# FTDでのAnyConnectリモートアクセスVPNでの ISE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>ネットワーク図とトラフィック フロー</u>	
<u>コンフィギュレーション</u>	
<u>FTD/FMC</u>	
ISE	
<u>確認</u>	
トラブルシュート	

# はじめに

このドキュメントでは、Identity Services Engine(ISE)に対してVPNユーザをポスチャするように Firepower Threat Defense(FTD)バージョン6.4.0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。

- ・ AnyConnect リモート アクセス VPN
- FTDでのリモートアクセスVPNの設定
- ・ Identity Services Engineとポスチャサービス

# 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。

- CiscoFirepower脅威対策(FTD)ソフトウェアバージョン6.4.0
- CiscoFirepowerマネジメントコンソール(FMC)ソフトウェアバージョン6.5.0
- Cisco AnyConnectセキュアモビリティクライアントバージョン4.7がインストールされた Microsoft Windows 10
- Cisco Identity Services Engine(ISE)バージョン2.6およびパッチ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

# ネットワーク図とトラフィック フロー



1.リモートユーザは、FTDへのVPNアクセスにCisco Anyconnectを使用します。

2. FTDがそのユーザのRADIUS Access-RequestをISEに送信します。

3.その要求が、ISE上のFTD-VPN-Posture-Unknownという名前のポリシーにヒットします。 ISEは、次の3つの属性を持つRADIUS Access-Acceptを送信します。

- cisco-av-pair = url-redirect-acl=fyusifovredirect:これは、リダイレクトされるトラフィックを 決定する、FTD上でローカルに定義されたアクセスコントロールリスト(ACL)の名前です。
- cisco-av-pair = urlredirect=<u>https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-</u> <u>11e9-98fb-0050568775a3&action=cpp</u>:リモートユーザのリダイレクト先となるURLです。
- DACL = PERMIT\_ALL\_IPV4\_TRAFFIC:ダウンロード可能ACL。この属性はオプションです。 このシナリオでは、すべてのトラフィックがDACLで許可されます)

4. DACLが送信された場合、DACLのコンテンツをダウンロードするためにRADIUSアクセス要求 /アクセス承認が交換されます

5. VPNユーザからのトラフィックがローカルに定義されたACLに一致すると、ISEクライアント プロビジョニングポータルにリダイレクトされます。ISEはAnyConnectポスチャモジュールとコ ンプライアンスモジュールをプロビジョニングします。 6.エージェントがクライアントマシンにインストールされると、プローブを使用してISEが自動的 に検索されます。ISEが正常に検出されると、エンドポイントでポスチャ要件がチェックされま す。この例では、エージェントはインストールされているマルウェア対策ソフトウェアを確認し ます。次に、ポスチャレポートをISEに送信します。

7. ISEがエージェントからポスチャレポートを受信すると、ISEはこのセッションのポスチャステ ータスを変更し、新しい属性でRADIUS CoAタイプのプッシュをトリガーします。今回は、ポス チャステータスが判明し、別のルールがヒットします。

- ・ ユーザが準拠している場合、フルアクセスを許可するDACL名が送信されます。
- ユーザが非準拠の場合、制限付きアクセスを許可するDACL名が送信されます。

8. FTDがリダイレクションを削除します。FTDがISEからDACLをダウンロードするために Access-Requestを送信します。特定の DACL が VPN セッションに付加されます。

コンフィギュレーション

FTD/FMC

ステップ 1:ISEおよび修復サーバ(存在する場合)のネットワークオブジェクトグループを作成 します。Objects > Object Management > Networkの順に移動します。

Overview Analysis	Policie	s Devices Objects AM	1P Intelligence					
Object Management	Intrus	sion Rules						
Network A network object represent	s one o	or more IP addresses. Network obj	jects are used in va	rious places, includ	ing access control p	policies, network va	riables, intrusion (	rules, identity rules, ne
Extended		Name					Value	
Standard		any-ipv4					0.0.0.0	/0
Address Pools		any-ipv6					::/0	
IPv6 Pools		enroll.cisco.com					72.163	.1.80
Application Filters		IPv4-Benchmark-Tests	Edit Network	Object				? ×
💮 Cipher Suite List		IPv4-Link-Local	Name	ISE_PSN				
Community List		IPv4-Multicast	Description					
Individual Objects		IPv4-Private-10.0.0.0-8						_
Object Groups     Object Group		IPv4-Private-172.16.0.0-12	Network	<ul> <li>Host</li> </ul>	C Range	C Network	C FQDN	
File List		IPv4-Private-192.168.0.0-16		192.168.15.14				
FlexConfig     FlexConfig Object     Text Object		IPv4-Private-All-RFC1918	Allow Overrides	•	1		Save	Cancel
Geolocation		IPv6-IPv4-Mapped					::###:0	.0.0.0/96
Mainterface		IPv6-Link-Local					fe80::/	10
Network		IPv6-Private-Unique-Local-Addr	esses				fc00::/	7
Þ 🌽 PKI		IPv6-to-IPv4-Relay-Anycast					192.88	.99.0/24

ステップ 2:リダイレクトACLを作成します。Objects > Object Management > Access List > Extendedの順に移動します。Add Extended Access Listをクリックして、リダイレクトACLの名前を指定します。この名前は、ISE認可結果と同じである必要があります。

Overview Analysis Polici	es Devices Obj	ects AN	IP Intelligence				Deploy 🧕 S
Object Management Intr	usion Rules	_					
Extended	as an access control l	ct (ACI) cel	acts the traffic to which a	service will apply. Standard-Idan	tifies traffic based on destina	Add	Extended Access List
Supports IPv4 and IPv6 address	es. You use these obje	cts when con	iguring particular feature	s, such as route maps.		tion out cas only recharge come oused	
Access List	New Extended	Access Li	st Obiect				? ×
B Extended							
Standard	Name	fyusifovre	lirect				
a 🖵 Address Pools	Entries (0)						
IPv4 Pools							DbA 🕥
PV6 Pools	Sequence	Action	Source	Source Port	Destination	Destination Port	
Y AS Path							
Cipher Suite List				No record	s to display		
Community List							
a 🜍 Distinguished Name							
Individual Objects							
Colject Groups							
DNS Server Group	Allow Overrides						
Tile List							
FlexConfig						Save	Cancel
FlexConfig Object							

ステップ3: リダイレクトACLエントリを追加します。[Add] ボタンをクリックします。DNS、 ISE、および修復サーバへのトラフィックをブロックして、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すると、リダイレクトがトリガーされます(必要に応じてACLエントリを より具体的にすることができます)。

Add Extended A	Access List Entry					? ×
Action:	× Block	<b>v</b>				
Logging:	Default	•				
Log Level:	Informational	Ψ				
Log Interval:	300	Sec.				
Network Por	rt					
Available Netwo	rks C	0	Source Networks (1)	Destina	ation Networks (1)	
Search by nar	me or value		any-ipv4		_PSN	i
🔁 any		-				
any-ipv4		Add to				
any-ipv6		Source				
enroll.cisco.c	om	Add to				
IPv4-Benchm	nark-Tests	Destination				
IPv4-Link-Lo	cal					
IPv4-Multicas	st					
IPv4-Private-	-10.0.0.0-8					
IPv4-Private-	-172.16.0.0-12	-1	Enter an ID address	Add Enter a	n ID address	Add
			Enter an IP address	Add	In IP address	Add
					Add	Cancel

ime	fyusifovre	direct				
itries (4)						O Ad
Sequence	Action	Source	Source Port	Destination	Destination Port	
1	🗙 Block	🖶 any	Any	Any	DNS_over_UDP	a 🖉
2	🗙 Block	💭 any-ipv4	Any	ISE_PSN	Any	Ø 🗄
3	🗙 Block	any-ipv4	Any	RemediationServers	Any	Ø 🗎
4	🛹 Allow	📰 any-ipv4	Any	any-ipv4	Апу	6

