes Precedent Actional Attibutes Prot Potor Security Intelligence Sinkhole Sinkhole Sinkhole Sinkhole	Name d posture_pool_97_0			Add II Name* postu Descrip IPv4 Ac 192.1 Format Mask* 255.2 Allic avoid multip b Ox	IPv4 Pool ture_pool ption ddress Range* .168.6.30-192.168.6.100 tt: ipaddr-ipaddr e.g., 10.72.1.1-10.72255.255.0 low Overrides figure device overrides in the address pool ob d IP address conflicts in case of object is shar liple devices bverride (0)	ject to red across	Cancel			Override O	/¥ /¥ /¥
Time Zone Tunnel Zone URL Variable Set								Displaying 1 -	2 of 2 row	s IC C Page	1of 1 > >1 C'

 $FMC_Add_New_7^{\circ}-JL$

ステップ 9: Certificate Objects > Object Management > PKI > Cert Enrollmentに移動します。Add Cert Enrollmentをクリックし、名前 を指定してSelf Signed Certificatein Enrollment Typeを選択します。Certificate Parametersタブをクリックし、Common Nameおよび Country Codeを入力します。次にSaveをクリックします。

Firewall Managemen Objects / Object Managemen	nt Center Overview Analysis Policies Devices	Objects Integration		Deploy Q 💕 🌣 🚱 fa	ngni 🗸 🔤 diala. SECURE
AAA Server Access List Address Pools Application Filters	Cert Enrollment A certificate enrollment object contains the Certification Authority (CA) of your Private Key Infrastructure (PKI).	server information and enrollment parameters t	that are required for creating Certificate Signing Requests (CSRs) and obtaining k	Add Cert Enrollment Q. Filter	hese activities occur in
AS Path BFD Template Cipther Suite List Community List DHCP IPv6 Pool DHCS Rever Group DHS Server Group DHS Server Group Sectional Attributes File List PREConfig Geslocation Interface Key Chain Network PRI Gent Enrollment External Corris Internal Corrups	Add Cert Enrollment Add Cert Enrollment Marre* Gemo_yon Description Enrollment Type: Self Signed Certificate Common Name (CK) is mandatory for self-signed certificate that is VPNL to configure (CK) presen marging to Exclinate arrameters' training to Cleant Certificate Parameters' training to Cleant Certificate Parameters' training to Continue the Parameters' training to Cleant Certificate Parameters' training to Cleant Certificate Parameters' training to Configure (CK) present Cleant Certificate Parameters' training to Cleant Certificate Parameters' training to Configure (CK) present Cleant Certificate Parameters' training to Configure (CK) present Cleant Certificate Parameters' training to Certificate Parameters' training to Configure (CK) present Cleant Certificate Parameters' training to Configure (CK) present Cleant Certificate Parameters' training to Certificate Parameters' training to Configure (CK) present Cleant Certificate Parameters' training to Certifica	used in Remote Access bb.	Add Cert Enrollment Name* demo_spn Description CA Information Certificate Parameters Key Revocation Include FQDN: Don't use FQDN in certificate * Include FQUN: Common Name (CR); Organization Unit (U); Organization (0): Locatly (L): State (ST); Eventer: For the forme (CR);	ryue Oren	100
Internal CA Groups Internal CAS Internal Cert Trusted CA Groups Trusted CA Groups Trusted CA Policy List Port Port Prefix List Route Map	Allow Overrides	Cancel Save	Enal (IC) Enal (Cancel Save Displaying 1 - 3 of 3 rows < < P	bga 1 of 1 > >1 C

FMC_Add_New_Cert_Enroll (登録ユーザのみ)

ステップ 10: Devices > Certificatesに移動します。Addをクリックし、DeviceでFTD名を選択し、Cert Enrollmentで以前に設定した 登録を選択します。をクリックします。Add

Firewall Manager	nent Center	Overview Analysis	Policies Devices	Objects Integration		Deploy Q 💕	🗘 🙆 🛛 fangni 🗸 🖓 disebs SECURE
Filter							Add
All Certificates	*						
Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status		
Add Now Cor	tificato			0			₽
Add New Cer	uncate			U I	G.CA LD		± 2 C T
Add a new certific	cate to the devi	ce using cert enr	ollment object which	is used to	O CA LD		± 2 C T
generate CA and	identify certifica	ate.	onnent object milen				₽
Device*:					O CA LD		± 2 C T
Posture-FTD-C	ML27						
Cert Enrollment*:							
demo_vpn		• +					
Cert Enrollment D	etails:						
Name:	demo_vp	n					
Enrollment Type:	Self-Sign	ed					
Enrollment URL:	N/A						
			Cancel	Add			

 $FMC_Add_New_Cert_To_FTD(\pi \forall \vartheta \exists)$

ステップ 11 Devices > VPN > Remote Accessに移動します。をクリックします。Add

ステップ 11.1:名前を入力し、FTDをSelected Devicesに追加します。をクリックします。Next

Firewall Management Center Overview Overview	Analysis Policies Devices Objects Integration		Deploy Q 💞 🌣 🔕 admin 🗸 🕬 SECURE
	Secure Client Access & Certificate Summary Secure Client Secure Client Summary Summary Deciption: Deciption: Deciption: Protocols: Secure Client Sec	Before You Start Before you start, ensure the following configuration elements to be inplace to complete Remote Access VPN Policy. Authentication Server Configure LOCAL or Healm or RADUS Server Oroup or SSO to authenticate VPN clients. Secure Client Package Make sure you have Secure Client package for VPN ciredentiats to download it during the witzart. Device Interface Interfaces should be already configured on targeted devices so that they can be used as a security zone interface group to enable VPN access.	
			Cancel Back Next

FMC_New_RAVPN_Wizard_1

ステップ 11.2: Authentication Server, Authorization Server, Accounting Serverで事前に設定したRADIUSサーバグループを選択します。ページを下にスクロールします。

Eirewall Management Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🕢 admin V 🔤
Remote Access VPN Policy Wizard	
1) Policy Assignment (2) Connection Profile (3) Secure Client (4) Access & Certificate (5) Summary	
Client Address Assignment:	
erieri enerieri enerieri energi (1719/18). Miane IV addessa ana ka asstanza danu 2.8.8 aanus 168M saanus and IV addessa asabu Ulkun suubista asstana ass	
	Cancel Back Next

 $FMC_New_RAVPN_Wizard_2$

ステップ 11.3: IPv4 Address Poolsで以前に設定したプール名を選択し、Group Policyで以前に設定したグループポリシーを選択します。Nextをクリックします。

