Configuración de SSL AnyConnect Management VPN en FTD

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Limitaciones Configurar Configuraciones Paso 1. Crear el perfil VPN de administración de AnyConnect Paso 2. Crear perfil VPN de AnyConnect Paso 3. Cargue el perfil VPN de administración de AnyConnect y el perfil VPN de AnyConnect en FMC Paso 4. Crear política de grupo Paso 5. Crear nueva configuración de AnyConnect Paso 6. Crear objeto URL Paso 7. Definir alias de URL Verificación Troubleshoot

Introducción

Este documento describe cómo configurar un túnel de Cisco AnyConnect Management en Cisco Firepower Threat Defense (FTD) que se administra mediante Cisco Firepower Management Center (FMC). En el ejemplo siguiente, Secure Sockets Layer (SSL) se utiliza para crear una red privada virtual (VPN) entre FTD y un cliente Windows 10.

Colaborado por Daniel Perez Vertti Vazquez, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Editor de perfiles de Cisco AnyConnect
- Configuración de SSL AnyConnect a través de FMC.
- Autenticación de certificado de cliente

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTD versión 6.7.0 (versión 65)
- Cisco FMC versión 6.7.0 (versión 65)
- Cisco AnyConnect 4.9.01095 instalado en el equipo 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Desde la versión 6.7, Cisco FTD admite la configuración de los túneles de AnyConnect Management. Esto corrige la solicitud de mejora previamente abierta <u>CSCvs78215</u>.

La función AnyConnect Management permite crear un túnel VPN inmediatamente después de que el terminal finalice su inicio. No es necesario que los usuarios inicien manualmente la aplicación AnyConnect, tan pronto como se enciende el sistema, el servicio de agente AnyConnect VPN detecta la función Management VPN e inicia una sesión AnyConnect mediante la entrada Host definida en la lista de servidores del perfil VPN de administración de AnyConnect.

Limitaciones

- Solo se admite la autenticación de certificado de cliente.
- Sólo los clientes de Windows admiten el almacén de certificados de equipo.
- No se admite en Cisco Firepower Device Manager (FDM) <u>CSCvx90058</u>.
- No soportado en clientes Linux.

Configurar

Configuraciones

Paso 1. Crear el perfil VPN de administración de AnyConnect

Abra el Editor de perfiles de AnyConnect para crear el perfil VPN de administración de AnyConnect. El perfil de administración contiene todos los ajustes utilizados para establecer el túnel VPN después de que se inicie el terminal.

En este ejemplo, se define una entrada de lista de servidores que apunta a Nombre de dominio completo (FQDN) dperezve.jyoungta-labdomain.cisco.com y se selecciona SSL como el protocolo principal. Para agregar una lista de servidores, navegue hasta **Lista de servidores** y seleccione el botón **Agregar**, rellene los campos obligatorios y guarde los cambios.

- 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	jement_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	

Además de la lista de servidores, el perfil de VPN de administración debe contener algunas preferencias obligatorias:

- AutomaticCertSelection debe establecerse en true.
- AutoReconnect debe configurarse en true.
- AutoReconnectBehavior se debe configurar para ReconnectAfterResume.
- AutoUpdate se debe establecer en false.
- BlockUnTrustedServers se debe establecer en true.
- CertificateStore debe configurarse para MachineStore.
- CertificateStoreOverride debe establecerse en true.
- EnableAutomaticServerSelection debe establecerse en false.
- EnableScripting se debe establecer en false.
- RetainVPNOnLogoff debe configurarse en true.

En el Editor de perfiles de AnyConnect, vaya a **Preferencias (Parte 1)** y ajuste la configuración de la siguiente manera:

 \times

File Help

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

A continuación, navegue hasta **Preferencias (Parte 2)** y desmarque la **opción Desactivar selección automática de certificados**.

 \Box \times

_

File Help

Backup Servers	Disable Automatic Ce	ertificate Selection	User Controllable	^
Certificate Matching	Proxy Settings	Native	V User Controllable	
	Pu	ublic Proxv Server Address:		
	Allow Local Proxy Co	ote: Enter public Proxv Server a onnections	ddress and Port here. Example:10.86.125.33:80	80
	Enable Optimal Gate	way Selection	User Controllable	
	Suspension Time T	hreshold (hours)	4	
	Performance Impro	vement Threshold (%)	20	
	Automatic VPN Policy Trusted Network Po	y blicy	Disconnect \vee	
	Untrusted Network	Policy	Connect ~	
	Trusted DNS Domai	ins		
	Trusted DNS Serve Note: adding	rs g all DNS servers in use is recon	nmended with Trusted Network Detection	
	Trusted Servers @	https:// <server>[:<port>]</port></server>		
	nttps://		Add	
			Delete	

 \sim

Paso 2. Crear perfil VPN de AnyConnect

Además del perfil de VPN de administración, se debe configurar el perfil VPN normal de AnyConnect. El perfil VPN de AnyConnect se utiliza en el primer intento de conexión; durante esta sesión, el perfil VPN de administración se descarga desde FTD.

