Configuration de la position ISE sur AnyConnect Remote Access VPN sur FTD

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Diagramme et flux du trafic du réseau
Configurations
FTD/FMC
<u>ISE</u>
Vérifier
Dépannage

Introduction

Ce document décrit comment configurer Firepower Threat Defense (FTD) version 6.4.0 pour positionner les utilisateurs VPN par rapport à Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN d'accès à distance AnyConnect
- Configuration VPN d'accès à distance sur le FTD
- · Services Identity Services Engine et services de posture

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Cisco Firepower Threat Defense (FTD) versions 6.4.0
- Logiciel Cisco Firepower Management Console (FMC) version 6.5.0
- Microsoft Windows 10 avec Cisco AnyConnect Secure Mobility Client version 4.7
- Cisco Identity Services Engine (ISE) version 2.6 avec patch 3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme et flux du trafic du réseau



- 1. L'utilisateur distant utilise Cisco Anyconnect pour l'accès VPN au FTD.
- 2. Le FTD envoie une requête d'accès RADIUS pour cet utilisateur à l'ISE.

3. Cette demande atteint la stratégie nommée FTD-VPN-Posture-Unknown sur l'ISE. L'ISE envoie un message d'acceptation d'accès RADIUS avec trois attributs :

- cisco-av-pair = url-redirect-acl=fyusifovredirect Il s'agit du nom de la liste de contrôle d'accès (ACL) définie localement sur le FTD, qui décide du trafic qui est redirigé.
- cisco-av-pair = urlredirect=<u>https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-</u> <u>11e9-98fb-0050568775a3&action=cpp</u> - II s'agit de l'URL vers laquelle l'utilisateur distant est redirigé.
- DACL = PERMIT_ALL_IPV4_TRAFFIC ACL téléchargeable : cet attribut est facultatif. Dans ce scénario, tout le trafic est autorisé dans DACL)

4. Si la DACL est envoyée, RADIUS Access-Request/Access-Accept est échangé afin de télécharger le contenu de la DACL

5. Lorsque le trafic provenant de l'utilisateur VPN correspond à la liste de contrôle d'accès définie localement, il est redirigé vers le portail d'approvisionnement du client ISE. ISE provisionne le module de posture et le module de conformité AnyConnect.

6. Une fois l'agent installé sur l'ordinateur client, il recherche automatiquement ISE avec des sondes. Lorsque ISE est détecté avec succès, les exigences de posture sont vérifiées sur le terminal. Dans cet exemple, l'agent recherche tout logiciel anti-programme malveillant installé. Il envoie ensuite un rapport de position à l'ISE.

7. Lorsqu'ISE reçoit le rapport de position de l'agent, elle modifie l'état de position pour cette session et déclenche le type RADIUS CoA Push avec de nouveaux attributs. Cette fois, l'état de la position est connu et une autre règle est activée.

- Si l'utilisateur est conforme, un nom DACL autorisant un accès complet est envoyé.
- Si l'utilisateur n'est pas conforme, un nom DACL autorisant un accès limité est envoyé.

8. Le FTD supprime la redirection. FTD envoie une requête d'accès afin de télécharger la liste de contrôle d'accès depuis ISE. La liste de contrôle d'accès spécifique est attachée à la session VPN.

Configurations

FTD/FMC

Étape 1. Créez un groupe d'objets réseau pour ISE et les serveurs de conversion (le cas échéant). Accédez à Objets > Gestion des objets > Réseau.

Overview Analysis	Policie	s Devices Objects AM	IP Intelligence					
Object Management	Intrus	sion Rules						
Network								
A network object represen	its one o	or more IP addresses. Network obj	ects are used in va	rious places, includi	ng access control	policies, network va	riables, intrusion r	ules, identity rules, ne
Extended		Name					Value	
Standard		any-ipv4					0.0.0.0	/0
Address Pools								
IPv4 Pools		any-ipv6					::/0	
IPV6 Pools		enroll.cisco.com					72.163.	1.80
Application Filters		IPv4-Benchmark-Tests	Edit Network	Object				2 X
Y AS Path		The difference of	Eurencework					
Community List		IPV4-LINK-LOCAI	Name	ISE_PSN				
A A Distinguished Name		IPv4-Multicast	Description					
Individual Objects	;	IPv4-Private-10.0.0.0-8						
Company Compan		IPv4-Private-172.16.0.0-12	Network	Host	C Range	C Network	C FQDN	
File List		IPv4-Private-192.168.0.0-16		192.168.15.14				
A D FlexConfig			Allow Overrides		1			
FlexConfig Object		IPv4-Private-All-RFC1918		-				
🚱 Text Object							Save	Cancel
Geolocation		IPv6-IPv4-Mapped					::###:0.	0.0.0/96
Interface		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

Étape 2. Créer une ACL de redirection. Accédez à Objets > Gestion des objets > Liste d'accès > Étendue. Cliquez sur Add Extended Access List et fournissez le nom de Redirect ACL. Ce nom doit être le même que dans le résultat de l'autorisation ISE.