ステップ 4: ISE PSNノードを追加します。Objects > Object Management > RADIUS Server Groupの順に移動します。Add RADIUS Server Groupをクリックし、名前を入力して、すべての チェックボックスをオンにし、プラス記号のアイコンをクリックします。

Edit RADIUS Server Group			? X
Name:*	ISE		
Description:			
Group Accounting Mode:	Single	•	
Retry Interval:*	10	(1-10) Seconds	
Realms:		•	
Enable authorize only			
Enable interim account update			
Interval:*	24	(1-120) hours	
🗹 Enable dynamic authorization			
Port:*	1700	(1024-65535)	
RADIUS Servers (Maximum 16 servers)	vers)		
IP Address/Hostname			
	No records to display		
		Save	Cancel

ステップ 5:開いたウィンドウで、ISE PSN IPアドレスとRADIUSキーを入力し、[Specific Interface] を選択し、ISEが到達可能なインターフェイス(このインターフェイスはRADIUSトラ フィックの送信元として使用されます)を選択してから、以前に設定した[Redirect ACL] を選択 します。

New RADIUS Server		? X
IP Address/Hostname:*	192.168.15.13 Configure DNC at Threat Defense Platform Settings to resolve hostnar	me
Authentication Port:*	1812 (1-65535)	
Key:*	•••••	
Confirm Key:*	•••••	
Accounting Port:	1813 (1-65535)	
Timeout:	10 (1-300) Seconds	
Connect using:	○ Routing ⓒ Specific Interface 🕕	
	ZONE-INSIDE	)-
Redirect ACL:	fyusifovredirect	>
	Save Cancel	

手順 6 : VPNユーザ用のアドレスプールを作成します。Objects > Object Management > Address Pools > IPv4 Poolsの順に移動します。Add IPv4 Poolsをクリックして、詳細を入力します。

Overview Analysis	Policies Devices Objects AMP Intelligence	Deploy 🤑 Sy
Object Management	Intrusion Rules	
IPv4 Pools IPv4 pool contains list of I	Pv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.	Add IPv4 Pools
🕃 Standard	Name	Value
Address Pools	Edit IPv4 Pool ? ×	172.16.1.10-172.16.1.20
<ul> <li>Inverpola</li> <li>Inverpola</li> <li>Profection</li> <li>As Path</li> <li>Cipher Suite List</li> <li>Community List</li> <li>Distinguished Name</li> <li>Individual Object</li> <li>Object Groups</li> <li>DNS Server Group</li> <li>File List</li> <li>FlexConfig</li> <li>FlexConfig</li> <li>FlexConfig Object</li> <li>Geolocation</li> <li>Interface</li> </ul>	Name*       VPN-172-Pool         IPv4 Address Range*       I72.16.1.10-172.16.1.20         Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150         Description         Allow Overrides         Image: Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices         Override (0)         Save	

手順 7:AnyConnectパッケージを作成します。Objects > Object Management > VPN > AnyConnect Fileの順に移動します。Add AnyConnect Fileをクリックしてパッケージ名を指定し 、Cisco Software Downloadからパッケージをダウンロードして、Anyconnect Client Image File Typeを選択します。

Overview Analysis Policies	s Devices Objec	AMP Intelligence	Deploy 🧕 Sy
Object Management Intrus	sion Rules		
AnyConnect File File objects represent files used in	configurations, typicall	for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image file	Add AnyConnect File
Policy List	Name		Value
A 🕒 Prefix List	Edit AnyConnect	File ? ×	anyconnect-win-4.7.01076-webdepl
<ul> <li>IPv4 Prefix List</li> <li>IPv6 Prefix List</li> <li>RADIUS Server Group</li> <li>Route Map</li> <li>Security Intelligence</li> <li>DNS Lists and Feeds</li> <li>URL Lists and Feeds</li> <li>Sinkhole</li> <li>SLA Monitor</li> <li>SLA Monitor</li> <li>Time Range</li> <li>Tunnel Zone</li> <li>URL</li> <li>Variable Set</li> <li>VLAN Tag</li> </ul>	Name:" File Name:" File Type:" Description:	AC47 anyconnect-win-4.7.01076-webdeploy-k9. Browse AnyConnect Client Image	

ステップ 8 : Certificate Objects > Object Management > PKI > Cert Enrollmentの順に移動します 。Add Cert Enrollmentをクリックして名前を入力し、Self Signed Certificate in Enrollment Typeを 選択します。Certificate Parametersタブをクリックして、CNを指定します。

Overview Analysis Po	cies Devices Objects AMP Intelligence		Deploy 🧕 Sy
Object Management	trusion Rules		
Cert Enrollment A certificate enrollment object activities occur in your Private	contains the Certification Authority (CA) server information and enrollment Key information (2011)	t parameters that are required for creating Certificate Signing Requ	ests (CSRs) and obtaining Identity Certificates fr
Access List	Add Cert Enrollment	? ×	Туре
Laddress Pools     Application Filters     Application Filters     Application Filters     Cipher Suite List     Community List     Distinguished Name     DNS Server Group     File List     File List     Geolocation     Interface     Key Chain     Network     PKI     Cert Enrollment     External Certs     Internal CA Groups     Internal CA Groups     Internal CA Groups     Internal CA Groups     Internal CA Groups	Name*     vpn-cert       Description     CA Information     Certificate Parameters     Key     Revoca       Enrollment Type:     Self Signed Certificate       Common Name (CN) is mandatory for self-signed certificate time       Configure CN, please navigate to 'Certificate Parameters' tab.	ation	Self Signed Ce
🔄 Internal Cert Groups			
Internal Certs Trusted CA Groups Trusted CAs Policy List	Allow Overrides		
Je Port	-	Save	Displaying 1 - 1 of 1 rows

ŀ	Add Cert Enrollme	ent						? ×	ξ
	Name*	vpr	n-cert						
	Description								
	CA Information	Certific	ate Parameters	Key	Revocation				
	Include FQDN:		Use Device Hostna	me as l	FQDN		~		
	Include Device's IP	Address:	10.48.26.99						
	Common Name (Cf	v):	vpn-cert.example.	com					
	Organization Unit (	CU):							
	Organization (O):		example						
	Locality (L):								
	State (ST):		Krakow						
	Country Code (C):		PL						
	Email (E):								
	Include Device's	Serial Nu	mber						
	Allow Overrides								
						Save		Cancel	)

ステップ 9 : リモートアクセスVPNウィザードを起動します。Devices > VPN > Remote Accessの順に移動し、Addをクリックします。

Overview Analysis	Policies	Devices Objects	AMP	Intelligence			Deploy	🔒 System	Help 🔻 adn	nin <del>v</del>
Device Management	NAT	VPN   Remote Access	QoS	Platform Settings	FlexConfig	Certificates				
									🕥 Add	
Name				Status		Last Modified				
	No configuration available Add a new configuration									