Utilice el Editor de perfiles de AnyConnect para crear el perfil VPN de AnyConnect. En este caso, ambos archivos contienen la misma configuración, por lo que se puede seguir el mismo procedimiento.

Paso 3. Cargue el perfil VPN de administración de AnyConnect y el perfil VPN de AnyConnect en FMC

Una vez creados los perfiles, el siguiente paso es cargarlos en el FMC como objetos de archivo AnyConnect.

Para cargar el nuevo perfil VPN de administración de AnyConnect en FMC navegue a **Objetos** > **Administración de objetos** y elija la opción **VPN** de la tabla de contenido, luego seleccione el **botón Add AnyConnect File**.

Proporcione un nombre para el archivo, elija **AnyConnect Management VPN Profile** como tipo de archivo y guarde el objeto.



Ahora, para cargar el perfil de VPN de AnyConnect navegue de nuevo a **Objetos > Administración de objetos** y elija la opción **VPN** de la tabla de contenido, luego seleccione el botón **Agregar archivo de AnyConnect**.

Proporcione un nombre para el archivo, pero esta vez elija **AnyConnect VPN Profile** como tipo de archivo y guarde el nuevo objeto.

Overview Analysis Policie	es Devices Objects	AMP Intelligen	ce				. Peploy System Help ▼ d	perezve 🔻
Object Management Intrus	sion Rules							
AnyConnect File File objects represent files used in co	infigurations, typically for remo	te access VPN policies.	They can contain AnyConnect Client Profile and Ar	nyConnect Clie	nt Image	e files.	Add AnyConnect File	
Security Group lag	Name			Value			Туре	
DNS Lists and Feeds	Anyconnect4.9_For_Windows	Edit AnyConnec	t File		? ×	9.01095-webc	AnyConnect Client Image	2 🥒 🖯
Vetwork Lists and Feeds	AnyConnect_Management_Tu					gement_Tunn	AnyConnect Management VPN Profile	2 🖉 🖯
Sinkhole	SSL_AnyConnect.xml	Name:*	SSL_AnyConnect.xml			cml	AnyConnect VPN Profile	200
G Time Range		File Name:*	SSL_AnyConnect.xml	Browse				
Time Zone		File Type:*	AnyConnect VPN Profile	~				
URL		Description:	AnyConnect Client Image AnyConnect VPN Profile	^				
\$ Variable Set			AnyConnect Management VPN Profile					
VLAN Tag			AMP Enabler Service Profile Feedback Profile					
ManyConnect File			ISE Posture Profile					
R ⁱ Certificate Map			NAM Service Profile					
Group Policy			Network Visibility Service Profile					
IKEv1 IPsec Proposal			Umbrella Roaming Security Profile					
IKEV1 Policy			Web Security Service Prome	÷				
IKEv2 Policy v						Displaying	1 - 3 of 3 rows 🛛 🔍 🖉 Page 1 of 3	l>>IC
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-111	5.cisco.com	How To					uluilu cisco

Los perfiles se deben agregar a la lista de objetos y marcar como **AnyConnect Management VPN Profile** y **AnyConnect VPN Profile** respectivamente.

Overview Analysis Policie	es Devices Objects AMP Intelligence			perezve 🔻
Object Management Intru	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 AnyConnect 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	-webd AnyConnect Client Image	2 🥒 🖯
Network Lists and Feeds URL Lists and Feeds	AnyConnect_Management_Tunnel	AnyConnect_Management_	Tunne AnyConnect Management VPN Profile	2 🥒 🖯
Sinkhole SLA Monitor SLA Monitor Time Range Time Zone Time Zone Time Zone URL VRL VRL VLN Tag VNN	SSL_AnyConnect.xml	SSL_AnyConnect.xml	AnyConnect VPN Profile	ž 🥜 词
AnyConnect File Arrow Certificate Map Certificate Map	٢	Disp	ələying 1 - 3 of 3 rows 🌾 🗧 Page 1 of 3	, , > > , ¢
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.cisco.com	How To		cisco

Paso 4. Crear política de grupo

Para crear una nueva política de grupo, navegue hasta **Objetos > Administración de objetos** y elija la opción **VPN** de la tabla de contenido, luego seleccione **Política de grupo** y haga clic en el **botón Agregar política de grupo** .