Overview Analysis Policies	Devices Obj	ects AMP	Intelligence				
Object Management Intrusion	n Rules						
Extended An access list object, also known as a Supports IPv4 and IPv6 addresses. Yi	an access control li ou use these object	st (ACL), selec ts when config	ts the traffic to which a se juring particular features, s	rvice will apply. Standard-Iden such as route maps.	tifies traffic based on destinati	on address only. Identifies traffic	Add Extended Access List
Access List	New Extended	Access List	t Object				? ×
Extended Standard	Name	fyusifoyredi	rect				
Address Pools	Entries (0)	17 dan off dan	uuq				
IPv4 Pools							😡 Add
IPv6 Pools	Sequence	Action	Source	Source Port	Destination	Destination Port	
Y AS Path							
💮 Cipher Suite List				No records	s to display		
🝰 Community List							
A 🖓 Distinguished Name							
Individual Objects							
Object Groups							
DNS Server Group	Allow Overrides						
A On Elex Confin							Save Cancel
G FlexConfig Object							

Étape 3. Ajouter des entrées ACL de redirection. Cliquez sur le bouton Add. Bloquez le trafic vers DNS, ISE et les serveurs de conversion pour les exclure de la redirection. Autorisez le reste du trafic, ce qui déclenche la redirection (les entrées de la liste de contrôle d'accès peuvent être plus spécifiques si nécessaire).

Add Extended A	Access List Entry				? ×
Action:	× Block	~			
Logging:	Default	•			
Log Level:	Informational	*			
Log Interval:	300	Sec.			
Network Po	rt				
Available Netwo	rks Ċ	٢	Source Networks (1)	Destination Netw	orks (1)
Search by nam	me or value		📻 any-ipv4	ISE_PSN	6
any		-			
any-ipv6		Add to Source			
enroll.cisco.c	com	Add to			
IPv4-Benchn	nark-Tests	Destination			
IPv4-Link-Lo	cal				
IPv4-Multicas	st				
IPv4-Private	-10.0.0.0-8				
IPv4-Private	-172.16.0.0-12	•	Enter an IP address	Add Enter an IP addre	ss Add
					Add Cancel

ame	e fyusifovredirect								
ntries (4)						O Add			
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	a			
3	🗙 Block	any-ipv4	Any	RemediationServers	Any	a			
4	Allow	any-ipv4	Any	any-ipv4	Any	a 🛛			

Étape 4. Ajoutez des noeuds PSN ISE. Accédez à Objets > Gestion des objets > Groupe de serveurs RADIUS. Cliquez sur Add RADIUS Server Group, puis fournissez un nom, activez toutes les cases à cocher et cliquez sur l'icône plus.

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 ser	vers)		
IP Address/Hostname			
	No records to display		
		Save	Cancel

Étape 5. Dans la fenêtre ouverte, fournissez l'adresse IP du PSN ISE, la clé RADIUS, sélectionnez Specific Interface et sélectionnez l'interface à partir de laquelle ISE est accessible (cette interface est utilisée comme source de trafic RADIUS), puis sélectionnez Redirect ACL qui a été configuré précédemment.

New RADIUS Server	? ×	
IP Address/Hostname:*	192.168.15.13 Configure DNS at Threat Defense Platform Settings to resolve hostname	
Authentication Port:*	1812 (1-65535)	
Key:*	•••••	
Confirm Key:*	•••••	
Accounting Port:	1813 (1-65535)	
Timeout:	10 (1-300) Seconds	
Connect using:	C Routing 🖲 Specific Interface 🕕	
	ZONE-INSIDE	
Redirect ACL:	fyusifovredirect 🗸	
	Save Cancel	

Étape 6. Créez un pool d'adresses pour les utilisateurs VPN. Accédez à Objets > Gestion des objets > Pools d'adresses > Pools IPv4. Cliquez sur Add IPv4 Pools et renseignez les détails.

Oversiew Applysic	Policies Davises Objects AMD Tatallisence	Deploy 0 St
Object Management	Tetracian Pulses	Depidy 43 Sy
Object Management	Indusion Rules	
TPv4 Pools		Add IPv4 Pools
IPv4 pool contains list of I	Pv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.	
Standard	A Name	Value
Address Pools	Edit IPv4 Pool ? ×	172.16.1.10-172.16.1.20
IPV4 Pools	Name* VPN-172-Pool	
Application Filters		
Y AS Path	IPv4 Address Range* 172.16.1.10-172.16.1.20	
Cipher Suite List	Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150	
Community List	Mask 255.255.255.0	
A 🗐 Distinguished Name	Description	
Individual Objects		
📇 Object Groups		
BNS Server Group	Allow Overrides 🔽	
File List	Oconfigure device overrides in the address pool object to avoid IP address conflicts in case of object	
4 🗛 FlexConfig	is shared across multiple devices	
FlexConfig Object	Override (0)	
Ca Text Object		
Geolocation	Save Cancel	
🕞 Interface		

Étape 7. Créez un package AnyConnect. Accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect. Cliquez sur Add AnyConnect File, fournissez le nom du package, téléchargez le package à partir de Cisco Software Download et sélectionnez Anyconnect Client Image File Type.



Étape 8. Accédez à Objets de certificat > Gestion des objets > PKI > Inscription de certificat. Cliquez sur Add Cert Enrollment, fournissez un nom, choisissez Self Signed Certificate in Enrollment Type. Cliquez sur l'onglet Certificate Parameters et indiquez CN.

