Configuration du VPN de gestion AnyConnect SSL sur FTD

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Limites Configuration Configurations Étape 1. Créer un profil VPN de gestion AnyConnect Étape 2. Créer un profil VPN AnyConnect Étape 3. Télécharger le profil VPN de gestion AnyConnect et le profil VPN AnyConnect sur FMC Étape 4. Créer une stratégie de groupe Étape 5. Créer une nouvelle configuration AnyConnect Étape 6. Créer un objet URL Étape 7. Définir l'alias d'URL Vérification Dépannage

Introduction

Ce document décrit comment configurer un tunnel de gestion Cisco AnyConnect sur un pare-feu Cisco Firepower Threat Defense (FTD) géré par Cisco Firepower Management Center (FMC). Par exemple, sous Secure Sockets Layer (SSL) est utilisé pour créer un réseau privé virtuel (VPN) entre FTD et un client Windows 10.

Contribué par Daniel Perez Vertti Vazquez, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Éditeur de profil Cisco AnyConnect
- Configuration SSL AnyConnect via FMC.
- Authentification du certificat client

Components Used

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

- Cisco FTD version 6.7.0 (build 65)
- Cisco FMC version 6.7.0 (build 65)
- Cisco AnyConnect 4.9.01095 installé sur l'ordinateur Windows 10

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.

Informations générales

Depuis la version 6.7, Cisco FTD prend en charge la configuration des tunnels de gestion AnyConnect. Cela corrige la demande d'amélioration précédemment ouverte <u>CSCvs78215</u>.

La fonction de gestion AnyConnect permet de créer un tunnel VPN immédiatement après le démarrage du point d'extrémité. Il n'est pas nécessaire que les utilisateurs lancent manuellement l'application AnyConnect, dès que leur système est sous tension, le service d'agent VPN AnyConnect détecte la fonctionnalité VPN de gestion et lance une session AnyConnect à l'aide de l'entrée d'hôte définie dans la liste de serveurs du profil VPN de gestion AnyConnect.

Limites

- Seule l'authentification du certificat client est prise en charge.
- Seul le magasin de certificats d'ordinateur est pris en charge pour les clients Windows.
- Non pris en charge par Cisco Firepower Device Manager (FDM) CSCvx90058.
- Non pris en charge sur les clients Linux.

Configuration

Configurations

Étape 1. Créer un profil VPN de gestion AnyConnect

Ouvrez l'Éditeur de profil AnyConnect pour créer un profil VPN de gestion AnyConnect. Le profil de gestion contient tous les paramètres utilisés pour établir le tunnel VPN après le démarrage du point d'extrémité.

Dans cet exemple, une entrée de liste de serveurs pointant sur Nom de domaine complet (FQDN) dperezve.jyoung-labdomain.cisco.com est définie et SSL est sélectionné comme protocole principal. Pour ajouter une liste de serveurs, accédez à **Liste de serveurs** et sélectionnez le bouton **Ajouter**, remplissez les champs requis et enregistrez les modifications.

- an	AnyConnect	Profile	Editor -	VPN
------	------------	---------	----------	-----

Server	Load Balancing Servers	SCEP Mobile Cer	tificate Pinning	
Prin	nary Server			Connection Information
Dis	splay Name (required)	AnyConnect_Manag	ement_Tunnel	Primary Protocol SSL V
FQ	DN or IP Address	User Grou	ıp	ASA gateway
dţ	perezve.jyoungta-labdom	nain.cisc / AnyConn	ect_Management_Tunnel	Auth Method During IKE Negotiation EAP
Gr	oup URL			IKE Identity (IOS gateway only)
dp	perezve.jyoungta-labdom	ain.cisco.com/AnyCo	nnect_Management_Tunnel	
		Backup Servers Host Address		Add
				Move Up
				Move Down
				Delete
			OK Cancel	

Outre la liste des serveurs, le profil VPN de gestion doit contenir certaines préférences obligatoires :

- AutomaticCertSelection doit être défini sur true.
- La reconnexion automatique doit être définie sur true.
- AutoReconnectBehavior doit être configuré pour ReconnectAfterResume.
- AutoUpdate doit avoir la valeur false.
- BlockUntrustServers doit être défini sur true.
- CertificateStore doit être configuré pour MachineStore.
- CertificateStoreOverride doit être défini sur true.
- EnableAutomaticServerSelection doit avoir la valeur false.
- EnableScripting doit avoir la valeur false.
- RetainVPNOnLogoff doit être défini sur true.