ステップ 10 : 名前を入力し、VPNプロトコルとしてSSLをチェックし、VPNコンセントレータと して使用されるFTDを選択して、Nextをクリックします。

Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Profile 3 AnyConnect	4 Access & Certificate 5 Summary		
Targeted Devices and Protocols         This wizard will guide you through the required min with a new user-defined connection profile.         Name:*       EmployeeVPN         Description:         VPN Protocols:       VSL         Targeted Devices:       Available Devices         Targeted Devices:       Available Devices         Image:       Image: Search         Image:       Image: Search         Image:       Image: Search	Selected Devices Add	<section-header><section-header><text><text><section-header><text><text><text></text></text></text></section-header></text></text></section-header></section-header>	
		В	ack Next Cancel

ステップ 11Connection Profileの名前を入力し、Authentication/Accounting Serversを選択し、以前に設定したアドレスプールを選択して、Nextをクリックします。

◆ 注:認証サーバは選択しないでください。1人のユーザに対して2つのアクセス要求がトリガーされます(1回目はユーザパスワード、2回目はパスワードcisco)。

Remote Access VPN Policy Wizard		
Policy Assignment     2 Connection Profile     3 AnyConnect     4	Access & Certificate S Summary	
Connection Profile: Connection Profiles specify ti Itself, how AAA is accomplish group policies. Connection Profile Name:*	he tunnel group policies for a VPN connection. These policies pertain to creating the tunnel ed and how addresses are assigned. They also include user attributes, which are defined in EmployeeVPN	
Authentication Authorization	This name is configured as a connection arias, it can be used to connect to the VPN gateway b & Accounting (AAA):	
Specify the method of author connections.	ntication (AAA, certificates or both), and the AAA servers that will be used for VPN	
Authentication Method	AAA Only	
Authentication Server:	* ISE VO- (Realm or RADIUS)	
Authorization Server:	Use same authentication server 👻 🔕 (RADIUS)	
Accounting Server:	ISE V (RADIUS)	
Client Address Assignment: Client IP address can be ass selected, IP address saint	iigned from AAA server, DHCP server and IP address pools. When multiple options are ment is tried in the order of AAA server, DHCP server and IP address pool.	
Use AAA Server (RA	DIUS only) ()	
Use DHCP Servers		
IPv4 Address Pool	VPN-172-Pool	
- IPv6 Address		
Group Policy:		
A group policy is a collection established. Select or create	of user-oriented session attributes which are assigned to client when a VPN connection is a Group Policy object.	
Group Policy:*	DfltGrpPolicy V Edit Group Policy	
	Bac	k Next Cancel

ステップ 12以前に設定したAnyConnectパッケージを選択し、Nextをクリックします。

Remote Access VPN Policy Wizard	
1 Policy Assignment 2 2 Connection Profile 3 AnyConnect	Access & Certificate S Summary
Remote AnyConnect User Client	Internet Outside VPN Device Inside Corporate Resources
AnyConnect Client Image	ally download the latest AnyConnect package to the client device when the VEN
connection is initiated. Minimize com connection is initiated. Minimize com Download AnyConnect Client packa	ges from Cisco Software Download Center.
	Show Re-order buttons
AC47	AnyConnect Client Package Name         Operating System           anyconnect-win-4.7.01076-webdeploy-k9         Windows
	Back

ステップ 13VPNトラフィックが予想されるインターフェイスを選択し、以前に設定した Certificate Enrollmentを選択して、Nextをクリックします。

Remote Access VPN Policy Wizard			
1 Policy Assignment 2 O Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary			
Network Interface for Incoming VPN Access Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections. Interface group/Security Zone:* ZONE-OUTSIDE			
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 VEN gateway. Certificate Enrollment:* W 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. Sypass Access Control Gicty for decrypted traffic (sysopt permit-vpn) This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downleaded from AAA server are still applied to VPN traffic.			
	Back	Next	Cancel

ステップ 14:サマリーページを確認し、Finishをクリックします。

Remote Access VPN Policy Cor	Additional Configuration Requirements
Firepower Management Center will Name: Device Targets: Connection Profile: Connection Alias: AAA: Authentication Method: Authentication Server: Authorization Server: Authorization Server: Address Assignment: Address from AAA: DHCP Servers: Address Pools (IPv4): Address Pools (IPv4): Address Pools (IPv6): Group Policy: AnyConnect Images: Interface Objects: Device Certificates:	<ul> <li>After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.</li> <li>Access Control Policy Update         <ul> <li>Access Control Policy Update</li> <li>An <u>decess Control</u> rule must be defined to allow VPN traffic on all targeted devices.</li> <li>NAT Exemption             If NAT is enabled on the targeted devices, you must define a <u>MAT Policy</u> to exempt VPN traffic.         </li> <li>DNS Configuration         To resolve hostname specified in AAA Servers or CA Servers, configure DNS using <u>FlaxConfig Policy</u> on the targeted devices.         Port Configuration         SL will be enabled on port 443. Please ensure that these ports are not used in <u>MAT Policy</u> or other services before deploying the configuration.         Metwork Interface Configuration         Mate sure to add interface from targeted devices. USE: VISIDE         OUTSIDE         OUTSIDE         Outside securityZone object 'ZONE-OUTSIDE'         OUTSIDE         Description         Description</li></ul></li></ul>

ステップ 15:FTDに設定を展開します。Deployをクリックし、VPNコンセントレータとして使用 するFTDを選択します。

Overview Analysis Policies Devi	ices Objects AMP Intelligence				Deploy	🧕 System Help 🔻 admin 🔻
Device Management NAT VPN •	Remote Access QoS Platform Settings FlexCo	onfig Certificates				
EmployeeVPN	Deploy Policies Version:2020-02-02 09:15 PM				? ×	Save Save
	☑ Device	Inspect Interruption	Type Group	Current Version	2	Policy Assignments (1)
Connection Profile Access Interfa	C 🖉 ⊕ 🚅 192.168.15.11	No	FTD	2020-02-02 09:10 PM		
						0
Name						
DefaultWEBVPNGroup						/ 5
EmployeeVPN						/ 8
	Selected devices: 1			Deploy Cancel		

ISE

ステップ1:ポスチャ更新を実行します。[Administration] > [System] > [Settings] > [Posture] > [Updates] に移動します。

Posture Updates	
<ul> <li>Web</li> </ul>	○ Offline
* Update Feed URL	https://www.cisco.com/web/secure/spa/posture-update.xml Set to Default
Proxy Address	(i)
Proxy Port	HH MM SS
Automatically che	eck for updates starting from initial delay 20 🔻 49 💌 18 💌 every 2 hours (i)
Save	date Now Reset

<ul> <li>Update Information</li> </ul>	
Last successful update on	2020/02/02 20:44:27(i)
Last update status since ISE was started	Last update attempt at 2020/02/02 20:44:27 was successful 🕡
Cisco conditions version	257951.0.0.0
Cisco AV/AS support chart version for windows	227.0.0.0
Cisco AV/AS support chart version for Mac OSX	148.0.0.0
Cisco supported OS version	49.0.0.0