Periode Access VPN Policy Witzard Policy Assignment <	Firewall Management Center Overview Analysis Policies	Devices Objects Integration	Deploy Q 🚱 🔅 🕢 admin 🗸 👶 SECURE
Policy Assignment Policy Policy Policy Assignment Policy Assignment Policy Policy Assignment Policy Policy Assignment Policy	Remote Access VPN Policy Wizard		
• Policy Assignment • Policy Assignment • Access & Cerriticate • () Policy Assignment • () Policy Policy () • () Policy () Policy () Policy () <p< td=""><td></td><td></td><td></td></p<>			
The main or RADUS Accounting Server: Ippice (IAADUS) Client Address Assignment: Client Padress 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 pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pools. When multiple options are selected, IP address pools. When multiple options are selected. IP address Pools. Up to PLCP Server and IP address pools. When multiple options are selected. IP address Pools. Use DAA Server (Reation or RADUS only) Use DAA Server (Reation or RADUS only) Use DAA Server (Reation or GADUS only) Use DAA Address Pools: Prof Address Pools: Prof Address Pool: Comp Policy: A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Selected opticy object. Group Policy: Destrem_sep Edit Group Policy:	Onnection Profile 3 Secure Client	Access & Certificate 5 Summary	
Accounting Server: Implies + Client Address Assignment: Ities assignment from AAA server, DHCP server and IP address pools. When multiple options are selected, P address assignment is trie in the order of AAA server, DHCP server and IP address pools. Is be abade set of the address assignment is trie in the order of AAA server, DHCP server and IP address pools. Is be abade set of the address assignment is trie in the order of AAA server, DHCP server and IP address pools. Is be DHCP Server: Is be DHCP Server: IP we Address Pools: Implies		(Realm or RADIUS)	
Client dAdress Assignment: Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address scale more assigned from AAA server, DHCP server and IP address pool. Use AAA Server (Realm or RADIUS only) • Use DHCP Servers Use IP Address Pools: IPv% Addre		Accounting Server: rtpise +	
Client Address Assignment: Client (P address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address Asserver, DHCP server and IP address pool. U las AAA server (Realm or RADIUS only) U be DHCP Servers V Use IP Address Pools: IPv4 Address Pools: IPv4 Address Pools: IPv4 Address Pools: IPv6 Address Pools		(RADIUS)	
Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address approximation is thread in the order of AAA server, DHCP server and IP address pool. Use AAA Server (Beatim or RADIUS only) ● Use DHCP Servers Use IP Address Pools IPv4 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6		Client Address Assignment:	
Use AAA Server (Realm or RADUS only) ● Use DHCP Servers ♥ Use PAA defress Pools ₩v4 Address Pools ₩v4 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: Ectit Group Policy:		Clent 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 DHCP Servers Use IP Address Pools IPv4 Address Pools IPv4 Address Pools IPv6 Address		Use AAA Server (Realm or RADIUS only)	
If Use IP Address Pools IPv4 Address Pools 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: Left Group Policy: Edit Group Policy		Use DHCP Servers	
IPv4 Address Pools:		Vise IP Address Pools	
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: Edit Group Policy: Edit Group Policy		IPv4 Address Pools: posture_pool	
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: Edit Group Policy: Edit Group Policy		IPv6 Address Pools:	
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 Edit Group Policy		Group Policy:	
Group Policy:* posture_ap + Edit 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.	
Edit Group Policy		Group Policy:* posture_gp +	
		Edit Group Policy	

Cancel Back Next

FMC_New_RAVPN_Wizard_3(推奨)

ステップ 11.4 : Linuxイメージのチェックボックスをオンにします。をクリックします。Next

Firewall Management Center Overview Analysis	Policies Devices Objects In	rtegration		Deploy	۹	¢ 9	admin	 slude SECURE
Remote Access VPN Policy Wizard								
Remote Access VFIV Folicy Wizard								
1 Policy Assignment (2) Connection Profile (3) Secure Cl	ient 4 Access & Certificate -	5 Summary						
	Remote Secure Client -	Outside Vpr	hside Corporate Pe Resources					
			9					
	Secure Client Image							
	The VPN gateway can automatically d connection is initiated. Minimize connect	ownload the latest Secure Client package to ion setup time by choosing the appropriate OS for	the client device when the VPN in the selected package.					
	Download Secure Client packages from	Cisco Software Download Center.						
			Show Re-order buttons +					
	Secure Client File Object Name	Secure Client Package Name	Operating System					
	client_image	cisco-secure-client-win-5.1.3.62-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(推奨)

ステップ 11.5:VPNインターフェイスのインターフェイスを選択します。ステップ9でFTDに登録した証明書の登録を選択します 。をクリックします。Next

Firewall 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	Access & Certificate S Summary	
Remote User	Secure Clent Outside UNA Cleases	
	Enable DTLS on member interfaces	
	All the devices must have interfaces as part of the Interface Group/Security Zone selected.	
	Device Certificates	
	Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.	
	Certificate Enrollment:*	
	Enroll the selected certificate object on the target devices	
	Access Control for VPN Traffic	
	All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.	
	Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)	

Cancel Back Next

FMC_New_RAVPN_Wizard_5

ステップ 11.6:サマリーページで関連情報を再度確認します。問題がなければ、Finishをクリックします。変更する必要がある場合は、Backをクリックします。



FMC_New_RAVPN_Wizard_6(推奨)

ステップ 12新しい設定をFTDに展開して、リモートアクセスVPNの設定を完了します。

Firewall Management Center Devices / VPN / Edit Connection Profile Overview Analysis	Policies Devices Objects Integration		Deploy Q. 🚱	C O admin ~ duda SECURE
posture_vpn			Q Advanced Deploy	pre warnings Deploy Cancel
hoarna rear			Posture-FTD-CML27	eady for Deployment ents.(1)
Connection Profile Access Interfaces Advanced				ty: None
Namo	АЛА	Group Policy		
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy		
posture_vpn	Authentication: rtpise (RADIUS) Authorization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	E posture_gp	1 selected 0 1 pending	2.0

FMC_Deploy_FTD

ISEでの設定

ステップ 13 Work Centers > Posture > Network Devicesに移動します。をクリックします。Add

=	dentity Services I	Engine					Work Centers	Posture				C	2 &	0	۹ ۱	۹
Щ	Bookmarks	Overview	Network De	vices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings					
	Dashboard															
명	Context Visibility	Net	Network Devices													
×	Operations												Selected	0 Total	4 0	۵
U	Policy	Ø Edit	+ Add	Duplicate	🕁 Import 🖒 Export	V 👌 Generate PAC	🛿 Delete 🗸								All 🗸	V
80	Administration		Name \land	IP/Mask	Profile Name	Location	Туре		Description							
3.	Work Centers	0	FTD-CML2		🖦 🗰 Cisco 🕕	All Locations	Firewall									
<u> </u>		0	FTD-CML2	-	🟥 Cisco 🕕	All Locations	Firewall									
(?)	Interactive Help		FTD+CML2		# Cisco 🛈	All Locations	Firewall									
			8.000	10.14	🖆 Cisco 🕕	All Locations	Firewall									