Dans AnyConnect Profile Editor, accédez à **Préférences (Partie 1)** et réglez les paramètres comme suit :

 \times

File Help

VPN ····································	Preferences (Part 1) Profile:nnect -FTD-Lab\.XML Prof	Preferences (Part 1) Profile:nnect -FTD-Lab\.XML Profile\AnyConnect_Management_Tunnel.xml								
Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List	□ Use Start Before Logon □ Show Pre-Connect Message Certificate Store Windows Machine ~ macOS All ~ Certificate Store Override	User Controllable	^							
	Auto Connect On Start	User Controllable								
	Local Lan Access	User Controllable								
	Disable Captive Portal Detection	User Controllable								
	🔽 Auto Reconnect	User Controllable								
	Auto Reconnect Behavior ReconnectAfterResume	User Controllable								
	🖂 Auto Update	User Controllable								
	RSA Secure ID Integration	User Controllable								
	Windows Logon Enforcement									
	SingleLocalLogon 🗸									
	Windows VPN Establishment									
	AllowRemoteUsers		~							
	6	Help								

Ensuite, accédez à **Préférences (Partie 2)** et décochez l'option **Désactiver la sélection** automatique de certificats.

 \Box \times

_

File Help

VPN Preferences (Part 1) Preferences (Part 2)	Preferences (Part Profile:nnect -F	2) ID-Lab\.XML Profile\AnyCon	nect_Management_Tunnel.	xml				
Backup Servers	Disable Automatic	: Certificate Selection	User Controllable		^			
Certificate Matching	Proxy Settings	Native	✓ User Controllable					
Berver List		Public Proxy Server Address:						
	Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080 Allow Local Proxy Connections							
	Enable Optimal G	ateway Selection	User Controllable					
	Suspension Time	e Threshold (hours)	4					
	Performance Im	provement Threshold (%)	20					
	Trusted Network	: Policy	Disconnect	\sim				
	Untrusted Netwo	rk Policy	Connect	\sim				
	Trusted DNS Do	mains						
	Trusted DNS Sei Note: add	vers ling all DNS servers in use is recom	mended with Trusted Network D	etection				
	Trusted Servers	@ https:// <server>[:<port>]</port></server>						
	https://		Add					
			Delete					
					~			
		👔 Help						

Étape 2. Créer un profil VPN AnyConnect

Outre le profil VPN de gestion, le profil VPN AnyConnect standard doit être configuré. Le profil VPN AnyConnect est utilisé lors de la première tentative de connexion. Au cours de cette session, le profil VPN de gestion est téléchargé à partir de FTD.

Utilisez l'éditeur de profil AnyConnect pour créer le profil VPN AnyConnect. Dans ce cas, les deux fichiers contiennent les mêmes paramètres afin que la même procédure puisse être suivie.

Étape 3. Télécharger le profil VPN de gestion AnyConnect et le profil VPN AnyConnect sur FMC

Une fois les profils créés, l'étape suivante consiste à les télécharger sur le FMC en tant qu'objets de fichier AnyConnect.

Afin de télécharger le nouveau profil VPN de gestion AnyConnect sur FMC, accédez à **Objets** > **Gestion des objets** et choisissez l'option **VPN** dans la table des matières, puis sélectionnez le bouton **Ajouter un fichier AnyConnect**.

Indiquez un nom pour le fichier, choisissez **AnyConnect Management VPN Profile** comme type de fichier et enregistrez l'objet.

 \sim



Maintenant, afin de télécharger le profil VPN AnyConnect naviguez à nouveau vers **Objets > Gestion des objets** et choisissez l'option **VPN** dans la table des matières, puis sélectionnez le bouton **Ajouter un fichier AnyConnect**.

Indiquez un nom pour le fichier, mais cette fois, choisissez **AnyConnect VPN Profile** comme type de fichier et enregistrez le nouvel objet.