ステップ 2:コンプライアンスモジュールをアップロードします。Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動します。Addをクリックし、Agent resources from Cisco siteを選択します

Download Remote Resources	×
Name 🔺	Description
AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
AnyConnectComplianceModuleOSX 3.6.11682.2	AnyConnect OS X Compliance Module 3.6.11682.2
AnyConnectComplianceModuleOSX 4.3.972.4353	AnyConnect OSX Compliance Module 4.3.972.4353
AnyConnectComplianceModuleWindows 3.6.11682.2	AnyConnect Windows Compliance Module 3.6.11682.2
AnyConnectComplianceModuleWindows 4.3.1053.6145	AnyConnect Windows Compliance Module 4.3.1053.6145
CiscoTemporalAgentOSX 4.8.03009	Cisco Temporal Agent for OSX With CM: 4.3.972.4353
CiscoTemporalAgentWindows 4.8.03009	Cisco Temporal Agent for Windows With CM: 4.3.1053.6145
ComplianceModule 3.6.11428.2	NACAgent ComplianceModule v3.6.11428.2 for Windows
MACComplianceModule 3.6.11428.2	MACAgent ComplianceModule v3.6.11428.2 for MAC OSX
MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Ab
MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3
MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Rele
MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 rele
MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Pat
For AnyConnect software, please download from http://cisco.com	/go/anyconnect. Use the "Agent resource from local disk" add
option, to import into ISE	
	Save

ステップ 3:<u>シスコソフトウェアダウンロード</u>からAnyConnectをダウンロードし、ISEにアップ ロードします。Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動 します。

Addをクリックし、Agent Resources From Local Diskを選択します。Categoryの下でCisco Provided Packagesを選択し、ローカルディスクからAnyConnectパッケージを選択して、 Submitをクリックします。

#### Agent Resources From Local Disk > Agent Resources From Local Disk

Agent	Resources	From	Local	Disk	
-------	-----------	------	-------	------	--

\* Server name rules

Call Home List

Back-off Timer

30

secs

Cate	gory Cisco Provided Packages Browse anyconnect-wire	Cisco Provided Packages       Image: Cisco Provided Packages         Image: Image: Image: Cisco Provided Packages       Image: Cisco Provided Packages         Image: Image: Image: Image: Cisco Provided Packages       Image: Cisco Provided Packages         Image: Image: Image: Image: Image: Cisco Provided Packages       Image: Cisco Provided Packages         Image: Ima				
	AnyConnect Uploaded Re	AnyConnect Uploaded Resources				
	Name	Name A Type Version Description				
	AnyConnectDesktopWindows 4	.7.10 AnyConnectDesktopWin	dows 4.7.1076.0	AnyConnect Secure Mobility Clie		

ステップ 4: AnyConnectポスチャプロファイルを作成します。Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動します。

Addをクリックし、AnyConnect Posture Profileを選択します。名前とポスチャプロトコルを入力します。

\*Server name rulesの下に\*を入力し、Discovery hostの下にダミーIPアドレスを入力します。

ISE Posture Agent Profile Settings > AC_Posture_Profile					
* Name: AC Posture Profile Description					
Parameter	Value	Notes	Description		
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure		
Discovery host	1.2.3.4		The server that the agent should connect to		

need to be blank by default to force admin to enter a value. "\*" means agent

List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP

address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the

Client Provisioning portal)

Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

will connect to all

A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. \*\*.cisco.com

A list of IP addresses, that defines the all the Policy service nodes that the agent

will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.

Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this

max time limit is reached

		1				
ス	テップ 5:Policy	> Policy Elements >	Results > Client Pr	ovisioning >	Resourcesの順	に移動し、
An	yConnect Configu	urationを作成します	-。Addをクリックし	、AnyConne	ect Configuratio	nを選択し
ま	す。AnyConnect	Packageを選択し、	Configuration Name	eを指定し、C	Compliance Mo	duleを選択
し、	Diagnostic and	Reporting Toolにチ	ェックマークを入れ	ι、Posture P	rofileを選択して	てSaveをク

* Select AnyConnect Package * Configuration Name Description:	AnyConnectDesktopWindows 4.7.1076.0   AC CF 47
Description	Value Notes
* Compliance Module	AnyConnectComplianceModuleWindows 4.3.1012.6 -
AnyConnect Module Selection ISE Posture VPN Network Access Manager Web Security AMP Enabler ASA Posture Network Visibility Umbrella Roaming Security Start Before Logon Diagnostic and Reporting Tool	
Profile Selection	
* ISE Posture	AC Posture Profile
VPN	
Network Access Manager	
Wab Poourity	
web Security	¥

AMP Enabler 
Vetwork Visibility
Umbrella Roaming Security
Customer Feedback

手順 6: Policy > Client Provisioningの順に移動し、Client Provisioning Policyを作成します。 EditをクリックしてからInsert Rule Aboveを選択し、名前を指定して、OSを選択し、前のステッ プで作成したAnyConnect Configurationを選択します。

olju CIS	dent	ity Services Engine	Home	♦ Cor	ntext Visibility		Operations	▼Policy		Administration	Work Centers			License Warning 🔺	0	0	0	φ.
P	licy Sets	Profiling Posture	Client Provis	sioning	Policy Ele	ement	s											
Clic Defi For For	Einst Provisioning Policy efine the Client Provisioning Policy to determine what users will receive upon login and user session initiation: or Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. or Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.																	
•		Rule Name		Identi	ty Groups		Operating Sys	tems		Other Condition	ns		Results					
	<b>~</b>	AC_47_Win	If	Any		and	Windows All		and	Condition(s)		then	AC_CF_47				Edit   •	
I	<b>~</b>	IOS	If	Any		and	Apple iOS All		and	Condition(s)		then	Cisco-ISE-NSP				Edit   🕶	
1	<b></b>	Android	If	Any		and	Android		and	Condition(s)		then	Cisco-ISE-NSP				Edit   •	
1		Windows	If	Any		and	Windows All		and	Condition(s)		then	CiscoTemporalAgentWi ndows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP				Edit   •	
1		MAC OS	I	Any		and	Mac OSX		and	Condition(s)		then	CiscoTemporalAgentO SX 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE- NSP				Edit   •	
I		Chromebook	I	Any		and	Chrome OS Al		and	Condition(s)		then	Cisco-ISE-Chrome- NSP				Edit   •	

手順 7: Policy > Policy Elements > Conditions > Posture > Anti-Malware Conditionでポスチャ条 件を作成します。この例では、定義済みの「ANY\_am\_win\_inst」が使用されます。

### を参照。

cisco Identity Services Er	ngine Home	Context Visibility	<ul> <li>Operations</li> </ul>	✓Policy	<ul> <li>Administration</li> </ul>	▶ Work Centers
Policy Sets Profiling Po	sture Client Provi	sioning <b>v</b> Policy Ele	ments			
Dictionaries - Conditions	Results					
Library Conditions Smart Conditions Time and Date	Anti-I	Malware Condition t - 나 Add 다 Duplicate	e XDelete Descr	iption		
Profiling		NY_am_win_inst	Any AM	l installation ch	eck on Wi	
✓ Posture		NY_am_win_def	Any AM	I definition che	ck on Wind	
Anti-Malware Condition		NY_am_mac_inst NY_am_mac_def	Any AM Any AM	l installation ch I definition che	ieck on Mac ck on Mac	
Anti-Spyware Condition						
Anti-Virus Condition						
Application Condition						
Compound Condition						
Disk Encryption Condition						
File Condition						
Firewall Condition						