Overview Analysis F	Policies Devices Objects	AMP Intelligence	Deploy 🍳 Sy
Object Management	Intrusion Rules		
Cert Enrollment A certificate enrollment obje	ect contains the Certification Auth	rity (CA) server information and enrollment parameters that are required for creatin	Gertificate Signing Requests (CSRs) and obtaining Identity Certificates fr
Access List	Add Cert Enrollmer	t ?	Х
 Address Pools Application Filters As Path Coher Suite List 	Name* Description	vpn-cert	Self Signed Ce
Community List	CA Information	Certificate Parameters Key Revocation	-
○ File List > > > FlexConfig <	Common Name (configure CN, ples	N) is mandatory for self-signed certificate that is used in Remote Access VPN. To se navigate to 'Certificate Parameters' tab.	
Key Chain			
Cert Enrollment External Cert Grou External Certs type="color: blue;"> Certs Certs Certs Certs Certs Certs Certs Certs Certs Certs Certs Certs	ps		
Internal CA Groups	os		
Trusted CA Groups	Allow Overrides		
de Port	-	Save	Displaying 1 - 1 of 1 rows 🛛 🕹

A	Add Cert Enrollme	ent						? ×
	Name*	vpr	-cert					
	Description							
	CA Information	Certific	ate Parameters	Key	Revocation			
	Include FQDN:		Use Device Hostna	me as f	QDN		~	
	Include Device's IP	Address:	10.48.26.99					
	Common Name (CN	N):	vpn-cert.example.	com				
	Organization Unit (0	DU):						
	Organization (O):		example					
	Locality (L):							
	State (ST):		Krakow					
	Country Code (C):		PL					
	Email (E):							
	Include Device's	Serial Nu	mber					
		_						
	Allow Overrides							
						Save		Cancel

Étape 9. Lancez l'assistant VPN d'accès à distance. Accédez à Devices > VPN > Remote Access et cliquez sur Add.

Overview Analysis	Policies	Devices Objects	АМР	Intelligence			Deploy 🤐	System Help 🔻 admin 🔻
Device Management	NAT	VPN Remote Access	QoS	Platform Settings	FlexConfig	Certificates		
								🔘 Add
Name				Status		Last Modified		
No configuration available Add a new configuration								

Étape 10. Fournissez le nom, cochez SSL as VPN Protocol, choisissez FTD qui est utilisé comme concentrateur VPN et cliquez sur Next.

Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Profile 3 AnyConne	t $>$ 4 Access & Certificate $>$ 5 Summary		
Targeted Devices and Protocols This wizard will guide you through the requirement of the requirement	v2 Selected Devices I 192.166.15.11	<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

Étape 11. Fournissez le nom du profil de connexion, sélectionnez Serveurs d'authentification/de comptabilité, sélectionnez le pool d'adresses qui a été configuré précédemment et cliquez sur Suivant.

Remarque : ne sélectionnez pas le serveur d'autorisation. Il déclenche deux demandes d'accès pour un seul utilisateur (une fois avec le mot de passe utilisateur et la deuxième fois avec le mot de passe cisco).

Policy Assignment Connection Pro	3 AnyConnect 4 Access & Certificate 5 Summary	
	Connection Profile:	
	Connection Profiles specify the tunnel group policies for a VPII connection. These policies pertain to creating the tunnel Itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.	
	Connection Profile EmployeeVPN Name:*	
	This name is configured as a connection alias, it can be used to connect to the VPN gateway	
	Authentication, Authorization & Accounting (AAA):	
	Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.	
	Authentication Method: AAA Only V	
	Authentication Server:* ISE C. (Realm or RADIUS)	
	Authorization Server: Use same authentication server 🔍 🚱 (RADIUS)	
	Accounting Server: ISE V (RADIUS)	
	Client Address Assignment:	
	Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.	
	Use AAA Server (RADIUS only) 🕕	
	Use DHCP Servers	
	Use IP Address Pools	
	IPv4 Address VPN-172-Pool	
	IPv6 Address	
	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:* DfltSrpPolicy V Edit Group Policy	

Étape 12. Sélectionnez le package AnyConnect qui a été configuré précédemment et cliquez sur Next.

Remote Access VPN Policy Wizard		
1 Policy Assignment 2 2 Connection Profile 3	3 AnyConnect 4 Access & Certificate 5 Summary	
Remote User	Client Image	
The VPN gatewar connection is initia	ay can automatically download the latest AnyConnect package to the client device when the VPN liated. Minimize connection setup time by choosing the appropriate OS for the selected package.	
Download AnyCon	onnect Client packages from Cisco Software Download Center. Show Re-order buttons	
AnyConnec	ect File Object Name AnyConnect Client Package Name Operating System	
✓ AC47	anyconnect-win-4.7.01076-webdeploy-k9 Windows	
		Jack Next

Étape 13. Sélectionnez l'interface à partir de laquelle le trafic VPN est attendu, sélectionnez Certificate Enrollment qui a été configuré précédemment et cliquez sur Next.

Remote Access VPN Policy Wizard			
1 Policy Assignment 2 2 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: Interface DTLS on member interfaces			
Device Certificates Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authencicate the UCN gateway Certificate Enrollment:* Vpn-cert 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. Physical Second Second Policy for decrypted traffic (sysopt permit-vpn) This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.			
	Back	Next	Cancel

Étape 14. Consultez la page de résumé et cliquez sur Terminer.