ISE_Add_New_デバイス

ステップ 13.1: Name, IP Addressコマンドを入力し、ページを下にスクロールします。

=	diale Identity Se	ervices Engine				w	ork Centers / I	Posture		
н	Overview	Network Devices	Client Provisioning	Poli	cy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
5	Network Dev	rices List > New Network D	evice							
16 16	Network	Devices								
×.	Name	posture-FTD		_						
ж	Descripti	on		_						
	:: IP	Address 🗸 * IP :	····· / 32		©					
?										
	Device Pr	rofile 👬 Cisco	~	()						
	Model Na	ame	~	_						
	Software	Version	~	_						
	Network	Device Group								
	Location	All Locations		~	Set To Default					
	IPSEC	Is IPSEC Devic	e	~	Set To Default					

ISE_Add_New_Devices_1

ステップ 13.2: RADIUS Authentication Settingsのチェックボックスをオンにします。Shared Secretを入力します。をクリックしま す。Submit

=	dentity Services	Engine					۷	Vork Centers / P	osture		۹ ۵ ۵ ۵ ۷	
щ	Bookmarks	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
=:	Dashboard		~ RADIUS Authent	tication Settings								
ьq	Context Visibility		RADIUS UDP Setting	5								
$^{\rm H}$	Operations		Protocol RA	DIUS								
0	Policy		Shared Secret		Show							
8.	Administration		Use Second Shared	Secret ()								
đ	Work Centers		Secor	nd Shared		Show						
۲	Internetive Male		CoA Port 1	700	Set To Defa	un						
	interactive Help		RADIUS DTLS Setting	gs 🕡								
			DTLS Required ()									
			Shared Secret rad	lius/dtls								
			CoA Port 2	083	Set To Defa	uit .						
			Issuer CA of ISE Certificates for CoA 5	ielect if required (optional)	~ 0							
			DNS Name									
			General Settings									
			🗌 Enable KeyWrap 💿)								
			Key Encryption Key		Show							
			Message Authenticator Code		Show							
			Key Insuit Encode									
			O ASCII O HEXA	DECIMAL								
			TACACS Author Author	tication Settings								
			 SNMP Settings 									
			 Advanced Trust 	Sec Settings								
											Submit	

ISE_Add_New_Devices_2

ステップ 14: <u>Cisco Software Download</u>からパッケージ名cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkgをダウ

ンロードし、ダウンロードしたファイルのmd5チェックサムが<u>Cisco Software Download page</u>と同じであることを確認して、ファイ ルの状態が良好であることを確認します。 パッケージ名cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkgは手順1で正常にダウン ロードされました。

ステップ 15: Work Centers > Posture > Client Provisioning > Resourcesに移動します。をクリックします。AddAgent resources from local diskを選択します。

≡	disclosed Identity Services Engine			Wo	rk Centers /	/ Posture			
Щ	Overview Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
== 18 ×	Client Provisioning Policy Resources Client Provisioning Portal	Resources	🚺 Duplicate 👘 Del	ete				Selec	cted 0 Total 16 🕃 All \lor ∇
Ψ.		Agent reso	ources from Cisco site		т	ype 🗸	Version	Last Update	Description
-0		Agent reso	ources from local disk		١	WinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Pro
-fili		Native Sup	plicant Profile		1	Native Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configurec
		Agent Con	figuration		1	Native Supplicant Pro	Not Applic	2023/07/04 07:55:16	Pre-configurec
?		Agent Pos	ture Profile		,	MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Prov
		AMP Enabl	ler Profile	5.1.3.062	(CiscoSecureClientDe	5.1.3.62	2024/05/08 10:20:06	Cisco Secure (
		CiscoSecure	ClientDesktopLinux 5.1	.3.062	(CiscoSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure (
		CiscoSecure	ClientComplianceModul	leWindows 4.3.4015.819	2 (CiscoSecureClientCo	4.3.4015	2024/05/08 10:26:57	Cisco Secure (
		CiscoSecure	ClientComplianceModul	leLinux 4.3.3139.0	(CiscoSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure (
		CiscoAgenti	essWindows 5.0.03061		(CiscoAgentlessWind	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
		CiscoAgenti	essOSX 5.0.03061		(CiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
		CiscoTempo	ralAgentWindows 5.0.03	3061	(CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
		CiscoTempo	ralAgentOSX 5.0.03061		(CiscoTemporalAgent	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE_Upload_Resource

ステップ 15.1: Cisco Provided Packageを選択します。Choose Fileをクリックして、cisco-secure-client-linux64-5.1.3.62-webdeployk9.pkgをアップロードします。をクリックします。Submit

≡	ahada Identity Services E	ngine		Work Centers / Posture	Q	۵	0	Q	8
月 日 同 火	Bookmarks Dashboard Context Visibility Operations	Client Provisioning Policy Resources Client Provisioning Portal	Agent Resources From Local I	Disk. > Agent Resources From Local Disk. m Local Disk.					
0 10 5	Policy Administration Work Centers		Category	Cisco Provided Package					
				Vagent Uploaded Resources Name Type Version Description CiscoSecureClientDesktopLi CiscoSecureClientDe 5.1.3.62 Cisco Secure Client for Ii					
			Submit	ancel					



注:ステップ14を繰り返して、cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkgをアップロードします。

ステップ 16: Work Centers > Posture > Client Provisioning > Resourcesに移動します。をクリックします。AddAgent Posture Profileを 選択します。

≡ :	isco Identity	Services Engine				Work Cent	ers / Posture		
Щ	Overview	Network Devices	Client Prov	risioning Policy Elements	Posture Policy	Policy	Sets Troubleshoo	t Reports Settin	ngs
	Client Provisi Resources	oning Policy	Reso	urces					
×	Client Provisi	oning Portal	D call	Late a Disease Bio					Selected 0 Total 16 🔗
0			Ean -	+ vag v () poblicate () p	oieto				All \checkmark Y
80				Agent resources from Cisco site	2	Version	Last Update	Description	
				Agent resources from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for Ii	
- mill				Native Supplicant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:01:12	Pre-configured Native S	
				Agent Configuration	oSecureClientCo	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu	
?				Agent Posture Profile	ntProfile	Not Applic	2024/05/08 10:37:17		
				AMP Enabler Profile	ntProfile	Not Applic	2024/05/16 15:15:49		

ISE_Add_Agent_Posture_プロファイル

ステップ 16.1: Name, Server name rulesを指定し、その他はデフォルトのままにします。をクリックします。Save

名前: linux_agent_profile

サーバー名の規則: *.example.com

≡ :	isco Identity	dentity Services Engine Work Centers / Posture									
Щ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings		
111 12 12 14 14 14 14 14 	Client Provis Resources Client Provis	ioning Policy	ISE Posture Agent Profile Set Agent Posture Profil Name * linux_agent_profile Description:	e							
?			Parameter		Value	D	escription				
			Enable debug log		No V	E	nables the debug log	on the agent			