ステップ 8: Policy > Policy Elements > Results > Posture > Remediation Actionsの順に移動し、 Posture Remediationを作成します。この例では、これはスキップされます。修復アクションはテ キストメッセージにすることができます。

ステップ 9: Policy > Policy Elements > Results > Posture > Requirementsの順に移動し、 Posture Requirementsを作成します。定義済みの要件Any\_AM\_Installation\_Winが使用されます。

cisco Identity Services Engine	Home	Operations -Policy	Administration     Work Centers		License Warning 🔺 🔍		ø
Policy Sets Profiling Posture Cli	ient Provisioning   Policy Element	5					
Dictionaries + Conditions - Result	IS						
0							
Authentication					-		(م
	Requirements						
<ul> <li>Authorization</li> </ul>	Name	Operating Systems	Compliance Module	Posture			_
	Wessage Text Only	Conditions	Remediation Actions			Edit   🕶	-
► Profiling	Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_def	then	
← Posture	AnyAVDefRemediationMa c					Edit   🕶	
Demodeller Actions	Any_AS_Installation_Mac	for MacOSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_inst	then	
• Remediation Actions	Message Text Only					Edit   🕶	
Requirements	Any_AS_Definition_Mac	for MacOSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_def	then	
Client Provisioning	AnyASDefRemediationMa c					Edit   🕶	
	Any_AM_Installation_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_inst	then	
	Message Text Only					Edit   🕶	
	Any_AM_Definition_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_def	then	
	AnyAMDefRemediationWi n					Edit   🕶	
	Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_inst	then	
	Message Text Only					Edit   🔻	
	Any_AM_Definition_Mac	for MacOSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_def	then	
	AnyAMDefRemediationM					Edit   🕶	-

ステップ 10 : Policies > Postureでポスチャポリシーを作成します。Windows OSのアンチマルウ ェアチェックのデフォルトのポスチャポリシーが使用されます。

ah cu	dentity :	Services Engine	Home	ty Operations	▼Policy A	dministration + Work Centers					License Warning 🔺	Q	0	•	ø
P	olicy Sets F	Profiling Postur	e Client Provisioning + Poli	oy Elements											
Po	sture Policy														
De	fine the Postur	e Policy by config	uring rules based on operating sy	stem and/or other or	onditions.						-				٦
															_
	Status	Policy Options	Rule Name	Identity Groups	Operating S	Systems Compliance Mod	ule Posture Type	Other Condi	tions	Requirements					-
	0	Policy Options	Default_AntiMalware_Policy If _Mac	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then	Any_AM_Installation_ Mac			Ed	it   •	
	0	Policy Options	Default_AntiMalware_Policy If _Mac_temporal	Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then	Any_AM_Installation_ Mac_temporal			Ed	it   •	
		Policy Options	Default_AntiMalware_Policy II _Win	Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Any_AM_Installation_ Win			Ed	it i 👻	
	0	Policy Options	Default_AntiMalware_Policy If _Win_temporal	Any	and Windows All	and 4.x or later	and Temporal Agent	and	then	Any_AM_Installation_ Win_temporal			Ed	it   •	
	0	Policy Options	Default_AppVis_Policy_Mao II	Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then	Default_AppVis_Requ irement_Mac			Ed	it   +	

ステップ 11Policy > Policy Elements > Results > Authorization > Downlodable ACLSの順に移動し 、異なるポスチャステータス用のDACLを作成します。

この例では、

- ・ ポスチャ不明DACL:DNS、PSN、およびHTTPとHTTPSのトラフィックを許可します。
- ポスチャ非準拠DACL:プライベートサブネットへのアクセスを拒否し、インターネットトラフィックのみを許可します。
- Permit All DACL:ポスチャ準拠ステータスのすべてのトラフィックを許可します。

#### Downloadable ACL List > PostureNonCompliant1

#### **Downloadable ACL**

* Name	PostureUnknown
Description	
IP version	● IPv4 C IPv6 C Agnostic ()
* DACL Content	1234567       permit udp any any eq domain         8910111       permit ip any host 192.168.15.14         2131415       permit tcp any any eq 80         1617181       permit tcp any any eq 443         9202122       2324252         6272829       3031323         3343536       3738394

#### Downloadable ACL List > New Downloadable ACL

#### Downloadable ACL

* Name	PostureNonCompliant
Description	
IP version	€ IPv4 C IPv6 C Agnostic (i)
* DACL Content	1234567 deny ig any 10.0.0.0 255.0.0.0
	0910111 0eny jg any 172.10.0.0 200.240.0.0
	1617181 permit jp any any
	9202122
	2324252
	6272829
	3031323
	3343636
	3/38394

* Name	DermitA
Description	
IP version	⊙ IPv4 C IPv8 C Agnostic ①
ACL Content	123456 permit jp any any
	7891011
	121314
	181920
	212223
	242528
	303132
	222/225

ステップ 12Posture Unknown、Posture NonCompliant、およびPosture Compliantステータス用の

3つの認可プロファイルを作成します。これを行うには、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動します。Posture Unknownプロファイルで、 Posture Unknown DACLを選択し、Web Redirectionにチェックマークを付け、Client Provisioningを選択し、Redirect ACL名(FTDで設定)を指定して、ポータルを選択します。

Authorization Profiles > New A	Authorization Profile					
Authorization Profile						
* Name	FTD-VPN-Redirect					
Description						11.
* Access Type	ACCESS_ACCEPT	*				
Network Device Profile	號 Cisco 🔻 🕀					
Service Template						
Track Movement	(i)					
Passive Identity Tracking						
▼ Common Tasks						
🗹 DACL Name	Postu	reUnknown	٢			
Veb Redirection (CWA, MD	M, NSP, CPP) 👔					
Client Provisioning (Posture	e) •	ACL fyus	ifovredirect	Valu	JE It Provisioning Portal (d	efault) 🔻
✓ Attributes Details Access Type = ACCESS_ACCEPT DACL = PostureUnknown cisco-av-pair = url-redirect-acl=fyusifovred cisco-av-pair = url-redirect=https://ip:por	direct rt/portal/gateway?sessionId=5	SessionIdValue&p	ortal=27b1bc30-2e58-11e9-9	8fb-0050568775	a3&action=cpp	11.