Remote Access VPN Policy Confi	tion	Additional Configuration Requirements
Firepower Management Center will o Name: Device Targets: Connection Profile: Connection Alias: AAA: Authentication Method: Authorization Server: Authorization Server: Address Assignment: Address Assignment: Address from AAA: DHCP Servers: Address Pools (IPv4): Address Pools (IPv6): Group Policy: AnyConnet Images: Interface Objects: Device Certificates:	vre an RA VPN Policy with the following settings loyeeVPN 92.168.15.11 loyeeVPN Only SE SE SE VPN-172-Pool VPN-172-Pool VPN-172-Pool VPN-172-Pool PftGrpPolicy IC47 VONE-OUTSIDE pn-cert	 After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets. Access Control Policy Update An Access Control Policy Update An Exemption If NAT is enabled on the targeted devices, you must define a <u>NAT Policy</u> to exempt VPN traffic. DNS Configuration To resolve hostname specified in AAA Servers or CA Servers, configure DNS using <i>ElexConfig Policy</i> on the targeted devices. Port Configuration SSL will be enabled on port 443. Please ensure that these ports are not used in <u>MAT Policy</u> to configuration. Metwork Interface Configuration Metwork Interface Configuration Make sure to add interface from targeted devices to SecurityZone object 'ZONE-OUTSIDE'

Étape 15. Déployer la configuration sur FTD. Cliquez sur Deploy et sélectionnez FTD qui est utilisé comme concentrateur VPN.

Overview Analysis Policies Devi	ces 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	9	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

Étape 1. Exécutez les mises à jour de posture. Accédez à Administration > System > Settings > Posture > Updates.

Posture Updates								
Web Offline								
* Update Feed URL https://www.cisco.com/w	veb/secure/spa/posture-update.xml Set to Default							
Proxy Address	(i)							
Proxy Port HH MM SS								
Automatically check for updates starting from	n initial delay 20 v 49 v 18 v every 2 hours (i)							
Save Update Now Reset	Save Update Now Reset							
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							

Étape 2. Téléchargez le module de conformité. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources. Cliquez sur Add et sélectionnez Agent resources from Cisco site

Download Remote Resources	×
Name 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 4.3.1053.6	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 Pal
For AnyConnect software, please download from http://ci	sco.com/go/anyconnect. Use the "Agent resource from local disk" add
option, to import into ISE	
	Save Cancel

Étape 3. Téléchargez AnyConnect à partir de <u>Cisco Software Download</u>, puis téléchargez-le vers ISE. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources.

Cliquez sur Add et sélectionnez Agent Resources From Local Disk. Choisissez Cisco Provided Packages sous Category, sélectionnez le package AnyConnect à partir du disque local et cliquez sur Submit.

Agent Resources From Local Disk > Agent Resources From Local Disk Agent Resources From Local Disk										
Category	Cisco Provided Packages	•								
	Browse anyconnect-win-4.7.010	Browse anyconnect-win-4.7.01076-webdeploy-k9.pkg								
	 AnyConnect Uploaded Resource 	s								
	Name 🔺	Туре	Version	Description						
	AnyConnectDesktopWindows 4.7.10	AnyConnectDesktopWindows	4.7.1076.0	AnyConnect Secure Mobility Clie						



Étape 4. Créez un profil de position AnyConnect. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources.

Cliquez sur Add et sélectionnez AnyConnect Posture Profile. Renseignez le nom et le protocole de posture.

Sous *Server name rules, placez * et placez toute adresse IP factice sous Discovery host.

ISE Posture Agent Profile Settings > AC_Posture_Profile											
* Name: 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								
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent 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								
Call Home List		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 Breastioning notable	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.								

Étape 5. Accédez à Policy > Policy Elements > Results > Client Provisioning > Resources et créez AnyConnect Configuration. Cliquez sur Add et sélectionnez AnyConnect Configuration. Sélectionnez AnyConnect Package, indiquez le nom de la configuration, sélectionnez Compliance Module, activez Diagnostic and Reporting Tool, sélectionnez Posture Profile et cliquez sur Save.

Enter value of back-off timer in seconds, the supported range is

between 10s - 600s.

30

secs

Back-off Timer

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

* Select AnyConnect Package	AnyConnectDesktopWindows 4.7.1076.0	
Description		
	11.	
Description * Compliance Module	Value AnyConnectComplianceModuleWindows 4.3.1012.6 -	Notes

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	v	
Web Security	*	
AMP Enabler	*	
Network Visibility	*	
Umbrella Roaming Security	*	
Customer Feedback	v	

Étape 6. Accédez à Policy > Client Provisioning et créez Client Provisioning Policy. Cliquez sur Edit, puis sélectionnez Insert Rule Above, fournissez un nom, sélectionnez OS et choisissez AnyConnect Configuration qui a été créé à l'étape précédente.