*ISE_*追加_エージェント_ポスチャ_プロファイル_1

≣	dentity	Services Engine			w	ork Centers / F	Posture			
IJ	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
<u>ار</u>	Client Provis Resources	ioning Policy	Posture Protocol							
×	Client Provis	ioning Portal	Parameter	Value			Description			
0			PRA retransmission ti	me 120	secs		This is the age communication	nt retry period n failure	if there is a Passive Reassessment	
R _o			Retransmission Delay	(i) 60	secs		Time (in secon	ids) to wait bef	fore retrying.	
สีเ			Retransmission Limit	① <u>4</u>			Number of retr	ies allowed for	r a message.	
?			Discovery host ()				Enter any IP ad detects and re portal.	ddress or FQDN directs that htt	N that is routed through a NAD. The NAD op traffic to the Client Provisioning)
			Discovery Backup Ser	ver List Choose	9		By default, An PSNs sequenti as the backup discovery prob	yConnect send ally if the PSN list and restrict ses.	is discovery probes to all the Cisco ISE is unreachable. Choose specific PSNs t the nodes to which AnyConnect sends	5
			Server name rules * () •.examp	ole.com		A list of wildca servers that th	irded, comma- e agent can co	separated names that defines the onnect to. E.g. "*.cisco.com"	
			Call Home List 🕕				A list of IP add that the agent endpoint does	iresses, that de will try to conn n't respond for	efines the all the Policy service nodes nect to if the PSN that authenticated the some reason.	9
			Back-off Timer ①	30	secs		Agent will con targets and pr packets till this	tinuously try to eviously conne s max time limit	reach discovery targets (redirection cted PSNs) by sending the discovery it is reached	
									Cancel Save	

*ISE*_追加_エージェント_ポスチャ_プロファイル_2

ステップ 17: Work Centers > Posture > Client Provisioning > Resourcesに移動します。をクリックします。AddAgent Configurationを 選択します。

= :	Identity Services En	gine				Work Cent	ers / Posture				
щ	Overview Network De	vices Client P	rovisioning	Policy Elements	Posture Policy	Policy S	Sets Trouble	eshoot Reports	Settings		
1-0 1-0	Client Provisioning Policy Resources	Res	ources								
×	Client Provisioning Portal									Selected 0 Total 16	C
		0 Edit	+ Add 🔿 🛛 🕻) Duplicate 🛛 🖨 Del	lete					All 😒	7
			Agent resource	es from Cisco site	3	Version	Last Update	Description			
H 0		0	Agent resource	es from local disk	oSecureClientDe	5.1.3.62	2024/05/08 10:3	31:28 Cisco Secure C	lient for li		ī
-fli			Native Supplie	ant Profile	ve Supplicant Pro	Not Applic	2016/10/07 04:0	01:12 Pre-configured	Native S		1
			Agent Configu	iration	oSecureClientCo	4.3.3139.0	2024/05/08 10:3	34:00 Cisco Secure C	lient Linu		1
?			Agent Posture	Profile	ntProfile	Not Applic	2024/05/08 10:3	37:17			1
			AMP Enabler	Profile	ntProfile	Not Applic	2024/05/16 15:1	5:49			1

ISE_Add_Agent_設定

ステップ 17.2:詳細を設定します。

エージェントパッケージの選択: CiscoSecureClientDesktopLinux 5.1.3.062

名前: linux_agent_config

コンプライアンスモジュール: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

チェックボックスをオンにする VPN, Diagnostic and Reporting Tool

をクリックします。Submit

≡ :	dentity	Services Engine		Work Cent	Work Centers / Posture				
JI.	Overview	Network Devices	Client Provisioning	Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings
	Overview Client Provis Client Provis	Network Devices	Client Provisioning * Select Agent Package: * Configuration Name: Inux_agent_config Description: Description Cisco Secure Client ISE Posture	Policy Elements	Posture Policy scoSecureClientDesktopLin	Policy Sets	Troubleshoot	Reports	Settings
			Secure Firewall Dosture Network Visibility Diagnostic and Reporting Tool Profile Selection * ISE Posture linux_ager	t_profile	×			St	ibmit Canc

ISE_Add_Agent_Configuration_1

ステップ 18: Work Centers > Posture > Client Provisioning > Client Provisioning Policyに移動します。ルール名の最後にあるEdit をク リックします。Insert new policy belowを選択します。

= -	dentity	Services Engin	e								v	Nork Ce	enters / Postu	ure						
щ	Overview	Network Devic	es C	lient Prov	sioning Poli	cy Element	ts	Posture Policy		Policy Sets	Trou	bleshoot	t Reports	Setti	ngs					
10 10 10 10 10 10	Client Provi Resources Client Provi	sioning Policy		Client Define the Cl for Agent Co for Native Su Vindows Age noted architect for Windows Mac ARM64 I f you configu vithout an Af	Provisioning Pe nfiguration: version pplicant Configurati ent, Mac Agent, Mac Agent ARM64 policiosi Agent ARM64 policiosi oolicios require no 0 re an ARM64 client RM64 condition. Thi	ing Po licy to determ of agent, age on: wizard pr : Temporal ar run the same ies, configure Other Conditi Uther Conditioning s is because	nine ent p rofile pac e Ser ons a polic an e	what users will receiv profile, agent complian a and/or wizard. Drag i fac Agentless policies kage for both architec ssion: OS-Architectur arm64 configurations. cy for an OS, ensure ti andpoint is matched se	ne up nce r and sup cture e EC hat t	con login and use module, and/or aç drop rules to chan port ARM64. Winn is. 2UALS arm64 in ti the ARM64 policy entially with the po	r session gent cus nge the dows po he Othe r is at the olicies lis	n initiation stomizatior order. plicies run r Conditio e top of th sted in this	: package. separate package ns column. he conditions list, s window.	es for ARM ahead of	44 and policies					
				~																
?					Rule Name		1	Identity Groups		Operating Syste	ems		Other Condition	s			Result	s		
				8 🖂	IOS		H A	Any a	nd	Apple IOS All		and	Condition(s)			then	Cisco-I	SE-NSP	Edit 😔	
				8 🖂	Android		H a	Any a	nd	Android		and	Condition(s)			then	Cisco-I	SE-NSP	Edit	
																	ſ	Duplicate above Duplicate below Insert new policy ab	ove	