Posture NonCompliantプロファイルで、ネットワークへのアクセスを制限するためにDACLを選択します。

#### Authorization Profiles > New Authorization Profile

Authorization Profile	
* Name	FTD-VPN-NonCompliant
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	dtto Cisco 👻 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
▼ Common Tasks	
DACL Name	PostureNonCompliant 📀

#### Attributes Details

Access Type = ACCESS\_ACCEPT DACL = PostureNonCompliant

Posture Compliantプロファイルで、ネットワークへのフルアクセスを許可するためにDACLを選択します。

Authorization Profiles > New Authorization Profile

Authorization Profile	
* Name	PermitAll
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	🗱 Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
▼ Common Tasks	
DACL Name	PermitAll 🛇
<ul> <li>Attributes Details</li> </ul>	
Access Type = ACCESS_ACCEPT	

ステップ 13Policy > Policy Sets > Default > Authorization Policyで認可ポリシーを作成します。 As条件として、Posture StatusとVNP TunnelGroup Nameが使用されます。

ahaha Id	entity Sen	vices Engine Home ♦ C	ontext Vis	ibility	<ul> <li>Operations</li> </ul>	▼Policy	Administration	Work Ce	nters			License Warnin	g 🔺	Q,	0	• •
Policy S	ets Profi	ling Posture Client Provisionin	g 🕨 Po	licy Elen	nents											
	$\odot$	Default	Default p	olicy set								Default Network	Access	×	- +	43
> Auth > Auth > Auth	nentication norization I norization I	Policy (3) Policy - Local Exceptions Policy - Global Exceptions														
▲ Auth	norization I	Policy (18)														
									Results							
+	Status	Rule Name	Condit	ions					Profiles		Security Gr	oups			Hits	Actions
Searc	h															
				£	Session-Posture	eStatus EQU	IALS Compliant									
	0	FTD-VPN-Posture-Compliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000/ EmployeeVi	/ASA/PIX7x-Tunnel-Gr PN	roup-	×PermitAll	+	Select from	list		+	4	¢
				ĥ	Session Posture	eStatus EQU	IALS NonCompliant			_						
	0	FTD-VPN-Posture-NonCompliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000/ EmployeeVI	/ASA/PIX7x-Tunnel-Gr PN	roup-	× FTD-VPN-NonCompliant	+	Select from	list		+	0	¢
				Ŀ	Session Posture	eStatus EQU	JALS Unknown									
	$\odot$	FTD-VPN-Posture-Unknown	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000/ EmployeeVi	/ASA/PIX7x-Tunnel-Gr PN	roup-	× FTD-VPN-Redirect	+	Select from	list		+	9	¢

# 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。

ISEでは、最初の検証ステップはRADIUSライブログです。Operations > RADIUS Live Logの順に 移動します。ここで、ユーザAliceが接続され、期待される認可ポリシーが選択されます。

cisco Additionly Statistical Cright	le Home + Cor	text Visibility	* Operation	s → Policy → Ad	Iministration + Work Ce	nters						License War	ning 🔺 🔍	
RADIUS Threat-Centric I	NAC Live Logs + TACA	CS Troub	leshoot + Ad	aptive Network Control	Reports									
Live Logs Live Sessions														
	Misconfigured Su	pplicants 0		lisconfigured Network	Devices ()	RADIUS Dro	eps O	Cli	ent Stopped Res	ponding ()	Repeat	Counter ()		
	0			0		0			0			0		
														_
									Refr	esh Never	Show Lates	t 20 records	Within Last 3	hours 🗾
C Refresh O Reset Rep	eat Counts 🛛 🛓 Export	To •							Refr	esh Never	Show Lates	t 20 records	Within Last 3	Filter • •
C Refresh O Reset Rep Time	eat Counts 🕹 Export Status	To • Details	Repeat	identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Refr Authorizati	IP Address	Show Lates	Device Port	Within Last 3	Filter • • • • • • • • • • • • • • • • • • •
C Refresh O Reset Rep Time X	eat Counts 🔮 Export Status	To • Details	Repeat	Identity Identity	Endpoint D Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Refr Authorizati	IP Address	Show Lates	Device Port	Within Last 3 Identity Group	Filter • • • • Posture Stati
C Refresh O Reset Rep Time X Feb 03, 2020 07:13:31	eat Counts Z Export Status	Details	Repeat	Identity Identity alice@training.e	Endpoint ID Endpoint ID 00:00:29:50:54:98	Endpoint Pr Endpoint Prc Windows10	Authenticat Authenticatik Default >>	Authorizati Authorization Default >>;	Authorizati Authorizatior FTD-VPN-R	IP Address IP Address IP Address 172.16.1.10	Show Lates	Device Port Device Port	Within Last 3 Identity Group	Filter • • • • • • • • • • • • • • • • • • •
Refresh     Reset Rep     Time     Feb 03, 2020 07:13:31     Feb 03, 2020 07:13:29	eat Counts 2 Export Status	To + Details	Repeat	Identity Identity alice@training.e #ACSACL#-IP-P	Endpoint ID Endpoint ID 00:00:29:50:5A:90	Endpoint Pr Endpoint Prc Windows10	Authenticat Authenticatk Default >>	Authorizati Authorization Default >>	Authorizati Authorizatior FTD-VPN-R	P Address IP Address 172.16.1.10	Show Lates	Device Port Device Port	Within Last 3	Filter • O • Posture Stati Pending

認可ポリシーFTD-VPN-Posture-Unknownが一致し、その結果、FTD-VPN-ProfileがFTDに送信されます。

### **Overview**

Event	5200 Authentication succeeded	
Username	alice@training.example.com	
Endpoint Id	00:0C:29:5C:5A:98 ⊕	
Endpoint Profile	Windows10-Workstation	
Authentication Policy	Default >> Default	
Authorization Policy	Default >> FTD-VPN-Posture-Unknown	
Authorization Result	FTD-VPN-Redirect	

### **Authentication Details**

Source Timestamp	2020-02-03 07:13:29.738
Received Timestamp	2020-02-03 07:13:29.738
Policy Server	fyusifov-28-3
Event	5200 Authentication succeeded
Username	alice@training.example.com

# ポスチャステータスは保留中です。

結果セクションには、FTDに送信される属性が表示されます。

lesult	
Class	CACS:00000000000c0005e37c81a:fyusifov-26-3/368560500/45
cisco-av-pair	url-redirect-acl=fyusifovredirect
cisco-av-pair	url-redirect=https://fyusifov-28-3.example.com:8443/portal /gateway?sessionId=0000000000000005e37c81a& portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp& token=0d90f1cdf40e83039a7ad8a226603112
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

FTDで、VPN接続を確認するために、ボックスにSSHで接続し、system support diagnostic-cliを 実行してから、show vpn-sessiondb detail anyconnectを実行します。この出力から、ISEから送 信された属性がこのVPNセッションに適用されていることを確認します。

```
<#root>
fyusifov-ftd-64#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username
            : alice@training.example.com
Index
            : 12
Assigned IP : 172.16.1.10
            Public IP
                       : 10.229.16.169
            : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
            : AnyConnect Premium
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Encryption
Hashing
            : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx
            : 15326
                                     Bytes Rx
                                                 : 13362
Pkts Tx
            : 10
                                     Pkts Rx
                                                  : 49
Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy
Tunnel Group : EmployeeVPN
Login Time
           : 07:13:30 UTC Mon Feb 3 2020
Duration
            : 0h:06m:43s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                     VLAN
                                                   : none
Audt Sess ID : 000000000000005e37c81a
Security Grp : none
                                     Tunnel Zone : 0
```

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 12.1 Public IP : 10.229.16.169 Encryption : none Hashing : none TCP Src Port : 56491 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes : win Client OS Client OS Ver: 10.0.18363 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7663 Bytes Rx : 0 Pkts Tx : 5 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 12.2 Assigned IP : 172.16.1.10 Public IP : 10.229.16.169 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 56495 TCP Dst Port : 443 : userPassword Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes : Windows Client OS Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7663 Bytes Rx : 592 Pkts Tx : 5 Pkts Rx : 7 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d DTLS-Tunnel: Tunnel ID : 12.3 Assigned IP : 172.16.1.10 Public IP : 10.229.16.169 : AES256 Encryption Hashing : SHA1 Ciphersuite : DHE-RSA-AES256-SHA UDP Src Port : 59396 Encapsulation: DTLSv1.0 : userPassword UDP Dst Port : 443 Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 0 Bytes Rx : 12770 Pkts Tx : 0 Pkts Rx : 42 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PostureUnknown-5e37414d