cisco iden	tity Services Engine	Home	Context Visib	ility	Operations	Policy	Administration	Work Centers			License Warning 🔺	Q	0	0	Φ.
Policy Sets	Profiling Posture	Client Provisi	ioning + Policy	Elemen	ts										
Client Prov Define the Cli For Agent Cor For Native Su	isioning Policy ent Provisioning Policy to Ifiguration: version of age pplicant Configuration: w	determine what int, agent profil izard profile an	at users will recei e, agent complian d/or wizard. Drag	ve upon l ce modu and drop	login and user sessi ale, and/or agent cus rules to change the	on initiation: tomization pa order.	ackage.								
*															
	Rule Name		Identity Groups		Operating System	s	Other Condition	ns	dia a s	Results					
	AC_47_Win	1	Any	and	Windows All	and	Condition(s)		then	AC_CF_47				Edit	
	IOS	lf	Any	and	Apple iOS All	and	Condition(s)		then	Cisco-ISE-NSP				Edit •	
	Android	lf	Any	and	Android	and	Condition(s)		then	Cisco-ISE-NSP				Edit •	
	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 •	
	MAC OS	H	Any	and	Mac OSX	and	Condition(s)		then	CiscoTemporalAgentO SX 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE- NSP				Edit •	
	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)		then	Cisco-ISE-Chrome- NSP				Edit •	

Étape 7. Créez une condition de posture sous Stratégie > Éléments de stratégie > Conditions > Posture > Condition anti-programme malveillant. Dans cet exemple, "ANY_am_win_inst" prédéfini est utilisé.

•

cisco Identity Services Engine	Home	◆ Operations ▼ Policy	 Administration 	Work Centers
Policy Sets Profiling Posture (Client Provisioning Policy Elem	ents		
Dictionaries - Conditions - Res	sults			
Library Conditions Smart Conditions Time and Date Profiling Posture Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Disk Encryption Condition File Condition	Anti-Malware Conditions	Delete Description Any AM installation ch Any AM definition check Any AM installation ch Any AM definition check Any AM definition check Any AM definition check	eck on Wi ck on Wind eck on Mac ck on Mac	

Étape 8. Naviguez jusqu'à Policy > Policy Elements > Results > Posture > Remediation Actions et créez Posture Remediation. Dans cet exemple, il est ignoré. L'action corrective peut être un message texte.

Étape 9. Accédez à Policy > Policy Elements > Results > Posture > Requirements et créez Posture Requirements. Condition prédéfinie : Any_AM_Installation_Win est utilisé.

cisco Identity Services Engine	Home Context Visibility	Operations -Policy	Administration Work Centers		License Warning 🔺 🔍	. 0 0	ø
Policy Sets Profiling Posture Cli	ent Provisioning Policy Elements	5					
Dictionaries + Conditions - Result	s						
0							
Authentication					-		P
	Requirements						
 Authorization 	Name	Operating Systems	Compliance Module	Posture			
1 Berline	Message 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	AnyAl/DefRemediationMa c					Edit •	1
- Demodiation 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 🕶	- 1
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 Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_def	then	
	AnyAMDefRemediationM					Edit •	•

Étape 10. Créez des stratégies de posture sous Stratégies > Posture. La stratégie de posture par défaut de tout contrôle anti-programme malveillant pour le système d'exploitation Windows est utilisée.

alta CIS	dentity	Services Engine	Home	ity + Operations	• Policy	Administration + Work Center	5			License	Naming 🔺 🤇	ર 😐	•	ø
P	licy Sets I	Profiling Postur	e Client Provisioning + Pol	icy Elements										
Pot	ture Policy	re Policy by config	juring rules based on operating s	ystem and/or other oc	nditions.						-			P
*														_
_	Status	Policy Options	Rule Name	Identity Groups	Operating	g Systems Compliance I	Module Posture Type		Other Conditions	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			ldit •	
	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			Edit •	
		Policy Options	Default_AntiMalware_Policy If _Win	Any	and Windows All	and 4.x or later	and AnyConnect	and	then	Any_AM_Installation_ Win			Edit 🕶	
	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			Edit 🔻	
	0	Policy Options	Default_AppVis_Policy_Mac If	Any	and Mac OSX	and 4 x or later	and AnyConnect	and	then	Default_AppVis_Requ irement_Mac		E	Edit +	

Étape 11. Accédez à Policy > Policy Elements > Results > Authorization > Downlodable ACLS et créez des DACL pour différents états de posture.

Dans cet exemple :

- DACL Posture Unknown : autorise le trafic vers DNS, PSN, HTTP et HTTPS.
- DACL non conforme à la position : refuse l'accès aux sous-réseaux privés et autorise uniquement le trafic Internet.
- Permit All DACL : autorise tout le trafic pour l'état de conformité à la position.

Downloadable ACL List > PostureNonCompliant1

Downloadable ACL

* Name	PostureUnknown
Description	
IP version	● IPv4 C IPv6 C Agnostic ①
* DACL Content	1234567 permit udg any any eq domain
	131111 permit (g any host 192, 168, 15, 14
	2 13 14 13 permit kg any any gg 00 1617181 permit kn any any en 443
	9002122
	2324252
	6272829
	3031323
	3343536
	3738394

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name	PostureNonCompliant
Description	
IP version	● IPv4 C IPv6 C Agnostic
* DACL Content	1234567 deny jg any 10.0.0 255.0.0.0
	8910111 deny ig any 172.16.0.0 255.240.0.0
	2131415 deny ig any 192.168.0.0 255.255.0.0
	1617181 permit ig any any
	9202122
	2324252
	6272829
	3031323
	3343536
	3738394

* Name	PermitAll
Description	
IP version	€ IPv4 C IPv8 C Agnostic (i)
ACL Content	123456 permit jg any any
	121314
	151817
	181920
	242526
	272829
	303132

Étape 12. Créez trois profils d'autorisation pour les états Posture Unknown, Posture NonCompliant

et Posture Compliant. Pour ce faire, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Dans le profil Posture Unknown, sélectionnez Posture Unknown DACL, cochez Web Redirection, sélectionnez Client Provisioning, fournissez le nom de la liste de contrôle d'accès de redirection (qui est configurée sur FTD) et sélectionnez le portail.