Overview Analysis Policie	es Devices Objects	AMP Intelliger					. Deploy System Help ▼ d	perezve 🔻
Object Management Intrus	sion Rules							
AnyConnect File File objects represent files used in co	infigurations, typically for remot	e access VPN policies.	They can contain AnyConnect Client Profile and A	nyConnect Clie	nt Image	files.	Add AnyConnect File	
Security Group (ag	Name			Value			Туре	
DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? ×	.9.01095-webd	AnyConnect Client Image	2 / 5
Vetwork Lists and Feeds	AnyConnect_Management_Tu					gement_Tunne	AnyConnect Management VPN Profile	200
Sinkhole	SSL_AnyConnect.xml	Name:*	SSL_AnyConnect.xml			cml	AnyConnect VPN Profile	205
Generation SLA Monitor		File Name:*	SSL_AnyConnect.xml	Browse				
Time Zone		File Type:*	AnyConnect VPN Profile	~				
URL		Description:	AnyConnect Client Image AnyConnect VPN Profile	î				
S VARIABLE Set			AnyConnect Management VPN Profile AMP Enabler Service Profile					
VPN AnyConnect File			Feedback Profile					
R Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile	- 1				
IKEv1 IPsec Proposal			Umbrella Roaming Security Profile	- 1				
IKEv1 Policy			Web Security Service Profile	~				
IKEv2 IPsec Proposal	<					Displaying	1 - 3 of 3 rows K < Page 1 of 3	>> C
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115	5.cisco.com	How To					

Les profils doivent être ajoutés à la liste des objets et marqués comme **Profil VPN de gestion AnyConnect** et **Profil VPN AnyConnect** respectivement.

Overview Analysis Policie	es Devices Objects	AMP Intelligence			. Peploy System Help ▼	dperezve 🔻
Object Management Intrus	sion Rules					
AnyConnect File File objects represent files used in co	onfigurations, typically for remote	access VPN policies. They can contain	AnyConnect Client Profile and AnyCo	onnect Client Image files.	Add AnyConnect File	
Security Group lag	Name			Value	Туре	
 Security Intelligence DNS Lists and Feeds 	Anyconnect4.9_For_Windows			anyconnect-win-4.9.01095-wel	od AnyConnect Client Image	2 🥒 🖯
Network Lists and Feeds	AnyConnect_Management_Tun	nel		AnyConnect_Management_Tun	ne AnyConnect Management VPN Profil	200
Sinkhole	SSL_AnyConnect.xml			SSL_AnyConnect.xml	AnyConnect VPN Profile	2 🥒 🖯
SLA Monitor						
Time Zone						
Contraction and the second sec						
\$ Variable Set						
📎 VLAN Tag						
A DVPN						
ManyConnect File						
R. Certificate Map						
Group Policy						
REVI IPSec Proposal						
IVENT POlicy	,					
REV2 IPSet Proposal				Displayir	ng 1 - 3 of 3 rows K < Page 1	of 1 > > C
La nate toney				0 opid jii	a contract to the toge	
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.c	isco.com	How To			uluilu cisco

Étape 4. Créer une stratégie de groupe

Afin de créer une nouvelle stratégie de groupe, accédez à **Objets > Gestion des objets** et choisissez l'option **VPN** dans la table des matières, puis sélectionnez **Stratégie de groupe** et cliquez sur le bouton **Ajouter une stratégie de groupe**.

Une fois la fenêtre **Ajouter une stratégie de groupe** ouverte, attribuez un nom, définissez un pool AnyConnect et ouvrez l'onglet **AnyConnect**. Accédez à **Profil** et sélectionnez l'objet qui représente le profil VPN AnyConnect régulier dans le menu déroulant **Profil client**.



Ensuite, accédez à l'onglet **Profil de gestion** et sélectionnez l'objet qui contient le profil VPN de gestion dans le menu déroulant **Profil de gestion**.



Enregistrez les modifications pour ajouter le nouvel objet aux stratégies de groupe existantes.

