# Configuración de la Autenticación Basada en Certificado de Anyconnect para el Acceso Móvil

### Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configuración de Cisco Anyconnect en FTD Diagrama de la red Agregar certificado a FTD Configuración de Cisco Anyconnect Crear certificado para usuarios móviles Instalación en dispositivo móvil Verificación Troubleshoot Depuraciones

# Introducción

Este documento describe un ejemplo de la implementación de la autenticación basada en certificados en dispositivos móviles.

# Prerequisites

Las herramientas y dispositivos utilizados en la guía son:

- Cisco Firepower Threat Defense (FTD)
- Centro de administración Firepower (FMC)
- Dispositivo Apple iOS (iPhone, iPad)
- Autoridad de certificación (CA)
- Software cliente Cisco Anyconnect

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN básica,
- SSL/TLS
- Infraestructura de clave pública
- Experiencia con FMC
- OpenSSL
- Cisco Anyconnect

#### **Componentes Utilizados**

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

- FTD de Cisco
- Cisco FMC
- Microsoft CA Server
- XCA
- Cisco Anyconnect
- Apple Ipad

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.

### Configuración de Cisco Anyconnect en FTD

Esta sección describe los pasos para configurar Anyconnect a través de FMC. Antes de comenzar, asegúrese de implementar todas las configuraciones.

#### Diagrama de la red



#### Agregar certificado a FTD

Paso 1. Cree un certificado para el FTD en el dispositivo FMC. Navegue hasta **Dispositivos > Certificado** y elija **Agregar**, como se muestra en esta imagen:

High Firepower Management Center Overview A	Analysis Policies Devices Objects AMP	Intelligence	् Deploy 🔮 🌣 🙆 admin 🔻
	2		
Name Domain	Enrollment Type Status		
V=FTD1			
FTD Global	Manual (CA & ID)		₽ 10 ℃ €
V = Tcoutrie-FTD2			
hd2 Giobal	PKCS12 file		₽ 12 ℃ 1
		How To	

Paso 2. Elija el FTD deseado para la conexión VPN. Elija el **dispositivo FTD** del menú desplegable de dispositivos. Haga clic en el icono + para agregar un nuevo método de inscripción de certificados, como se muestra en esta imagen:

← → C @ O A http	s://tcoutrie-fmc. <b>tcoutrie-</b>	security301.com/ddd/#F	iCerificate 🏠	S 🕹 🖿	□ 0		e <mark>-</mark>	<b>₹</b> =
Getting Started C School C Work							۵°	ther Bookmarks
Firepower Management Center Devices / Certificates	Overview Ar	nalysis Policies	Devices Objects AMP Intelligence	۹	Deploy	¢	° 0	admin 🔻
								Add
Name	Domain	Enrollment Type	Status					
V=FTD1								
FTD	Global	Manual (CA & ID)	(LCA) (L1D)			B	e c	Ψ.
V Coutrie-FTD2								
ftd2	Global	PKCS12 file	Add New Certificate			B	e c	Ì
			Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.					
			How To					

Paso 3. Agregue los certificados al dispositivo. Elija la opción que es el método preferido para obtener certificados en el entorno.

**Consejo:** Las opciones disponibles son: **Certificado firmado automáticamente**: genere un nuevo certificado localmente, **SCEP** - Use Simple Certificate Enrollment Protocol para obtener un certificado de una CA, **Manual**- Instale manualmente el certificado raíz e identidad, **PKCS12** - Cargue un paquete de certificado cifrado con raíz, identidad y clave privada.

Paso 4. Cargue el certificado en el dispositivo FTD. Introduzca el código de acceso (sólo PKCS12) y haga clic en **Guardar**, como se muestra en esta imagen:

Add Cert Enrollme	nt	?
Name* ftdcert Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	PKCS12 File	- 1
PKCS12 File*:	Tcoutrie-ftd2.p12 Browse PKCS12 File	- 1
Passphrase:		- 1
	Skip Check for CA flag in basic constraints of the CA Certificate	
	Cancel	ave

**Nota:** Una vez guardado el archivo, la implementación de los certificados se produce inmediatamente. Para ver los detalles del certificado, elija la ID.

#### Configuración de Cisco Anyconnect

Configure Anyconnect a través de FMC con el asistente de acceso remoto.

Procedimiento:

Paso 1. Inicie el asistente de política VPN de acceso remoto para configurar Anyconnect.