Delete

ポリシー

ステップ 18.1 : 詳細を設定します。

ルール名: Linux

オペレーティングシステム: すべてLinux

結果: linux_agent_config

Done およびSaveをクリックします。

	dentity Services Engine		Work Centers / Posture	
Ц	Overview Network Devices	Client Provisioning Policy Elements Posture Polic	y Policy Sets Troubleshoot Reports Settings	
三 同 火 し あ	Client Provisioning Policy Resources Client Provisioning Portal	Client Provisioning Policy Define the Client Provisioning Policy to determine what users will rec For Agent Configuration: version of agent, agent profile, agent comp For Native Supplicant Configuration: wizard profile and/or wizard. Dr Windows Agent, Mac Agent, Mac Temporal and Mac Agentless polic Intel architectures. Mac policies run the same package for both arch For Windows Agent ARM64 policies, configure Session: OS-Archite Mac ARM64 policies require on Other Conditions arm64 configuration theore and ARM64 cellient provisioning policy for an OS, ensu- tion of the 4 cendities. The interpret age and refut to rest the	telve upon login and user session initiation: liance module, and/or agent customization package. ag and drop rules to change the order. ies support ARM64, Windows policies run separate packages for ARM4 and tectures. ture EQUALS arm64 in the Other Conditions column. ns. re that the ARM64 policy is at the top of the conditions list, ahead of policies.	
0		Rule Name Identity Groups II IOS If Any II Android If Any II Linux If Any	and Apple IOS All and Condition(s) and Android and Condition(s) and Linux All and Condition(s)	Results then Cisco-ISE-NSP Edit then Cisco-ISE-NSP Edit then Iinux_agent_config Edit

ISE_Add_New_Provisioning_Policy_1

=	dealer Identity Services Engine	Work Centers / Posture	
н	Overview Network Devices	Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings	
11 13 X	Conditions V Anti-Malware Anti-Spyware Anti-Virus	File Conditions Q. Vew	Selected 0 Total 385 🥥 🔕
Ĩ	Application	Name Description File name Condition Type	
40	Dictionary Compound	pc_XP64_KII2797052_M513 Cisco Predefined Check: SYSTEM_PROGRAMS\C Cisco-Defined	8
កា	Dictionary Simple	pc_W8_64_KB3124275_MS Cisco Predefined Check: SYSTEM_ROOT(sysnativ Cisco-Defined	
	Disk Encryption External DataSource	pc_Vista_K02893294_MS13 Clsco Predefined Check: SYSTEM_32\Imagehip.dll Clsco-Defined	
?	File	pc_W81_64_K83033889_M Cisco Predefined Check: SYSTEM_ROOT/sysnativ Cisco-Defined	
	Firewall	pc_Vista64_KB925902_MS0 Cisco Predefined Check: SYSTEM_ROOT/winsxs\a Cisco-Defined	
	Patch Management	pc_W10_64_1709_KB45803 Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Registry	pc_XP_K82653956_M512-0 Clsco Predefined Check: SYSTEM_32\Wintrust.dll Clsco-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	
	030	pc_W7_K82681578_MS12 Cisco Predefined Check: SYSTEM_32\Win32k.sys Cisco-Defined	
	Remediations >	pc_W10_KB3081436_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	ps_W8_64_KB2727528_MS Cisco Predefined Check: SYSTEM_ROOT\sysnativ Cisco-Defined	
	Authorization Profiles	pc_W8_64_K82092611_MS Clsco Predefined Check: SYSTEM_ROOT\sysnativ Clsco-Defined	
	Downloadable ACLs	pc_W7_K03078601_MS15 Cisco Predefined Check: SYSTEM_32(Win32k.sys Cisco-Defined	

ISE_Add_New_File_条件

名前: linux_demo_file_exist

オペレーティングシステム: すべてLinux

ファイルの種類: FileExistence

ファイルパス:home、Desktop/test.txt

ファイル演算子:存在します

をクリックします。Submit

=	diale Identity Services Engine				Work Cen	ters / Post	ture	5 5
н	Overview Network Devices	Client Provisioning Policy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings	
	Conditions v Anti-Malware Anti-Spyware Anti-Vilus Application Compound Dictionary Compound Dictionary Simple Diste Encryption External DistaSource File Firemal: Hardware Attributes Patch Management Benitry	File Conditions List > New File Condition File Condition Name *	 	iest.txt	<u></u>			
	Script Service USB						Submit	Cancel
	Requirements > Allowed Protocols . Authorization Profiles . Downloadable ACLs .							

ISE_Add_New_File_Condition_1

ステップ 20: Work Centers > Posture > Policy Elements > Requirementsに移動します。ルール名の最後にあるEdit をクリックします。 。Insert new Requirementを選択します。

=	dentity Services E	Engine							Work	Centers / P	osture					
н	Bookmarks	Overview	Network Devices	Client Provisioning	Policy	/ Elements	Posture	Policy Policy Sets	Tro	ubleshoot	Reports 5	settings				
	Dashboard Context Visibility	Conditions Anti-Make	v sare									Guide Me				
×	Operations	Anti-Spyr	ware	Requirements												
0	Policy	Applicatio	s an	Name		Operating Sys	tem	Compliance Module		Posture Type	•	Conditions		Remediations Actions		
a .,	Administration	Compoun	d	Any_AV_Installation_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_inst	then	Message Text Only	Edit 🖂	
	West Control	Dictionary	Compound	Any_AV_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_av_win_def	then	AnyAVDefRemediation/Win	Edit	Duplicate
nili	Work Centers	Dictionary	y Simple	Any_AS_Installation_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_inst	then	Message Text Only	Edit	Insert new
		External D	yption JataSource	Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit	Delete
(?)	Interactive Help	File		Any_AV_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_inst	then	Message Text Only	Edit 🗵	1
		Firewall		Any_AV_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_av_mac_def	then	AnyAVDefRemediationMac	Edit 🤟	
		Hardware	Attributes	Any_AS_Installation_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_inst	then	Message Text Only	Edit 🤟	
		Patch Mar	nagement	Any_AS_Definition_Mac	for	Mac OSX	using	3.x or earlier	using	Agent	met if	ANY_as_mac_def	then	AnyASDefRemediationMac	Edit 🛩	
		Script		Any_AM_installation_Wir	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_inst	then	Message Text Only	Edit 🗵	
		Service		Any_AM_Definition_Win	for	Windows All	using	4.x or later	using	Agent	met if	ANY_am_win_def	then	AnyAMDerRemediationWin	Edit 🛩	
		USB		Any_AM_Installation_Ma	c for	Mac OSX	using	4.x or later	gnieu	Agent	met if	ANY_am_mac_inst	then	Message Text Only	Edit 😔	
				Any_AM_Definition_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	ANY_am_mac_def	then	AnyAMDefRemediationMac	Edit 👻	
		Remediation	•	Any_AM_Installation_Un	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_inst	then	Select Remediations	Edit 😔	
		Requirement	15	Any_AM_Definition_Lin	for	Linux All	using	4.x or later	using	Agent	met if	ANY_am_lin_def	then	Select Remediations	Edit 9	
		Allowed Prot	tocols	USB_Block	for	Windows All	using	4.x or later	using	Agent	met if	USB_Check	then	USB_Block	Edit 😔	
		Authorization	e ACLs	Default_AppVis_Requirer ent_Win	n for	Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Win	then	Select Remediations	Edit 🤟	
				Default_AppVis_Requirer ent_Mac	n for	Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_Co ndition_Mac	then	Select Remediations	Edit 👻	
				Default_Hardware_Attrib es_Requirement_Win	ut for	Windows All	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 😔	
				Default_Hardware_Attrib es_Requirement_Mac	ut for	Mac OSX	using	4.x or later	using	Agent	met if	Hardware_Attribute s_Check	then	Select Remediations	Edit 👻	