Authorization Profiles > New	Authorization Profile		
Authorization Profile			
* Name	FTD-VPN-Redirect]	
Description			li.
* Access Type	ACCESS_ACCEPT]	
Network Device Profile	dete Cisco 👻 🕀		
Service Template			
Track Movement			
Passive Identity Tracking	(<i>i</i>)		
▼ Common Tasks			
DACL Name	PostureUnknown	٢	
Web Redirection (CWA N			
Client Provisioning (Post	re) - ACL fyu	usifovredirect	Value It Provisioning Portal (default) 🔻
✓ Attributes Details			
Access Type = ACCESS_ACCEPT DACL = PostureUnknown cisco-av-pair = url-redirect-acl=fyusifov cisco-av-pair = url-redirect=https://ip:	edirect ort/portal/gateway?sessionId=SessionIdValue&p	portal=27b1bc30-2e58-11e9-98fb-0050!	568775a3&action=cpp

Dans le profil Posture NonCompliant, sélectionnez DACL afin de limiter l'accès au réseau.

Authorization Profiles > New Authorization Profile

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

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PostureNonCompliant

fil D źГ **.**+i. lot Da n: 4 c יה D. à u réseau. 4 \sim

Dans le profil Postul	e Compliant, selectionnez DACL atin d'autoriser l'acces complet au l
Authorization Profiles > Ne Authorization Profile	w Authorization Profile
Autionzation Frome	
* Name	PermitAll
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	🗰 Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
▼ Common Tasks	
DACL Name	PermitAll
▼ Attributes Details	
Access Type = ACCESS_ACCEPT DACL = PermitAll	

Étape 13. Créez des stratégies d'autorisation sous Stratégie > Jeux de stratégies > Par défaut > Stratégie d'autorisation. En tant que condition Posture Status et VNP TunnelGroup Name est utilisé.

alada Id	lentity Sen	vices Engine Home • C	context Vis	ibility	 Operations 		Administration	• Work Ce	nters		License Warning 🔺	٩	0	•
Policy S	Sets Profi	ling Posture Client Provisionin	g ⊧Po	licy Elen	nents		-							
	\odot	Default	Default p	olicy set							Default Network Access		× * +	43
		Dallar (D)												
 Autr 	nenucation	Policy (3)												
> Auti	horization I	Policy - Local Exceptions												
> Auti	horization I	Policy - Global Exceptions												
× Aut	horization I	Policy (18)												
- Pada	nonzation	oncy (10)												
+									Results					
•	Status	Rule Name	Condit	ions					Profiles	Security	Groups		Hits	Actions
Searc	ch													
				Ê;	Session-Posture	Status EQU	IALS Compliant			_				
	\odot	FTD-VPN-Posture-Compliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000// EmployeeVF	ASA/PIX7x-Tunnel-Gro PN	oup-	<pre></pre>	+ Select fro	m list 🔹	+	4	¢
				ŝ	Session-Posture	eStatus EQU	IALS NonCompliant			_				
	0	FTD-VPN-Posture-NonCompliant	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000// EmployeeVP	ASA/PIX7x-Tunnel-Gro PN	up-	× FTD-VPN-NonCompliant	Select fro	m list 🔹	+	0	¢
				ĥ	Session-Posture	Status EQU	IALS Unknown							
	\odot	FTD-VPN-Posture-Unknown	AND	ĥ	Cisco-VPN3000 Name EQUALS	CVPN3000// EmployeeVF	ASA/PIX7x-Tunnel-Gro PN	up-	×FTD-VPN-Redirect	+ Select fro	m list 🔹	+	9	¢

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Sur ISE, la première étape de vérification est RADIUS Live Log. Accédez à Operations > RADIUS Live Log. Ici, l'utilisateur Alice est connecté et la stratégie d'autorisation attendue est sélectionnée.