Overview Analysis Policie	s Devices Objects AMP Intelligence	\rm 🕘 Deploy System	Help 🔻 dperezve 🔻
Object Management Intru:	sion Rules		
			Ciller
Group Policy		Add Group Policy	Sec. 19
A Group Policy is a set of attribute an profile.	id value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the g	roup policy or it is obtained	from the current connection
Security Group lag	Name		
Security Intelligence	Nume		
DNS Lists and Feeds	AnyConnect_Management_Tunnel		6
Network Lists and Feeds	DfltGrpPolicy		1 A
URL Lists and Feeds	encerps ency		
Sinkhole			
SLA Monitor			
📆 Time Range			
💮 Time Zone			
Tunnel Zone			
() URL			
\$ Variable Set			
S VLAN Tag			
A 🛃 VPN			
MayConnect File			
R. Certificate Map			
Group Policy			
IKEv1 IPsec Proposal			
IKEv1 Policy			
IKEv2 IPsec Proposal			
KEv2 Policy	Displayi	ng 1 - 2 of 2 rows 🛛 🔍 🔍	Page 1 of 1 > > C
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.cisco.com How To		cisco

Étape 5. Créer une nouvelle configuration AnyConnect

La configuration de SSL AnyConnect dans FMC est composée de 4 étapes différentes. Pour configurer AnyConnect, accédez à **Devices > VPN > Remote Access** et sélectionnez le bouton **Add**. Ceci doit ouvrir l'**Assistant Stratégie VPN d'accès à distance**.

Dans l'onglet **Affectation de stratégie**, sélectionnez le périphérique FTD en main, définissez un nom pour le profil de connexion et cochez la case SSL.

Overview Analysis Policies Devic Dashboards • Reporting Summary •	es Objects AMP Intelli	igence			₽ ₁ Deploy Syste	n Help v	dperezve 🔻
Remote Access VPN Policy Wiz	zard						
1 Policy Assignment 2 Conn	ection Profile $>$ 3 AnyCo	onnect 🔪 4	Access & Certificate > (5 Summary			
Targeted Devic This wizard will gui a new user-defined Name:* Description: VPN Protocols: Targeted Devices:	es and Protocols de you through the required minima connection profile. AnyConnect_Management_Tunnel SSL IPsec-IKEv2 Available Devices Search Rivedperezve ftdv-fejimene	Add	he Remote Access VPN policy with Selected Devices	Before You S Before you start, configuration eleme complete Remote A Authentication Se Configuration authentic AnyConnect Cliene Make sure you hav for VPN client do the relevant Clicco it during the wizard Device Interfaces should b targeted <u>devices</u> so as a security zone enable VPN access.	ensure the following ensure the following entis to be in place to cccess VPN Policy. rver RADIUS Server Group ate VPN clients. t Package e AnyConnect package wiloaded or you have redentials to download e already configured on that they can be used or interface group to		
					Back	ext	Cancel
Last login on Thursday, 2021-03-25 at 17:01:05 PM	from rtp-vpn6-107.cisco.com		How To				ahaha

Dans **Profil de connexion** sélectionnez **Certificat client uniquement** comme méthode d'authentification. Il s'agit de la seule authentification prise en charge pour la fonctionnalité.

Overview Analysis Policies Devices Objects AMP Intelli	igence	(Deploy	System Helj	🔻 dperezve 🔻
Device Management NAT VPN > Remote Access QoS Platfo	orm Settings FlexConfig	Certificates			
Remote Access VPN Policy Wizard					
1 Policy Assignment 2 Connection Profile 3 AnyC	connect > 🖪 Access &	Certificate S Summary			
Connection Profile:					^
Connection Profiles specify the tunnel gro accomplished and how addresses are ass	oup policies for a VPN connection. signed. They also include user attr	These policies pertain to creating the tunnel itself, how AAA is ibutes, which are defined in group policies.			
Connection Profile Name:* Ar	nyConnect_Management_Profile				
Thi	is name is configured as a connectio	n alias, it can be used to connect to the VPN gateway			
Authentication, Authorization & Acco	ounting (AAA):				
Specify the method of authentication (AM	NA, certificates or both), and the A	AA servers that will be used for VPN connections.			
Authentication Method: CI	lient Certificate Only	*			
Username From Certificate: SA	AA Only AML	^ istinguished Name) as username			
Primary Field: Cl	lient Certificate Only				
Secondary Field: Cl	lent Certificate & AAA	v			
Authorization Server:		▼ ③• (Realm or RADIUS)			
Accounting Server:		▼ (RADIUS)			
Client Address Assignment: Client IP address can be assigned from A assignment is tried in the order of AAA s	AAA server, DHCP server and IP ad erver, DHCP server and IP address	dress pools. When multiple options are selected, IP address s pool.			
Use AAA Server (Realm or RAD	DIUS only) 🕕				
			Back	Next	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How T				

Sélectionnez ensuite l'objet Stratégie de groupe créé à l'étape 3 dans la liste déroulante **Stratégie de groupe**.