ISE_Add_New_Posture_Requirement

ステップ 20.1: 詳細を設定します。

名前: Test_exist_linux

オペレーティングシステム: すべてLinux

コンプライアンスモジュール:4.x以降

ポスチャタイプ: Agent

条件: linux_demo_file_exist

Done およびSaveをクリックします。

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

ISE_Add_New_Posture_Requirement_1



注:現時点では、修復機能としてLinuxエージェント用のシェルスクリプトのみがサポートされています。

ステップ 21: Work Centers > Posture > Policy Elements > Authorization Profilesに移動します。をクリックします。Add

ステップ 21.1: 詳細を設定します。

名前: unknown_redirect

チェックボックスをオンにする Web Redirection(CWA,MDM,NSP,CPP)

選択 Client Provisioning(Posture)

ACL: リダイレクト

値:クライアントプロビジョニングポータル(デフォルト)

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

 $ISE_Add_New_Authorization_$ プロファイル_リダイレクト_1



注:このACL名リダイレクトは、FTDで設定された対応するACL名と一致する必要があります。

ステップ 21.2: Add を繰り返し、詳細を含む、準拠していないエンドポイントと準拠しているエンドポイント用に別の2つの認可 プロファイルを作成します。

名前: non_compliant_profile

DACL名:DENY_ALL_IPv4_TRAFFIC

名前: compliant_profile

DACL名:PERMIT_ALL_IPv4_TRAFFIC



注:準拠または非準拠エンドポイントのDACLは、実際の要件に従って設定する必要があります。

ステップ 22: Work Centers > Posture > Posture Policyに移動します。ルールの最後にあるEdit をクリックします。Insert new policyを 選択します。

=	deale Identity Services I	Engine							Work Centers	/ Por	iture					Q	۵	0	٩	15
н	Bookmarks	Overview	v Ne	twork Devices	Client Provisioning P	Policy Elements	Posture Policy	Policy Se	ts Troubleshoo		Reports Settings									
	Dashboard					L														
N	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.										2			0
U	Policy		~																	
1.	Administration		Status	Policy Options	Rule Name	Identity Groups	Operating	Systems	Compliance Module		Posture Type	Other Conditions		Requirements	_					
3	Work Centers			Policy Options	Default_AntiMalware_Policy_Ma c	if Any	and Mac OSX	80	4.x or later	and	Agent	and	the	 Any_AM_Installation_Ma c 	Edit 🛩					
				Policy Options	Default_AntiMalware_Policy_Ma c_temporal	ii Any	and Mac OSK	an	4.x or later	and	Temporal Agent	and		Any_AM_installation_Ma	Duplicate Edit					
1	Interactive Help			Policy Options	Default_AntiMalware_Policy_Wi	ii Any	and Windows A	i in	4.x or later	and	Agent	and	the	Any_AM_Installation_Wi	Edit Centre					
				Policy Options	n Default_AntiMalware_Policy_Wi	ii Aey	and Windows A		4.x or later	and	Temporal Agent	and	ite	n Any_AM_Installation_Wi	Edt v					
				Balley Desires	n_temporal	i ku	and March 1977		dia mentana		in an			n_temporal						
			0	Pointy Options	Changed and Long Long		in marcan			-				ment_Mac	EOI ~					
				Policy Options	Default_AppVis_Policy_Mac_te mporal	if Any	and Mac OSK	and	4.x.or later	and	Temporal Agent	and	0.6	 Default_AppVis_Require ment_Mac_temporal 	Edit 🗸					
				Policy Options	Default_AppVis_Policy_Win	ii Any	and Windows A		4.x or later	and	Agent	and	the	Default_AppVIs_Require mont_Wis	Edt v					
				Policy Options	Default_AppVis_Policy_Win_te mporal	ii Any	and Windows A	an an	4.x or later	and	Temporal Agent	and	the	Default_AppVis_Require ment_Win_temporal	Edit 9					
				Policy Options	Default_Firewall_Policy_Mac	ir Any	and Mac OSK	80	4.x or later	and	Agent	and	114	Default_Firewall_Require ment_Mac	Edt v					
				Policy Options	Default_Firewall_Policy_Mac_te mporal	ii Any	and Mac OSX	in the	4.x or later	and	Temporal Agent	and	110	Default_Firewall_Require ment_Mac_temporal	Edit					
				Policy Options	Default_Firewall_Policy_Win	ir Any	and Windows A	an an	4.x or later	and	Agent	and	the	Default_Firewall_Require ment_Win	Edit v					
				Policy Options	Default_Firewall_Policy_Win_temporal	ir Any	and Windows A	an an	4.x or later	and	Temporal Agent	and	the	Default_Firewall_Require ment_Win_temporal	Edit v					
				Policy Options	Default_Hardware_Attributes_P olicy_Mac	ii Any	and Med OSK	and a	4.x or later	and	Agent	and	the	Default_Hardware_Attrib utes_Requirement_Mac	Edit v					
				Policy Options	Default_Hardware_Attributes_P olicy_Mac_temporal	ii Any	and Mac OSK	an	4.x or later	and	Temporal Agent	and	the	Default_Handware_Attrib utes_Requirement_Mac_ temporal	Edt v					
				Policy Options	Default_Hardware_Attributes_P olicy_Win	ii Any	and Windows A		4.x or later	and	Agent	and	- 14	Default_Hardware_Attrib utes_Requirement_Win	Edit 9					
			-	A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.	A.A.A. MILALIN MILALIN A		il waite a		· · · · · · · · · · · · · · · · · · ·		******									

 $ISE_Add_New_Posture_ポリシ-$

ステップ 22.1: 詳細を設定します。

ルール名:Demo_test_exist_linux

IDグループ:任意

オペレーティングシステム: すべてLinux

コンプライアンスモジュール:4.x以降

ポスチャタイプ: Agent

要件:Test_exist_linux

Done およびSaveをクリックします。

Post	ture Policy	Guide Me	ting	system and/o	r other cor	nditions	i.									~
~																
	Policy Options	Default_Firewall_Policy_Mac	H	Any	and	Mac	OSX	and	4.x or later	- 64	d	Agent	and	the	 Default_Firewall_Require ment_Mac 	Edit 🗸
	Policy Options	Default_Firewall_Policy_Mac_te mporal	1	Any	and	Mac	OSX	and	4.x or later	à	d	Temporal Agent	and	the	n Default_Firewall_Require ment_Mac_temporal	Edit 😔
	Policy Options	Default_Firewall_Policy_Win	18	Any	and	Win	Jows All	and	4.x or later	-24	d	Agent	and	the	n Default_Firewall_Require ment_Win	Edit 😔
	Policy Options	Default_Firewall_Policy_Win_te mporal	1f	Any	and	Win	lows All	and	4.x or later	- 10	d	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	and	4.x or later	- 87	d	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	and	4.x or later		d	Temporal Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Mac_ temporal 	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win	H	Any	and	i Win	Jows All	and	4.x or later	- 10	d	Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Win 	Edit 😔
	Policy Options	Default_Hardware_Attributes_P olicy_Win_temporal	11	Any	and	Win	lows All	and	4.x or later	20	d	Temporal Agent	and	the	 Default_Hardware_Attrib utes_Requirement_Win_t emporal 	Edit 😔
	Policy Options	Default_USB_Block_Policy_Win	H	Any	and	Win	dows All	and	4.x or later	51	d	Agent	and	the	n USB_Block	Edit 😔
		Default LICB Black Ballou Min		Anu	204	i Wie	Inws All	and	4.x or later		d	Temporal Agent	and	the	USB_Block_temporal	Edb. U