- RADULE Threat Contria NAC I	ive Least > TACA	CS Troubl	esheet b Ad	antive Network Control	Reports	110013									
Live Logs Live Sessions	me cogs i i i i i i i i i i i i i i i i i i i	1000		aparte metalon control	Nepula										
	Misconfigured Su	pplicants 0	M	isconfigured Network	Devices ()	RADIU S Dro	ps O	Cli	ent Stopped Res	ponding 0		Repeat	Counter ()		
	0			0		0			0				0		
									Refr	esh Never		Show Lates	t 20 records	Within Last 3	hours 🔻
C Refresh O Reset Repeat Co	ounts 📕 Export	To •							Refr	esh Never		Show Lates	at 20 records	Within Last 3	Filter • O
C Refresh O Reset Repeat Co Time	ounts 🛓 Export	To • Details	Repeat	identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Refr Authorizati	IP Address		Show Lates	t 20 records	Within Last 3	Filter • O Posture Sta
C Refresh O Reset Repeat Co Time X	ounts 🛓 Export Status	To • Details	Repeat	Identity Identity	Endpoint ID Endpoint ID	Endpoint Pr	Authenticat	Authorizati	Refr Authorizati	P Address		Show Lates	Device Port	Within Last 3	Filter • O Posture Stat.
C Refresh O Reset Repeat Co Time X Feb 03, 2020 07:13:31.92	Status	To • Details	Repeat	Identity Identity alice@training.e	Endpoint ID Endpoint ID 00.0C:29.5C:5A:96	Endpoint Pr Endpoint Prc Windows10	Authenticat Authenticatik Default >>	Authorizati Authorization Default >>	Refr Authorizati Authorizatior FTD-VPN-R	IP Address IP Address IP Address 172.16.1.10	×	Show Lates	Device Port	Within Last 3 Kidentity Group	Filter • • • • • • • • • • • • • • • • • • •
Refesh Reset Repeat Co Time Feb 03, 2020 07.13.31.92 Feb 03, 2020 07.13.29.74	Status	To • Details	Repeat	Identity Identity alice@training.e #ACSACL#IP-P	Endpoint ID Endpoint ID 00.0C:29.5C:5A.98	Endpoint Pr Endpoint Prc Windows10	Authenticat Authenticatik Default >>	Authorizati Authorization Default >>	Refr Authorizati Authorizatior FTD-VPN-R	IP Address IP Address IP Address 172.16.1.10		Show Lates	Device Port	Within Last 3	Filter • • • • • • • • • • • • • • • • • • •

La stratégie d'autorisation FTD-VPN-Posture-Unknown est mise en correspondance et, par conséquent, FTD-VPN-Profile est envoyé à FTD.

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

État de la position en attente.

NAS IPv4 Address	192.168.15.15
NAS Port Type	Virtual
Authorization Profile	FTD-VPN-Redirect
Posture Status	Pending
Response Time	365 milliseconds

La section Résultat indique quels attributs sont envoyés au FTD.

Result	
Class	CACS:000000000000005e37c81a:fyusifov-28-3/368560500/45
cisco-av-pair	url-redirect-acl=fyusifovredirect
cisco-av-pair	url-redirect=https://fyusifov-26-3.example.com:8443/portal /gateway?sessionId=0000000000000005e37c81a& portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp& token=0d90f1cdf40e83039a7ad6a226603112
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PostureUnknown-5e37414d
cisco-av-pair	profile-name=Windows10-Workstation
LicenseTypes	Base and Apex license consumed

Sur FTD, afin de vérifier la connexion VPN, établissez une connexion SSH au boîtier, exécutez la commande system support diagnostic-cli et ensuite show vpn-sessiondb detail anyconnect. À partir de ce résultat, vérifiez que les attributs envoyés depuis ISE sont appliqués pour cette session VPN.

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

Tunnel Zone : 0 Security Grp : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: : 12.1 Tunnel ID 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 Client OS : win Client OS Ver: 10.0.18363 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.7.01076 : 0 Bytes Tx : 7663 Bytes Rx 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 : SHA384 Hashing Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 56495 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 23 Minutes Client OS : Windows 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: : 12.3 Tunnel ID Assigned IP : 172.16.1.10 Public IP : 10.229.16.169 Encryption : AES256 Ciphersuite : DHE-RSA-AES256-SHA : SHA1 Hashing Encapsulation: DTLSv1.0 UDP Src Port : 59396 UDP Dst Port : 443 Auth Mode : userPassword 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 : 12770 : 0 Bytes Rx Pkts Tx : 42 Pkts Rx : 0 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=0000000000000005e37c81 Redirect ACL : fyusifovredirect Les stratégies de provisionnement client peuvent être vérifiées. Accédez à Operations > Reports > Endpoints and Users > Client Provisioning.

dentity Services Engine	Home + Context Visibili	ty Operations Policy	Administration			License Warr	ling 🔺 🔍	
+ RADIUS Threat-Centric NAC Liv	e Logs + TACACS + Tro	subleshoot + Adaptive Network Cont	trol Reports					
Export Summary	Client Provisioning From 2020-02-03 00:00:00 Reports exported in last 7	0.0 to 2020-02-03 08:14:07.0 days 0				+ My Reports	Export To •	© Schedule
• Reports								
► Audit	Logged At	Server	Event	Identity	Endpoint ID	IP Address	Clie	nt Provisioning Pol
Device Administration	Today 💌 🗙			Identity	Endpoint ID			
Diagnostics	2020-02-03 08:06:4	fyusifov-28-3	Client provisioning succeeded	alice@training.example.com	00:0C:29:5C:5A:98	172.16.1.10	AC	_47_Win
Endpoints and Users Authentication Summary Client Provisioning Current Active Sessions						Rows/Page 1	1 🚍	1 Total Rows

Le rapport de position envoyé depuis AnyConnect peut être vérifié. Accédez à Operations > Reports > Endpoints and Users > Posture Assessment by Endpoint.



Afin de voir plus de détails sur le rapport de posture, cliquez sur Détails.

dianti laentity Services Engine	
Posture More Detail Assessment	
From 2020-01-04 00:00:00 to 2020-02-03 08:13:36.0 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

Une fois le rapport reçu sur ISE, l'état de la position est mis à jour. Dans cet exemple, l'état de posture est conforme et la poussée CoA est déclenchée avec un nouvel ensemble d'attributs.