ISE Posture: Redirect URL : https://fyusifov-26-3.example.com:8443/portal/gateway?sessionId=00000000000000005e37c83 Redirect ACL : fyusifovredirect クライアントプロビジョニングポリシーを確認できます。Operations > Reports > Endpoints and Users > Client Provisioningの順に移動します。

dentity Services Engine	Home + Context Visibili	y Operations Policy +	Administration + Work Centers			License Warr	ing 🔺 🔍 😝 👩 🔿
RADIUS Threat-Centric NAC Liv	e Logs + TACACS + Tro	ubleshoot + Adaptive Network Contr	ol Reports				
Export Summary	Client Provisioning From 2020-02-03 00:00:00 Reports exported in last 7 of	0 to 2020-02-03 08:14:07.0				+ My Reports	Z Export To • O Schedule
* Reports							
+ Audit	Logged At	Server	Event	Identity	Endpoint ID	IP Address	Client Provisioning Pol
Device Administration	Today 💌 🗙			Identity	Endpoint ID		
Diagnostics	2020-02-03 08:06:4	fyusifov-26-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	AC_47_Win
Endpoints and Users     Authentication Summary     Client Provisioning     Current Active Sessions	<u>.</u>					Rows/Page 1 V	1 📩 o or 1 Total Rows

AnyConnectから送信されたポスチャレポートをチェックできます。Operations > Reports > Endpoints and Users > Posture Assessment by Endpointの順に移動します。

dentity Services Engine	Home	▼Operations	Policy      Administratio	n			License Warning	<b>▲                                    </b>
+ RADIUS Threat-Centric NAC Li	ive Logs + TACACS + Troubl	leshoot + Adaptive	Network Control Reports					
Export Summary	Posture Assessment by E From 2020-02-03 00:00:00.0 t	Endpoint ()	48.0	-			+ My Reports	Export To - O Schedule
My Reports	Reports exported in last 7 days	s <b>0</b>						
- Reports							<b>T</b> F	Filter • 📿 Refresh 🔹 •
▶ Audit	Logged At	Status	Details PRA Actio	n	Identity	C Endpoint ID	IP Address	Endpoint OS
Device Administration	× Today •	<	•		Identity	Endpoint ID		Endpoint OS
▶ Diagnostics	2020-02-03 08:07:5	<b>~</b>	N/A		alice@training.example.com	00:0C:29:5C:5A:96	172.16.1.10	Windows 10 Professional
▼ Endpoints and Users	•						Rows/Page 1 💌 💷 1	► ► 1 Total Rows
Authentication Summary								
Current Active Sessions								
External Mobile Devic								
Manual Certificate Pro								
PassiveID								
Posture Assessment by								
Posture Assessment by								

ポスチャレポートの詳細を表示するには、Detailsをクリックします。

Identity Services Engine	
Posture More Detail Assessment	
From 2020-01-04 00:00:00.0 to 2020-02-03 08:13:38.0 Generated At: 2020-02-03 08:13:37:37	
Client Details	
Username	alice@training.example.com
Mac Address	00:0C:29:5C:5A:96
IP address	172.16.1.10
Location	All Locations
Session ID	00000000000c0005e37c81a
Client Operating System	Windows 10 Professional 64-bit
Client NAC Agent	AnyConnect Posture Agent for Windows 4.7.01076
PRA Enforcement	0
CoA	Received a posture report from an endpoint
PRA Grace Time	0
PRA Interval	0
PRA Action	N/A
User Agreement Status	NotEnabled
System Name	DESKTOP-IE3556M
System Domain	n/a

### ISEでレポートを受信すると、ポスチャステータスが更新されます。この例では、ポスチャステ ータスは準拠しており、CoAプッシュは新しい属性セットでトリガーされます。

S	Refresh 💿 Reset Repeat Cou	nts 🔮 Export To	-												<b>▼</b> Filter	- 0-
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Authorizati	IP Address		Network Device	Device Port	Identity Group	Posture \$
×		•			Identity	Endpoint ID	Endpoint Prc	Authenticatic	Authorization	Authorization	IP Address	•	Network Device	Device Port	Identity Group	Posture
	Feb 03, 2020 08:07:52.05	<b>~</b>	0			10.229.16.169				PermitAccess	7		FTD			Complia
	Feb 03, 2020 08:07:50.03	0	0	0	alice@training.e	00:0C:29:5C:5A:96	Windows10	Default >>	Default >>	FTD-VPN-R	172.16.1.10					Compliar
	Feb 03, 2020 07:13:29.74	<b>~</b>	0		#ACSACL#-IP-P								FTD			
	Feb 03, 2020 07:13:29.73		0		alice@training.e	00:0C:29:5C:5A:96	Windows10	Default >>	Default >>	FTD-VPN-R			FTD		Workstation	Pending
/																

Last Updated: Mon Feb 03 2020 09:10:20 GMT+0100 (Central European Standard Time)

Records Shown: 4

verview	
Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	10.55.218.19 🕀
Endpoint Profile	
Authorization Result	PermitAll

uthentication Details	
Source Timestamp	2020-02-03 16:58:39.687
Received Timestamp	2020-02-03 16:58:39.687
Policy Server	fyusifov-28-3
Event	5205 Dynamic Authorization succeeded
Endpoint Id	10.55.218.19
Calling Station Id	10.55.218.19
Audit Session Id	00000000000e0005e385132
Network Device	FTD
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.15.15
Authorization Profile	PermitAll
Posture Status	Compliant
Response Time	2 milliseconds

Other Attributes	
ConfigVersionId	21
Event-Timestamp	1580749119
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	af49ce55-d55c-4778-ad40-b03ea12924d2
CoASourceComponent	Posture
CoAReason	posture status changed
CoAReason CoAType	posture status changed COA-push
CoAReason CoAType Network Device Profile	posture status changed COA-push Cisco
CoAReason CoAType Network Device Profile Location	posture status changed COA-push Cisco Location#All Locations
CoAReason CoAType Network Device Profile Location Device Type	posture status changed         COA-push         Cisco         Location#AII Locations         Device Type#AII Device Types
CoAReason CoAType Network Device Profile Location Device Type IPSEC	posture status changed         COA-push         Cisco         Location#All Locations         Device Type#All Device Types         IPSEC#ls IPSEC Device#No
CoAReason CoAType Network Device Profile Location Device Type IPSEC Device IP Address	posture status changed         COA-push         Cisco         Location#All Locations         Device Type#All Device Types         IPSEC#Is IPSEC Device#No         192.168.15.15

FTDで、VPNセッション用の新しいリダイレクトACLとリダイレクトURLが削除され、PermitAll DACLが適用されていることを確認します。

<#root>
fyusifov-ftd-64#
show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username :
alice@training.example.com
Index : 14
Assigned IP : 172.16.1.10 Public IP : 10.55.218.19