ISE_Add_New_Posture_Policy_1

ステップ 23: Work Centers > Posture > Policy Setsに移動します。クリックしてInsert new row aboveします。

≡	dentity Services	Engine				Work Centers / P	osture			۹ () ()	٥	A
FI.	Bookmarks	Overview	Network Devices Clien	t Provisioning Policy Eleme	ents Posture Policy Policy	Sets Troubleshoot	Reports	Settings					
51 13	Dashboard Context Visibility		Policy Sets						Reset Policyset	Hitcount		Save	
*	Operations		 Status Policy Set Name 	Description	Conditions				Allowed Protocols / Server Sequence	e Hits	Action	s Vie	*
U	Policy		Q Search										
4. A	Administration Work Centers		C Default	Default policy set					Default Network Access	- 0	豪	>	
٢	Interactive Help								Insert	new row	above		
										Reset		Save	

ISE_Add_New_ポリシー_セット

ステップ 23.1: 詳細を設定します。

ポリシーセット名:ファイアウォールポスチャ

条件:ネットワークアクセスデバイスのIPアドレスが等しい[FTD IPアドレス]

をクリックします。 Save

=	dentity Services	Engine							Work Centers /	Posture						c	۵ ۵	۲	۹ ۱	۹
F.	Bookmarks	Overview	Network	k Devices	Client Provisionir	Policy Elemen	ts Posture Policy	Policy Sets	Troubleshoot	Reports	Settings									
11 13	Dashboard Context Visibility	P	olicy Sets											Reset	Reset P	olicyset H	itcounts		Save	
*	Operations		🕑 Status	Policy Set P	iame Desc	ription	Conditions						Allow	red Protocol	/ Server S	lequence	Hits	Actions	View	
Ð	Policy		Q. Search	h																
8.	Administration		•	Firewall Posts	~e		Network Access Device	IP Address EQUALS					Det	rult Network	locess	2+	7	٨	,	
ភា	Work Centers		•	Default	Defay	It policy set							Def	ult Network	locess	11		\$	>	
٢	Interactive Help																Reset		Save	

ISE_Add_New_Policy_Set_1

ステップ 23.2:>をクリックして、ポリシーセットを入力します。 ポスチャ準拠、非準拠、および不明ステータスの新しい認可ル ールを作成します。をクリックします。Save

compliant_profile準拠

non_compliant_profileによる非準拠

unknown_redirectによる不明

disco Identi	ity Se	ervice	s Engine					Work Cen	ters / Postu	re						antaria Martina Martina Martina
Overview	v V s	Netwo	rk Devices Clie	nt Provisioning Po	olicy Elements	Posture Policy	Policy Sets	Troubleshoot	Reports	Settings						
		0	Firewall Posture		D Netw	ork Access-Device IP Add	ress EQUALS :						Default Network	k Access	0	+ •
∼A	Authent	ication	Policy(1)													
	⊕ s	tatus	Rule Name	Conditions								Use			Hits	Actions
	Q	Search														
								+								
												All_User_	ID_Stores	0		
		0	Default									> Option	ns		48	(2)
> A <	luthori	tation P	olicy - Local Exception	5												
> A	luthori	ration P	olicy - Global Exception	ns												
VA	Authori	tation P	Policy(4)													
										Results						
	⊕ s	tatus	Rule Name	Conditions						Profiles		Security Gr	roups		Hits	Actions
	Q	Search														
	[۲	Compliant	는 Session-Postur	eStatus EQUALS Con	nplant				compliant_profile	/ +	Select fro	m list	<i>•</i> +	15	¢
	[0	Non_Compliant	E Session Postur	eStatus EQUALS Non	Compliant				non_compliant_profile	0+	Select fro	m list	1+	5	(2)
	[0	Unknown	E Session Postur	eStatus EQUALS Unk	ngwn				unknown_redirect	0 +	Select fro	m list	2+	47	(2)
	Sverview Overview	Cverview Cverview ✓Authent ④ S Q : >Authori >Authori ×Authori ×Authori Q : Q : Q : Q : Q : Q : Q : Q :	Overview Netwo Overview Netwo Coverview Coverview Coverview Coverview Coverview Coverview	Overview Network Devices Clie Overview Network Devices Clie Overview Prevail Posture Authentication Policy(1) Status Rule Name Q Search Authorization Policy - Local Exception Authorization Policy - Global Exception Authorization Policy(4) Status Rule Name Q Search O Status Rule Name Q Status Rule Name Q Search O Comptiant O Unknown	Status Rule Name Conditions > Authorization Policy(1) © Status Rule Name > Authorization Policy - Local Exceptions > Authorization Policy(4)	Overview Network Devices Client Provisioning Policy Elements Overview Prevail Posture Posture Post	Status Rule Name Conditions Authorization Policy - Local Exceptions Authorization Policy(4)	Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Image: Status Prevail Posture Image: Status Rule Name Conditions Image: Status Rule Name Conditions Image: Status Image: Status Image: Status Image: Status Rule Name Conditions Image: Status I	dentity Services Engine Work Cent Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot	dentity Services Engine Work Centers / Postur Overview Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Conditions Image: Status Rule Name Conditions Image: Conditions Image: Conditions Image: Status Rule Name Conditions Image: Conditions Image: Conditions Image: Status Rule Name Conditions Image: Conditions	Uterritie Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings • Pression • Pression • Policy Sets Troubleshoot Reports Settings • Pression • Pression • Policy Sets • Policy Sets • Pression	Work Conters / Posture Overview Overview Image: Conditions	Udentity Services Engine Work Centers / Posture Overview Network Devices Client Provisioning Policy Elements Policy Sets Troubleshoot Reports Settings Immediate Access Device IP Address Element Immedia Access Device IP Address Element Immediate Access Device IP Address Immediate Access Device IP Address	Work Centers / Posture Overview Network Davides Client Provisioning Policy Elements Policy Stat Troubleshoot Reports Settings Constitution Pressin Policy Policy Elements Policy Elements Policy Elements Policy Elements Constitution Policy Elements Policy Elements Policy Elements Policy Elements Policy Elements Constitution Policy Elements Policy Elements Policy Elements Policy Elements Policy Elements Constitution Constitution Use Policy Elements Policy Elements Policy Elements Status Rule Name Constitution Use Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements All Uter Constitution Policy Elements Policy Elements Policy Elements <td>Work Canter's / Posture</td> <td>Work Conters / Posture</td>	Work Canter's / Posture	Work Conters / Posture