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		0			10.229.16.169				PermitAccess	7		FTD			Complia
Feb 03, 2020 08:07:50.03	0	<u>o</u>	0	alice@training.e	00:0C:29:5C:5A:96	Windows10	Default >>	Default >>	FTD-VPN-R	172.16.1.10					Complia
Feb 03, 2020 07:13:29.74		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

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					
СоАТуре	COA-push					
Network Device Profile	Cisco					
Location	Location#All Locations					
Device Type	Device Type#All Device Types					
IPSEC	IPSEC#Is IPSEC Device#No					
Device IP Address	192.168.15.15					

Vérifiez sur FTD que les nouvelles ACL de redirection et URL de redirection sont supprimées pour la session VPN et que la liste DACL PermitAll est appliquée.

<#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 MinutesIdle TO Left : 28 MinutesClient OS: WindowsClient Type: DTLS VPN ClientClient Ver: Cisco AnyConnect VPN Agent for Windows 4.7.01076Bytes Tx: 38612Pkts Tx: 62Pkts Tx Drop :0Filter Name:
```

#ACSACL#-IP-PermitAll-5e384dc0

fyusifov-ftd-64#

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour un flux de posture détaillé et pour dépanner AnyConnect et ISE, cliquez sur ce lien : <u>Comparaison des styles de posture ISE pour Pre et Post 2.2.</u>

• Tunnel Fractionné

L'un des problèmes courants, lorsqu'il y a un tunnel de broche est configuré. Dans cet exemple, la stratégie de groupe par défaut est utilisée, ce qui permet de tunnels tout le trafic. Dans le cas où seul un trafic spécifique est tunnellisé, les sondes AnyConnect (enroll.cisco.com et hôte de découverte) doivent traverser le tunnel en plus du trafic vers ISE et d'autres ressources internes.

Afin de vérifier la stratégie de tunnel sur FMC, vérifiez d'abord quelle stratégie de groupe est utilisée pour la connexion VPN. Accédez à Devices > VPN Remote Access.

Overview Analysis Policies Devices Object	AMP Intelligence		Deploy 🍳 System Help 🔻 admin 🔻
Device Management NAT VPN > Remote Acc	s QoS Platform Settings FlexConfig	Certificates	
EmployeeVPN			Save Save Cancel
			Policy Assignments (1)
Connection Profile Access Interfaces Advar	ed		
			0
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfitGrpPolicy	/ 6
EmployeeVPN	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: ISE (RADIUS)	DftGrpPolicy	a 6

Accédez ensuite à Objects > Object Management > VPN > Group Policy et cliquez sur Group Policy configured for VPN.



• NAT d'identité

Un autre problème courant, lorsque le trafic de retour des utilisateurs VPN est traduit avec l'utilisation d'une entrée NAT incorrecte. Afin de résoudre ce problème, la NAT d'identité doit être créée dans un ordre approprié.

Tout d'abord, vérifiez les règles NAT pour ce périphérique. Accédez à Devices > NAT, puis cliquez sur Add Rule pour créer une nouvelle règle.

Ove	Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🍕 System Help 🔻 admin 🔻											
Dev	rice Managemer	t NAT	VPN VQ0	6 Platform Set	tings FlexConfig	Certificates						
FT	FTD_11											
Ente	r Description											
	_										📑 Policy As	signments (1)
Rule	:5											
譜 Filt	er 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											

Dans la fenêtre ouverte, sous l'onglet Interface Objects, sélectionnez Security Zones. Dans cet exemple, l'entrée NAT est créée de ZONE-INSIDE à ZONE-OUTSIDE.

Add NAT Rule						? >	
NAT Rule:	Manual NAT Rule	▼	Insert:	In Category	▼ NAT Rules Before	•	
Туре:	Static V Enable						
Description:							
Interface Objects	Translation PA	T Pool Advand	ced				
Available Interface C)bjects 🖒		Source Interface Object	ts (1)	Destination Interface O	bjects (1)	
🔍 Search by name			LONE-INSIDE	6	ZONE-OUTSIDE	6	
ZONE-INSIDE							
ZONE-OUTSIDE		Add to					
		Source					
		Add to Destination					
					0	Cancel	

Sous l'onglet Translation, sélectionnez les détails des paquets d'origine et traduits. Comme il s'agit de la NAT d'identité, la source et la destination restent inchangées :

Edit NAT Rule							? ×
NAT Rule:	Manual NAT R	ule 💙	Inse	rt:	In Category	▼ NAT Rules Before ▼	
Туре:	Static	~	🗹 Enable				
Description:							
Interface Objects	Translation	PAT Pool	Advanced				
Original Packet					Translated Packet		
Original Source:*	any			~ 📀	Translated Source:	Address	~
Original Destination:	Address			~		any	v O
	VPN_Sub	net		~ 🔾	Translated Destination:	VPN_Subnet	~ O
Original Source Port:				• 0	Translated Source Port:		v O
Original Destination P	ort:		•	• •	Translated Destination Port:		~ 📀
						ок	Cancel

Sous l'onglet Advanced, cochez les cases comme indiqué dans cette image :

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.