Navegue hasta **Dispositivos > Acceso remoto** y elija **Agregar**.

Listo Devices / VPN / Remote Access Overview Analysis Policies	Devices Objects AMP Intelligence		् Deploy 🗳 🏠 🚳 admin 🔻
Name	Status	Last Modified	
RAVPN	Targeting 1 devices Up-to-date on all targeted devices	2021-07-09 17:10:31 Modified by "admin"	/ 1
	How To		

Paso 2. Asignación de política.

Complete la asignación de políticas: a. Nombre la política

- b. Elija los protocolos VPN deseados
- c. Elija el dispositivo objetivo para aplicar la configuración

Remote Access VPN Policy Wizard           Orolcy Assignment              • Connection Profile             • AnyConnect             • Access & Certificate             • Summary		
Tigged Devices and Protocols     Tigget Devices with a new user-defined connection profile.     Tigget Devices        Devices </td <td>Before You Start      Before You Start, ensure the following configuration     elsements to be in place to complete Remote Access VYP Policy.      Authentication Server      Configure Realm or RADUS Server Group or SSO to     authenticate VYPK clients.      AnyConnect Client Package      Any Connect Client Package      Any Connect Client Package      Any Connect Client Package      Mais surge you have the relevant Clico     credentials to download de alung the wizard.      Device Interface      Interfaces should be already configured on targeted     devices so that they can be used as a security zone     or interface group to enable VPN access.</td> <td></td>	Before You Start      Before You Start, ensure the following configuration     elsements to be in place to complete Remote Access VYP Policy.      Authentication Server      Configure Realm or RADUS Server Group or SSO to     authenticate VYPK clients.      AnyConnect Client Package      Any Connect Client Package      Any Connect Client Package      Any Connect Client Package      Mais surge you have the relevant Clico     credentials to download de alung the wizard.      Device Interface      Interfaces should be already configured on targeted     devices so that they can be used as a security zone     or interface group to enable VPN access.	
How To		Cancel Back Next

Paso 3. Perfil de conexión.

- a. Nombre el perfil de conexión
- b. Establezca el método de autenticación en Client Certificate Only

- c. Asignar un conjunto de direcciones IP y, si es necesario, crear una nueva política de grupo
- d. Haga clic en Next (Siguiente)

Remote Access VPN Policy Wizar	rd
A finite balance of a first first	m () Indexed () Invest Particus () Second
Princy Assignment — O Connection Home	IR C Anyuntest C Access & Unitial C Access & Countries
	Connection Profile:
	Connection Parlies specify the same for grap partices for a VM connection. These policies particles to relative the functional task, free and And accompliable at an environment. They also include user attributes, which and defined in graps policies. Connection Parlies Name.* #ANdPM1
	O This name is configured as a connection alias, it can be used to connect to the VPU gateway
	Authentication, Authoritation & Accounting (AAA):
	Specify the method of authentication (MAA, confluences or both), and the AAA servers that will be used for VPN connections.
	Authentication Marhold Diperc CentRoate DHy +
	Usersame Form 🔹 May specific field 🔷 Use write DX (Distinguished Name) as usersame
	Prinny Tetti D (Qonnan Nana) +
	Secondary Field. Name +
	Autocitation Server +
	Maran II Abarta
	Accounting Server: United Terror
	Client Address Assignment:
	Oter P advisors are to assigned from AAA server, DFOP server and IP address prote. These multiple optimes are satisfactors, P address are protongenerative train of the advisors of AAA server, GFOP server and P address prot.
	C be AAA Server (Reatin or RADUS sch)} ●
	Det DRP Servers
	IPA Addes Poor.
	strop parcy.
	A group patisky is a coffection of near-nomented session and/bulkers which are assigned to client when a VPN connection is expenditured. Select or constrained a Soup-Parky experi.
	Group Policy.* DRDsybiley + +
	Edit Group Puricy

**Nota:** Elija el campo principal que se utilizará para introducir el nombre de usuario para las sesiones de autenticación. En esta guía se utiliza la CN del certificado.

Paso 4. AnyConnect.

Agregue una imagen de Anyconnect al dispositivo. Cargue la versión preferida de Anyconnect y haga clic en **Next**.

Nota: Los paquetes de Cisco Anyconnect se pueden descargar desde Software.Cisco.com.