Una vez que se abra la ventana **Agregar política de grupo**, asigne un nombre, defina un grupo de AnyConnect y abra la pestaña **AnyConnect**. Navegue hasta **Profile** y seleccione el objeto que representa el perfil VPN normal de AnyConnect en el menú desplegable **Client Profile**.



A continuación, navegue hasta la ficha **Perfil de administración** y seleccione el objeto que contiene el perfil de VPN de administración en el menú desplegable **Perfil de administración**.



Guarde los cambios para agregar el nuevo objeto a las directivas de grupo existentes.

Overview Analysis Policie	es Devices Objects AMP Intelligence	loy System Help	▼ dperezve ▼
Object Management Intru	sion Rules		
Group Policy	S Add Gr	oup Policy Filte	3F
A Group Policy is a set of attribute an profile.	nd value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or	it is obtained from the	current connection
Security Group lag	Name		
Security Intelligence	None.		
DNS Lists and Feeds	AnyConnect_Management_Tunnel		6 🖬
Network Lists and Feeds	DftGroPolicy		08
URL Lists and Feeds			
Sinkhole			
SLA Monitor			
Time Range			
💮 Time Zone			
Tunnel Zone			
URL			
\$ Variable Set			
S VLAN Tag			
4 🛃 VPN			
MnyConnect File			
R. Certificate Map			
Group Policy			
IKEv1 IPsec Proposal			
IKEv1 Policy			
IKEv2 IPsec Proposal			
1KEv2 Policy	Displaying 1 - 2 of 2	rows 📧 🔍 Page 1	of 1 > > C
			بار بار
Last login on Saturday, 2021-03-27 at	19:12:55 PM from rtp-vpn1-1115.cisco.com How To		cisco

Paso 5. Crear nueva configuración de AnyConnect

La configuración de SSL AnyConnect en FMC consta de 4 pasos diferentes. Para configurar AnyConnect, navegue hasta **Devices > VPN > Remote Access** y seleccione el **botón Add**. Esto debe abrir el **Asistente de Políticas de VPN de Acceso Remoto**.

En la pestaña **Asignación de políticas** seleccione el dispositivo FTD que se encuentra en la mano, defina un nombre para el perfil de conexión y marque la casilla de verificación SSL.

Overview Analysis Policies Devic	es Objects AMP Intellig	jence			$oldsymbol{\theta}_{1}$ Deploy Syst	em Help 🔻	dperezve 🔻
Remote Access VPN Policy Wiz	ard						
1 Policy Assignment 2 Conne	ection Profile 🔰 3 AnyCo	nnect 🔰 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 minimal : connection profile. AnyConnect_Management_Tunnel SSL IPSec-IKEv2 Available Devices Search Michael Content fidv-fejimene	steps to configure th	e Remote Access VPN policy with Selected Devices	Before Y Before you s configuration complete Rem Authenticati Configure Res or SSO to auti AnyConnect Make sure yo for VPN Cleft the relevant C it during the w Device Inter Interfaces sho targeted devia as a security enable VPN ac	You Start start, ensure the following elements to be in place to ote Access VPN Policy. on Server im or RADIUS Server Group henticate VPN clients. Client Package u have AnyConnect package ti downloaded or you have isco credentials to download vizard. face uld be already configured on cess of that they can be used zone or interface group to cess.		
Last loon on Thursday, 2021-03-25 at 12-01-05 DM	from the units 107 circo com		How To		Back	Next	Cancel

En **Perfil de conexión** seleccione **Certificado de cliente solamente** como método de autenticación. Esta es la única autenticación admitida para la función.