Overview Analysis Policies Devices Objects AMP Intell	igence	. Deploy	System	Help 🔻	dperezve	•
Device Management NAT VPN > Remote Access QoS Platfe	orm Settings FlexConfig Certificates					
Remote Access VPN Policy Wizard						
1 Policy Assignment 2 Connection Profile 3 AnyC	connect $>$ 4 Access & Certificate $>$ 5 Summary					
Authorization Server:	(Realm or RADIUS)					^
Accounting Server:	V (RADIUS)					
Client Address Assignment: Client IP address can be assigned from A assignment is tried in the order of AAA s	WAA server, DHCP server and IP address pools. When multiple options are selected, IP addre erver, DHCP server and IP address pool.	is				
Use AAA Server (Realm or RAD Use DHCP Servers Use IP Address Pools	DIUS only) 🕕					
IPv4 Address Pools: A	nyConnect-Pool 🥜					
IPv6 Address Pools:	Ø					
Group Policy:						
A group policy is a collection of user-orie or create a Group Policy object.	ented session attributes which are assigned to client when a VPN connection is established.	elect				
Group Policy:*	nyConnect_Management_Tunnel 🔽 📀					
	AnyConnect_Management_Tunnel					
E	DfltGrpPolicy v					
						~
		Back	Nex	t	Cancel	
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To				սիսի	

Sous l'onglet **AnyConnect**, sélectionnez l'**objet de fichier AnyConnect** en fonction du système d'exploitation (OS) du point de terminaison.

Overview Analysis Policies	Devices Objects	AMP Inte	elligence	Shu Guadha	C			0 ₁	Deploy	System	Help 🔻	dperezve 🔻
Remote Access VPN Poli	icy Wizard	Q05 Pla	trorm Settings	FlexConfig	Certificates							
1 Policy Assignment 2	2) Connection Profile	3 Any	Connect	4 Access 8	Certificate	5 Summary	/					
	AnyConnect Client I The VPN gateway can au initiated. Minimize connect	mage tomatically down tion setup time b	load the latest Ar	nyConnect packag propriate OS for t	je to the client of the selected pack	AAA device when the VPN c age.	connection is					^
	Download AnyConnect Cla	ent packages noi	in cisco sortware i	Download Center.	5	Show Re-order buttons	0					
	AnyConnect File C	Windows	AnyConnect O	lient Package N	lame leplov-k9.pkg	Operating System						
						TINUOWS						
								l	Back	Next	t	Cancel
Last login on Saturday, 2021-03-27 at 19	9:12:55 PM from rtp-vpn1-11	15.cisco.com		How	Го							uluilu cisco

Sur Access & Certificate spécifiez le certificat qui doit être utilisé par le FTD pour tester son identité sur le client Windows.

Note: Puisque les utilisateurs ne doivent pas interagir avec l'application AnyConnect lors de l'utilisation de la fonctionnalité VPN de gestion, le certificat doit être entièrement fiable et ne doit pas imprimer de message d'avertissement.

Note: Afin d'empêcher les erreurs de validation de certificat, le champ Nom commun (CN) inclus dans le nom d'objet du certificat doit correspondre au nom de domaine complet défini dans la liste des profils XML du serveur (Étape 1 et Étape 2).

Overview Analysis Policies Devices Objects AMP Intelligence	$oldsymbol{ extsf{0}}_1$ Deploy	System Help 🔻	dperezve 🔻
Device Management NAT VPN > Remote Access QoS Platform Settings FlexConfig Certificates			
Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary			
Interface group/Security Zone:* Outside V Q V			· · · · · · · · · · · · · · · · · · ·
Device Certificates Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select certificate which is used to authenticate the VPN gateway.	a		
Certificate Enrollment:* SSL_AnyConnect Certificate object on the target devices			
Access Control for VPN Traffic All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.			
Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded fron AAA server are still applied to VPN traffic.	0		
	Back	Next	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To			uluilu cisco

Enfin, sélectionnez **Terminer** dans l'onglet **Résumé** pour ajouter la nouvelle configuration AnyConnect.



Étape 6. Créer un objet URL

Accédez à **Objets > Gestion des objets** et sélectionnez **URL** dans la table des matières. Sélectionnez ensuite **Ajouter un objet** dans la liste déroulante **Ajouter une URL**.