Paso 5. Acceso y certificado.

Aplique el Certificado a una Interfaz y habilite Anyconnect en el Nivel de Interfaz, como se muestra en esta imagen, y haga clic en **Siguiente.** 



Paso 6. Summary.

Revise las configuraciones. Si se desprotege, haga clic en **finalizar** y, a continuación, **implementar**.

### Crear certificado para usuarios móviles

Cree un certificado para agregarlo al dispositivo móvil utilizado en la conexión.

Paso 1. XCA.

a. Abrir XCA

b. Iniciar una nueva base de datos

Paso 2. Crear CSR

- a. Elija Solicitud de firma de certificado (CSR)
- b. Elija Nueva solicitud
- c. Introduzca el valor con toda la información necesaria para el certificado
- d. Generar una nueva clave
- e. Cuando haya terminado, haga clic en Aceptar

● ◎ ●	💞 X Certificate and Key management
Create Certificate signing request	(a) Presinants Brickant 7000
Source	Extensions Key usage Netscape Advanced
Distinguished name	
Internal name	organizationName
countryName	organizationalUnitName
stateOrProvinceName	commonName Cisco Test
localityName	emailAddress
Туре	Content Add
	Delete
Brivate kov	
Private Key	
Cisco_Test_1 (RSA:2048 bit)	Used keys too Generate a new key
	Cancel

Nota: Este documento utiliza el CN del certificado.

Paso 3. Enviar CSR

- a. Exportar CSR
- b. Enviar CSR a CA para obtener un certificado nuevo

•••	I	X Certificate and Key management	
	Private Keys	Certificates   Templates   Revocation lists	
Internal name A commonName Signed			
Cisco_Test Cisco_Test Unhandled			New Request
			Export
			Import
			Show Details
			Delete
			Jarminute Minute
			fine
Database: /Users/tcoutrie/cisco.xdb		Search	

Nota: Utilice el formato PEM de la CSR.

#### Instalación en dispositivo móvil

Paso 1. Agregue el certificado del dispositivo al dispositivo móvil.

Paso 2. Comparta el certificado con la aplicación Anyconnect para agregar la nueva aplicación de certificado.

**Precaución:** La instalación manual requiere que el usuario comparta el certificado con la aplicación. Esto no se aplica a los certificados enviados a través de MDM.

Cocuments		certs	Ē	Select
Q Search				Ŷ
Cisco_Test.p1	DMChain.p7b	DMS	Certificate Periodal	Certificate Period
Сору	ሮ	4/25/21, 1:50 1 KB	driod.p12 5/13/21, 7:04	driod_1.p12 5/13/21, 7:05
Duplicate	æ		4 KB	4 KB
Move	8	Q 4	P 4	( P
Delete	団	Certificate Perional	Certificate Perional	Certificate Perional
Info	(j)	Noblesse_IPA D_2.p12	Noblesse_IPh one.p12	Noblesse_IPh one_1.p12
Quick Look	۲	4/25/21, 11:18 4 KB	4/25/21, 10:31 3 KB	4/25/21, 11:01 4 KB
Tags	$\bigcirc$			
Rename	1	Certificate Personal	Certificate Perional	Certificate Personal
Share	Û	Noblesse_MA	Noblesse_Wi	Noblesse_Wi
Compress		<b>C_2.p12</b> 4/25/21, 11:19 4 KB	<b>ndows.p12</b> 4/25/21, 12:56 3 KB	ndowsIKE.p12 5/12/21, 12:42 4 KB

Paso 3. Introduzca la contraseña del certificado para el archivo **PKCS12**.

Paso 4. Cree una nueva conexión en Anyconnect.

Paso 5. Navegar a nuevas conexiones; **Conexiones > Agregar conexión VPN**.

AnyConnect	VPN Connections
PRIMARY VIRTUAL PRIVATE NETWORK	
AnyConnect VPN	CALO Enabled
Connections CALO >	HOMEIKE
Details Disconnected >	HOMEIKE-IN
GENERAL	HOMESSL-IN
Settings >	HomelPEC-IN (i)
Diagnostics >	HomelPSEC
About >	HomeSSL
	rtp-vpn-cluster.cisco.com
	Add VPN Connection

Paso 6. Introduzca la información de la nueva conexión.

Descripción: Nombre de la conexión

Dirección del servidor: Dirección IP o FQDN de FTD

Avanzado: Configuraciones adicionales

Paso 7. Elija Advanced.