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256 Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1 Hashing : 53990 Bytes Tx Bytes Rx : 23808 : 73 Pkts Rx : 120 Pkts Tx Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : EmployeeVPN Login Time : 16:58:26 UTC Mon Feb 3 2020 : 0h:02m:24s Duration Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 000000000000005e385132 Security Grp : none Tunnel Zone : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 14.1 Public IP : 10.55.218.19 Encryption : none Hashing : none TCP Src Port : 51965 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : win Client OS Ver: 10.0.18363 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7663 Bytes Rx : 0 Pkts Tx Pkts Rx : 5 : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 14.2 Assigned IP : 172.16.1.10 Public IP : 10.55.218.19 Encryption : AES-GCM-256 : SHA384 Hashing Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 51970 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 Bytes Tx : 7715 Bytes Rx : 10157 Pkts Tx : 6 Pkts Rx : 33 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PermitAll-5e384dc0 DTLS-Tunnel: Tunnel ID : 14.3 Assigned IP : 172.16.1.10 Public IP : 10.55.218.19 : SHA1 Encryption : AES256 Hashing Ciphersuite : DHE-RSA-AES256-SHA Encapsulation: DTLSv1.0 UDP Src Port : 51536 UDP Dst Port : 443 Auth Mode : userPassword

Idle Time Out	:	30 Minutes		Idle TO	Left	:	28	Minutes
Client OS	:	Windows						
Client Type	:	DTLS VPN Client						
Client Ver	:	Cisco AnyConnect	VPN	Agent for	Windo	SW:	s4.	7.01076
Bytes Tx	:	38612		Bytes R>	(	:	136	551
Pkts Tx	:	62		Pkts Rx		:	87	
Pkts Tx Drop	:	0		Pkts Rx	Drop	:	0	
Filter Name	:							

#ACSACL#-IP-PermitAll-5e384dc0

fyusifov-ftd-64#

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。

ポスチャフローの詳細と、AnyConnectおよびISEのトラブルシューティングについては、次のリ ンクを確認してください。 <u>ISE ポスチャ スタイルの 2.2 前後の比較</u>

• こぼれたトンネル

スプリットトンネルが設定されている場合の一般的な問題の1つです。この例では、すべてのトラ フィックをトンネリングするデフォルトのグループポリシーが使用されます。特定のトラフィッ クだけがトンネル化される場合は、ISEおよびその他の内部リソースへのトラフィックに加えて 、AnyConnectプローブ(enroll.cisco.comおよび検出ホスト)もトンネルを通過する必要があります 。

FMCのトンネルポリシーを確認するには、まず、VPN接続に使用されているグループポリシーを 確認します。Devices > VPN Remote Accessの順に移動します。

Overview Analysis Policies Devices	Objects AMP Intelligence		De	ploy 🧕 System Help 🔻 admin 🔻
Device Management NAT VPN > Remot	te Access QoS Platform Settings	FlexConfig Certificates		
EmployeeVPN Enter Description				Save Save
Connection Profile Access Interfaces	Advanced			Policy Assignments (1)
				0
Name	ААА		Group Policy	
DefaultWEBVPNGroup	Authentication: / Authorization: / Accounting: /		DfltGrpPolicy	/ 5
EmployeeVPN	Authentication: I Authorization: I Accounting: I	ISE (RADIUS) ISE (RADIUS) ISE (RADIUS)	DftGrpPolicy	/ 5

次に、Objects > Object Management > VPN > Group Policyの順に移動し、VPN用に設定された Group Policyをクリックします。

Overview Analysis Policies Devices Objects	AMP Intelligence	
Object Management Intrusion Rules		
Object Management       Intrusion Rules         Group Policy       A Group Policy is a set of attribute and value pairs, stored in a generative stored in a generative stored in a generative store of a generative store sto	Edit Group Policy       ? ×         Name:*       DftGrpPolicy         Description:	icy or
IKEv1 Policy     IKEv2 IPsec Proposal	Save Cancel	
B IKEv2 Policy		Disp

• アイデンティティNAT

もう1つの一般的な問題は、VPNユーザのリターントラフィックが誤ったNATエントリを使用し て変換されることです。この問題を解決するには、アイデンティティNATを適切な順序で作成す る必要があります。

最初に、このデバイスのNATルールを確認します。Devices > NATの順に移動し、Add Ruleをクリックして新しいルールを作成します。

Ov	Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🍳 System Help 🔻 admin 🔻											
Dev	vice Management	NAT	VPN VO	6 Platform Set	tings FlexConfig	Certificates						
FT	D_11		_							A Show Warnings	Save	🔀 Cancel
Ente	r Description											
	_										📑 Policy As	ssignments (1)
Rule	25											
台Fi	ter by Device										0	Add Rule
						Original Packet			Translated Packet		•	
#	Direction	Туре	Source Interface Ob	Destination Interface Ob	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
• N/	AT Rules Before											

開いているウィンドウのInterface Objectsタブで、Security Zonesを選択します。この例では、 NATエントリはZONE-INSIDEからZONE-OUTSIDEに作成されます。

Add NAT Rule						? :
NAT Rule:	Manual NAT Rule	<b>▼</b>	Insert:	In Category	VAT Rules Befo	ore 💌
Type:	Static	▼ Fnable	e			
Description:						
Interface Objects	Translation PA	T Pool Advance	ced			
Available Interface C	)bjects 🖒		Source Interface Object	ts (1)	Destination Interface	e Objects (1)
Search by name			ZONE-INSIDE	ũ	ZONE-OUTSIDE	ii ii
ZONE-INSIDE						
ZONE-OUTSIDE		Add to				
		Source				
		Add to Destination				
						OK Cancel

Translationタブで、元のパケットと変換されたパケットの詳細を選択します。アイデンティティ NATであるため、送信元と宛先は変更されません。

Edit NAT Rule									? :	×
NAT Rule:	Manual NAT Ru	le 💌	Inser	t:		In Category	NAT Rules	Before 💌		
Туре:	Static	<b>~</b>	🗹 Enable							
Description:										
Interface Objects	Translation	PAT Pool	Advanced							
Original Packet					Translat	ed Packet				
Original Source:*	any			<b>~</b> 📀	Translate	d Source:	Address		<b>~</b>	
Original Destination:	Address		•	~			any		<b>~</b> O	
	VPN_Subr	iet		• 📀	Translate	d Destination:	VPN_Subnet		<b>V</b> O	
Original Source Port:				• 💿	Translate	d Source Port:			<b>v</b> 📀	1
Original Destination Po	ort:			• 0	Translate	d Destination Port:			<b>v</b> 🔾	
								ок	Cancel	

Advancedタブで、次の図に示すようにチェックボックスをオンにします。

Edit NAT Rule						? >
NAT Rule:	Manual NAT F	Rule 💌	Insert:	In Category	▼ NAT Rules 8	Before 💙
Type:	Static	•	Enable			
Description:						
Interface Objects	Translation	PAT Pool	Advanced			
Translate DNS repl	ies that match tl	his rule				
Fallthrough to Inter	face PAT(Destin	ation Interfac	ce)			
IPv6						
Net to Net Mapping						
Do not proxy ARP	on Destination I	nterface	7			
Perform Route Loo	kup for Destinat	ion Interface				
🗖 Unidirectional			- `			
					[	OK Cancel

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。