Fournissez un nom pour l'objet et définissez l'URL à l'aide du même nom de domaine complet/groupe d'utilisateurs spécifié dans la liste Management VPN Profile Server (Étape 2). Dans cet exemple, l'URL doit être dperezve.jyoungtalabdomain.cisco.com/AnyConnect_Management_Tunnel.

Overview Analysis Policies	Devices Objects	AMP Intelligence					em Help v	dperezve 🔻
Object Management Intrusion	on Rules							
URL URL object represents a single URL or	IP address. You can use URL obi	ects and groups in vario	us places, including access control p	olicies and event searches. I	For example, vo	Add URL •	Filter	ised Objects
Security Group Tag	Name			v	alue		Override	
A Security Intelligence								
DNS Lists and Feeds			No reco	rds to display				
Network Lists and Feeds		New URL Object	5	? >	c			
URL Lists and Feeds								
C Sinkhole		Name	lanagement_Tunnel					
SLA Monitor		Description						
🚮 Time Range								
🗑 Time Zone								
and Tunnel Zone		URL	ttps://dperezve.jyoungta-labdoma					
URL		Allow Overrides						
\$ Variable Set				Canaal				
S VLAN Tag				Save				
A VPN								
AnyConnect File								
R, Certificate Map								
Group Policy								
REVI IPSec Proposal								
IVEN2 IDeas Proposal								
REV2 Insec Proposal						No data to display	< Page 1 o	f1 > > C
			How To					cisco

Enregistrez les modifications pour ajouter l'objet à la liste des objets.

Étape 7. Définir l'alias d'URL

Afin d'activer l'alias d'URL dans la configuration AnyConnect, accédez à **Devices > VPN > Remote Access** et cliquez sur l'icône représentant un crayon pour la modifier.

Ensuite, dans l'onglet Profil de connexion, sélectionnez la configuration à portée de main, accédez à **Alias**, cliquez sur le bouton **Ajouter** et sélectionnez l'**objet URL** dans la **liste déroulante Alias URL** . Assurez-vous que la case **Enabled** est cochée.

Overview Analysis Policies Device	Edit Connection Profile ? >	🗛 Deploy System Help 🔻 dperezve 🔻
Device Management NAT VPN ► Rem AnyConnect_Management_	Connection Profile:* AnyConnect_Management_Tunnel Group Policy:* AnyConnect_Management_Tunnel Context_Management_Tunnel Co	Save Save
Connection Profile Access Interfaces	Client Address Assignment AAA Aliases	Policy Assignments (1)
Name DefaultWEBVPNGroup	Alias Names: Add URL Alias ? Incoming users can ch can be turned on or of Name OK Cancel	0 2 3
AnyConnect_Management_Tunnel		nnel 🥜 🖥
	URL Alias: Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.	
	URL Status	
	Save	
Last login on Monday, 2021-04-05 at 23:55:27 PM from	rtp-vpn4-759.cisco.com How To	cisco

Enregistrez les modifications et déployez les configurations sur FTD.

Vérification

Une fois le déploiement terminé, une première connexion AnyConnect manuelle avec le profil VPN AnyConnect est nécessaire. Pendant cette connexion, le profil VPN de gestion est téléchargé à partir de FTD et stocké dans C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun. À partir de ce point, les connexions suivantes doivent être initiées via le profil VPN de gestion sans aucune interaction utilisateur.

Dépannage

Pour les erreurs de validation de certificat :

- Assurez-vous que le certificat racine de l'autorité de certification (CA) est installé sur le FTD.
- Assurez-vous qu'un certificat d'identité signé par la même autorité de certification est installé sur le Windows Machine Store.
- Assurez-vous que le champ CN est inclus dans le certificat et qu'il est identique au nom de domaine complet défini dans la liste des serveurs du profil VPN de gestion et du nom de domaine complet défini dans l'alias d'URL.

Pour le tunnel de gestion non initialisé :

- Vérifiez que le profil VPN de gestion a été téléchargé et stocké dans
 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun.
- Vérifiez que le nom du profil VPN de gestion est VpnMgmtTunProfile.xml.

Pour les problèmes de connectivité, collectez l'offre DART et contactez le TAC Cisco pour plus d'informations.