Paso 8. Elija Certificate y elija su certificado recién agregado.

AnyConnect	VPN Connections	
PRIMARY VIRTUAL PRIVATE NETWOR	IK I	
AnyConnect VPN	Advanced Select Certificate	(j)
Connections FT		(i)
Details Disconnecte	Disabled	Ŭ
Details	Selecting this option will disable certificate authentication.	í
	Automatic	(i)
GENERAL	This will automatically select a certificate for authentication.	$\odot$
Settings	Noblesse_IPAD	(j)
	Issuer: DMsliders-TCOUTRIE-SRV-CA	(j)
Diagnostics	Expiration Date: Apr 25, 2022 11:00:36	
About	Cisco_Test	í
	V Issuer: DMsliders-TCOUTRIE-SRV-CA	
	Expiration Date: Aug 02, 2022 08:12:47	
	Issuer: DMsliders-TCOUTRIE-SRV-CA	(i)
	Expiration Date: Apr 25, 2022 11:04:38	
	Noblesse_IPAD	
	Issuer: DMsliders-TCOUTRIE-SRV-CA	
	Expiration Date: Apr 25, 2022 00:42:05	
CISCO		
CISCO		

Paso 9. Vuelva a **Conexiones** y realice la prueba.

Una vez que se ha realizado correctamente, la alternancia permanece activa y los detalles se muestran en el estado conectado.



### Verificación

El comando **show vpn-sessiondb detail Anyconnect** muestra toda la información sobre el host conectado.

**Consejo:** La opción para filtrar este comando más a fondo son las palabras clave 'filter' o 'sort' agregadas al comando.

Por ejemplo:

Tcoutrie-FTD3# show vpn-sessiondb detail Anyconnect Username : Cisco\_Test Index : 23 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel License : Anyconnect Premium, Anyconnect for Mobile Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 8627 Bytes Rx : 220 Pkts Tx : 4 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : SSL Tunnel Group : SSL Login Time : 13:03:28 UTC Mon Aug 2 2021 Duration : 0h:01m:49s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a7aa95d000170006107ed20 Security Grp : none Tunnel Zone : 0 Anyconnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 Anyconnect-Parent: Tunnel ID : 23.1 Public IP : 10.118.18.168 Encryption : none Hashing : none TCP Src Port : 64983 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : apple-ios Client OS Ver: 14.6 Client Type : Anyconnect Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 6299 Bytes Rx : 220 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 23.2 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM- SHA384 Encapsulation: TLSv1.2 TCP Src Port : 64985 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : SSL VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 2328 Bytes Rx : 0 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 23.3 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 51003 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : DTLS VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 0 Bytes Rx : 0 Pkts Tx : 0 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

### Troubleshoot

#### Depuraciones

Las depuraciones necesarias para solucionar este problema son:

Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255 Si la conexión es IPSEC y no SSL:

Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14 Registros de la aplicación móvil Anyconnect:

#### Vaya a Diagnostic > VPN Debug Logs > Share logs.

AnyConnect	Diagnostics	
PRIMARY VIRTUAL PRIVATE NETWORK		
AnyConnect VPN	VPN Debug Logs	
Connections Asa1 >	Logs	$\supset$
Details Disconnected >	System Information	>
	Share Logs	
GENERAL	Customize Debug Logs	>
Settings >		
Diagnostics	Certificates	>
About >	Profile	>
	Localization	>
CISCO		

- Problema
- Pasos para reproducir

A continuación, navegue hasta Enviar > Compartir con.

3:49 PM Wed Sep 29		•••		奈 47% ■
AnyConnect			Diagnostics	
AnyConnect VPN	Cai	ncel Share Logs	Send	
Connections Asa	Plea follo	ase describe the problem and steps to r owing fields.	Email logs to	>
Details Disconnecte	PRO	BLEM	Administrator	>
GENERAL	Test		Cisco	
Settings	STEPS TO REPRODUCE			>
Diagnostics	nostics Test			
About				>
				>
	The data sent is for diagnostic purposes only and may contain information about configured connections, as well as server and endpoint identities, IP addresses, and username. This data will appear to come from the email address you specify and will not be used for marketing or advertising purposes.			
CISCO				

Esto presenta la opción de utilizar un cliente de correo electrónico para enviar los registros.