Overview Analysis Policies Devices Objects AMP Intelligence	. ● Deploy System Help ▼ dperezve ▼
Device Management NAT VPN > Remote Access QoS Platform Settings	«Config Certificates
Remote Access VPN Policy Wizard	
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4	ccess & Certificate S Summary
Connection Profile: Connection Profiles specify the tunnel group policies for a VF	connection. These policies pertain to creating the tunnel itself, how AAA is
accomplished and how addresses are assigned. They also in	ie user attributes, which are defined in group policies.
Connection Profile Name:* AnyConnect_Manager	it_Profile
This name is configured	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 bo	, and the AAA servers that will be used for VPN connections.
Authentication Method: Client Certificate Only	×
Username From Certificate: AAA Only SAML	Istinguished Name) as username
Primary Field: Client Certificate Only	
Secondary Fleld: Client Certificate & AA	v
Authorization Server:	V Q • (Realm or RADIUS)
Accounting Server:	V (RADIUS)
Client Address Assignment:	
Client IP address can be assigned from AAA server, DHCP se assignment is tried in the order of AAA server, DHCP server	r and IP address pools. When multiple options are selected, IP address I IP address pool.
Use AAA Server (Realm or RADIUS only) 0 Use DHCP Servers	
	Back Next Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com	How To

A continuación, seleccione el objeto Group Policy creado en el paso 3 en el menú desplegable **Group Policy**.

Overview Analysis Policies Devices Objects AMP Intelli	gence	0 ₁ Deploy	System	Help 🔻	dperezve 🔻	
Device Management NAT VPN > Remote Access QoS Platfo	rm Settings FlexConfig Certificates					
Remote Access VPN Policy Wizard						
1 Policy Assignment 2 Connection Profile 3 AnyCo	onnect > 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 se	AA server, DHCP server and IP address pools. When multiple options are selected, IP address rver, DHCP server and IP address pool.					
Use AAA Server (Realm or RAD Use DHCP Servers Use IP Address Pools	IUS only) 🕕					
IPv4 Address Pools: An	yConnect-Pool 🥜					l
IPv6 Address Pools:	Ø					
Group Policy:						
A group policy is a collection of user-orier or create a Group Policy object.	ated session attributes which are assigned to client when a VPN connection is established. Se	ect				
Group Policy:*	yConnect_Management_Tunnel 🛛 💙 🔇					
(H)	AnyConnect_Management_Tunnel					l
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				-diada	

En la ficha **AnyConnect**, seleccione el **objeto de archivo AnyConnect** según el sistema operativo (SO) del terminal.

Overview Analysis Policies	Devices Objects AMP Inte	elligence		. Peploy System Help ▼ dperezve ▼
Remote Access VPN Polic	PN ▶ Remote Access QoS Pla cv Wizard	tform Settings FlexConfig Certificate	S	
1 Policy Assignment 2) Connection Profile 3 Any	Connect 4 Access & Certificate	5 Summary	
	AnyConnect Client Image The VPN gateway can automatically down initiated. Minimize connection setup time b Download AnyConnect Client packages from	load the latest AnyConnect package to the client y choosing the appropriate OS for the selected par n Cisco Software Download Center.	AAA device when the VPN connection is kage. Show Re-order buttons	^
	AnyConnect File Object Name Anyconnect4.9_For_Windows	AnyConnect Client Package Name anyconnect-win-4.9.01095-webdeploy-k9.pkg	Operating System	
				Back Next Cancel
Last login on Saturday, 2021-03-27 at 19:	12:55 PM from rtp-vpn1-1115.cisco.com	How To		, ili ili i cisco

En Access & Certificate especifique el certificado que debe utilizar FTD para sondear su identidad al cliente de Windows.

Nota: Dado que los usuarios no deben interactuar con la aplicación AnyConnect cuando utilizan la función Management VPN, el certificado debe ser de plena confianza y no debe imprimir ningún mensaje de advertencia.

Nota: Para evitar errores de validación de certificados, el campo Nombre común (CN) incluido en el Nombre de asunto del certificado debe coincidir con el FQDN definido en la lista de servidores de perfiles XML (Paso 1 y Paso 2).

Overview Analysis Policies Devices Objects AMP Intelligence		y 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 3 Access & Certificate 5 Summary				
Interface group/Security Zone:* outside 🗸 🗸				
Enable DTLS on member interfaces				
Device Certificates				
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Selec certificate which is used to authenticate the VPN gateway.	ta			
Certificate Enrollment:* SSL_AnyConnect V 🔇				
Enroll the selected certificate object on the target devices				
Access Control for VPN Traffic				
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.				
Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded fro AAA server are still applied to VPN traffic.	202			
	Back	Nex	t	Cancel
Last login on Saturday, 2021-03-27 at 19:12:55 PM from rtp-vpn1-1115.cisco.com How To				uluiu cisco

Por último, seleccione el botón **Finalizar** en la pestaña **Resumen** para agregar la nueva configuración de AnyConnect.