ISE_Add_New_Policy_Set_2

Ubuntuでの 設定

ステップ 24: GUIを使用してUbuntuクライアントにログインします。ブラウザを開いてVPNポータルにログインします。この例では、demo.example.comです。

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}	≡

N	Logon		
Group Username	posture_vpn	v	
Password	Logon		

Ubuntu_Browser_VPN_ログイン

ステップ 25:をクリックします。Download for Linux

Cisco S	Secu	re Client Insta	allati×	:	+					e	ø	×
\leftarrow	\rightarrow	C	08	2	https://demo. example.com /CACHE/stc/2/index.html	F	80%	ជ		\bigtriangledown	\mathbf{F}	≡
		Secure	re Clien	t								
					Cisco Secure Client Download							4
					Download & Install							
					Download Cisco Secure Client and install it on your computer. Download for Linux							
						0	🕂 Inst	ructio	าร			

*Ubuntu_Browser_VPN_*ダウンロード_1

ダウンロードしたファイルの名前はcisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.shです。



*Ubuntu_Browser_VPN_*ダウンロード_2

ステップ 26:ブラウザを使用してVPN証明書をダウンロードし、ファイル名を<certificate>に変更します。crt。これは、Firefoxを 使用して証明書をダウンロードする例です。

-	demo.example.c	om/+CSCOE× +		\sim		ē	×
\leftarrow	\rightarrow G	O Anttps://demo.examp	le.com/+CSCOE+/logon.html#form_title_text	\bigtriangledown	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) transmitted over the o view information tr tled across the netwo	Internet. aveling between computers. It i ork. Help		

ステップ 27: Ubuntuクライアントで端末を開きます。path home/user/Downloads/に移動して、Cisco Secure Clientをインストールします。

<#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\$

ステップ28: UbuntuクライアントのVPNポータル証明書を信頼します。

<#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

ステップ 29: UbuntuクライアントでCisco Secure Clientを開き、VPNをdemo.example.comに正常に接続します。

		Cisco Secure	Client				×
AnyCor							
		ייו יי cisc	11 0				
Connect to:	demo.exa	ample.com			~	•	\$
Group:	posture_v	pn				~	-
Username:	isetest						
Password:	******						



Ubuntu_Secure_Client_接続

ステップ 30:ブラウザを開き、ISE CPPポータルへのリダイレクトをトリガーするWebサイトにアクセスします。ISE CPPポータ ルから証明書をダウンロードし、ファイル名を<certificate>に変更します。crt。 次に、ダウンロードにFirefoxを使用する例を示し ます。



Ubuntu_Browser_CPP_Cert_ダウンロード

ステップ 30.1: Ubuntuクライアント上のISE CPPポータル証明書を信頼します。

<#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.
```

ステップ 31: ISE CPPポータルStart でクリックします。

Oevice Security Check × +	e	ø	×					
← → C () A https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08 ☆		${igardown}$	≡					
You must log in to this network before you can access the Internet.			\times					
Client Provisioning Portal								
Device Security Check Your computer requires security software to be installed before you can connect to the network.								
Ubuntu_Browser_CPP_開始								
ステップ 32 : Click here to download and install Agent								

Device Security C	heck × +	- 0	×					
$\leftarrow \ \rightarrow \ G$	https://demoise.example.com ::8443/portal/ClientProvisionStart.action?from=CL 🏠	${igardown}$	≡					
🚺 You must log in	to this network before you can access the Internet.		\times					
cisco.	Client Provisioning Portal							
Device Security Check Your computer requires security software to be installed before you can connect to the network. Unable to detect Posture Agent								
+ This is my first time here								
 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.								
•	+ Remind me what to do next							

*Ubuntu_Browser_CPP_Download_*ポスチャ

ステップ 33: Ubuntuクライアントで端末を開きます。パスhome/user/Downloads/に移動して、ポスチャモジュールをインストール します。

<#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_0NcLgcMURfyZmR6HoI

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.

ステップ 34: UbuntuクライアントのUIで、Cisco Secure Clientを終了し、再度開きます。ISEポスチャモジュールがインストールされ、正常に実行されます。



Ubuntu_Secure_Client_ISE_Posture_Installed (インストール済み)

ステップ 35: Ubuntuクライアントで端末を開きます。pathに移動home/user/Desktoptest.txt し、ISEで設定されたファイル条件を満たすファイルを作成します。

<#root>

user@ubuntu22-desktop:~\$

cd Desktop/

user@ubuntu22-desktop:~/Desktop\$

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ1: UbuntuクライアントでVPNをdemo.example.comに接続します。

	- • ×							
AnyConnect \	/PN 🛃 Stat	tistics	🎯 ISE Posture	About				
cisco								
Connect to: demo.example.com -								
Group: pos	ture_vpn			~				
Username: isete	est							
Password:	****							

	🇞 Di	isconnect
Connected to demo.example.c	om.	

確認_Ubuntu_セキュア_クライアント_接続

ステップ2: UbuntuクライアントでISEポスチャステータスを確認します。



確認_Ubuntu_Secure_Client_Compliant

ステップ3: ISEのRADIUSライブログを確認します。Operations > RADIUS Live Logに移動します。

=	dentity Services Engine			Oper	ations / RADIUS			Q & @ Q A
Ц	Live Logs Live Sessions							
55								
14	Misconfigured Supplicants 🕕	Miscor	figured Network Dev	ices 🕕	RADIUS Drops		Client Stopped Responding ①	Repeat Counter 🕕
*	0		0		0		0	0
U							Refresh Show	Within
a.							Never v Latest 20 red	cords 🗸 Last 24 hours 🗸
đ	💭 🕁 Reset Repeat Counts ්	🗅 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 A	Authorization Policy
	May 29, 2024 09:08:48.798 PM	٥	isetest	52:54:00:17:68: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	rewall Posture >> Unknown

確認ISE_ライブログ

ステップ4:SSHまたはコンソールを使用してFTD CLIに移動します。

<#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

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Cisco Secure ClientとISEのポスチャフローとトラブルシューティングについては、CCOの『<u>2.2前後のISEポスチャスタイルの比較</u> 』および『<u>ISEセッション管理とポスチャのトラブルシューティング</u>』を参照してください。

関連情報

 <u>Cisco Identity Services Engineネットワークコンポーネントの互換性、リリース3.3</u>

- <u>Cisco Identity Services Engine 管理者ガイド リリース 3.3</u>
- シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。