Paso 6. Crear objeto URL

Navegue hasta **Objetos > Administración de objetos** y seleccione **URL** en la tabla de contenido. A continuación, seleccione **Agregar objeto** en el menú desplegable **Agregar URL**.

Proporcione un nombre para el objeto y defina la dirección URL utilizando el mismo FQDN/grupo de usuarios especificado en la lista de servidores de perfiles de VPN de administración (paso 2). En este ejemplo, la URL debe ser dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel.

Overview Analysis Policie	es Devices Objects	AMP Intelligence					tem Help v	dperezve 🔻
Object Management Intrus	sion Rules							
URL URL object represents a single URL of	r IP address. You can use URL	objects and groups in vari	ous places, including access control p	olicies and event searches. Fi	or example, you	Add URL •	Filter	used Objects ocks a specific
Security Group Tag	Name			Va	alue		Override	
A Security Intelligence								
DNS Lists and Feeds			No reco	rds to display				
Network Lists and Feeds		New URL Object	ts	? X				
URL Lists and Feeds		Name						
Sinkhole		Name	Management_Tunnel					
SLA Monitor		Description						
🚮 Time Range								
🕣 Time Zone								
and Tunnel Zone		URL	https://dperezve.jyoungta-labdoma					
() URL		Allow Overrides						
\$ Variable Set				Cancel				
VLAN Tag				Save Cancer				
▲ ∰2 VPN								
AnyConnect File								
Certificate Map								
Group Policy								
IKEVI IPSec Proposal								
IVEN2 IDeas Proposal								
D TKEY2 Insec Proposal						No data to display	< Page 1	of 1 > > C
	_				_			abab
			How To					cisco

Guarde los cambios para agregar el objeto a la lista de objetos.

Paso 7. Definir alias de URL

Para habilitar el Alias de URL en la configuración de AnyConnect, navegue hasta **Devices > VPN** > **Remote Access** y haga clic en el icono del lápiz para editarlo.

A continuación, en la ficha Perfil de conexión, seleccione la configuración que desee, navegue hasta **Alias**, haga clic en el **botón Agregar** y seleccione el **objeto URL** en el menú desplegable Alias URL. Asegúrese de que la casilla de verificación **Enabled** esté activada.

Overview Analysis Policies Device	Edit Connection Profile		? ×	👌 Deploy System	Help 🔻 dperezve 🔻
Device Management NAT VPN + Rem AnyConnect_Management_	Connection Profile:* AnyConnect_Management Group Policy:* AnyConnect_Management Edit Group Policy	_Tunnel			Save Sancel
Connection Profile Access Interfaces	Client Address Assignment AAA Aliases				Policy Assignments (1)
Name	Alias Names: Add URL Alias	? Management_Tunnel	s configured on this device		0
DefaultWEBVPNGroup	Name	OK Cancel			J 🗍
AnyConnect_Management_Tunnel				inel	0
	URL	Status			
			Save Cancel		
Last login on Monday, 2021-04-05 at 23:55:27 PM fro	m rtp-vpn4-759.cisco.com	How To			, ili ili cisco

Guarde los cambios e implemente configuraciones en FTD.

Verificación

Una vez finalizada la implementación, se necesita una primera conexión AnyConnect manual con el perfil VPN de AnyConnect. Durante esta conexión, el perfil de VPN de administración se descarga de FTD y se almacena en C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun. A partir de este punto, las conexiones subsiguientes se deben iniciar a través del perfil VPN de administración sin ninguna interacción del usuario.

Troubleshoot

Para errores de validación de certificados:

- Asegúrese de que el certificado raíz para la Autoridad de Certificación (CA) esté instalado en el FTD.
- Asegúrese de que un certificado de identidad firmado por la misma CA esté instalado en Windows Machine Store.
- Asegúrese de que el campo CN se incluye en el certificado y es el mismo que el FQDN definido en la lista de servidores del perfil VPN de administración y el FQDN definidos en el alias URL.

Para túnel de administración no iniciado:

- Asegúrese de que el perfil de VPN de administración se haya descargado y almacenado en C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun.
- Asegúrese de que el nombre del perfil de VPN de administración sea
 VpnMgmtTunProfile.xml.

Para los problemas de conectividad, recopile el paquete DART y póngase en contacto con el TAC de Cisco para obtener más información.