# AnyConnect certificaatgebaseerde verificatie voor mobiele toegang configureren

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Cisco AnyConnect op FTD configureren Netwerkdiagram Certificaat aan FTD toevoegen Cisco AnyConnect configureren Certificaat voor mobiele gebruikers maken Installatie op mobiel apparaat Verifiëren Problemen oplossen Debugs

# Inleiding

In dit document wordt een voorbeeld beschreven van de invoering van op certificaten gebaseerde echtheidscontrole op mobiele apparatuur.

## Voorwaarden

De gereedschappen en hulpmiddelen die in de handleiding worden gebruikt, zijn:

- Cisco Firepower Threat Defense (FTD)
- FireSIGHT Management Center (FMC)
- Apple iOS-apparaat (iPhone, iPad)
- certificaatinstantie (CA)
- Cisco AnyConnect-clientsoftware

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis VPN,
- SSL/TLS
- Infrastructuur in openbare vorm
- Ervaring met FMC
- OpenSSL
- Cisco AnyConnect

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTD
- Cisco FMC
- Microsoft CA-server
- XCA
- Cisco AnyConnect
- Apple iPad

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Cisco AnyConnect op FTD configureren

In dit gedeelte worden de stappen beschreven om AnyConnect via FMC te configureren. Zorg ervoor dat alle configuraties worden geïnstalleerd voordat u begint.

#### Netwerkdiagram



#### Certificaat aan FTD toevoegen

Stap 1. Maak een certificaat voor de FTD op het FMC-apparaat. Navigeren in op **Apparaten > Certificaat** en kiezen **Toevoegen**, zoals in deze afbeelding:

Firepower Management Center Overview A	nalysis Policies Devices	Objects AMP	Intelligence	Q. Deploy	e o e	admin 🔻
	2				$\bullet$	Add
Name Domain	Enrollment Type Status					
V 🖛 FTD1						
FTD Global	Manual (CA & ID)	2			₽ ₽ 0	÷ 1
V Tcoutrie-FTD2						
ftd2 Global	PKCS12 file				₽ ₽ 0	÷ 1
		_	_			
			low To			4

Stap 2. Kies de gewenste FTD voor de VPN-verbinding. Kies het **FTD** apparaat uit de afvoerslang. Klik op het pictogram + om een nieuwe inlogmethode voor certificaten toe te voegen, zoals in deze afbeelding:

← → C @ O Å https	://tcoutrie-fmc. <b>tcoutrie-</b> :	security301.com/ididi/#F	KiCerificate	☆ ©	坐 lin 🚥	• 🖬 n 🗖 👅 =
Getting Started 🗅 School 🗅 Work						C Other Bookmark
Firepower Management Cente Devices / Certificates	r Overview Ar	nalysis Policies	Devices Objects AMP Intelligence		Q Deplo	oy 🔮 🌣 😝 admin 🔻
						Add
Name	Domain	Enrollment Type	Status			
V em FTD1						
FTD	Global	Manual (CA & ID)				₽ # C ₹
∨ 🚥 Tcoutrie-FTD2						
ftid2	Global	PKCS12 file	Add New Certificate			₽ ₽ C ₽
			Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.			
			How To			

Stap 3. Voeg de certificaten toe aan het apparaat. Kies de optie die de beste methode is om certificaten in de omgeving te verkrijgen.

**Tip**: De beschikbare opties zijn: **Zelfgetekend certificaat** - genereer lokaal een nieuw certificaat, **SCEP** - gebruik eenvoudig protocol voor **certificaatinschrijving** voor een certificaat bij een CA, **handleiding** - installeer handmatig het **PKCS12**-geüpload certificaat met wortel, identiteit en privé-sleutel.

Stap 4. Upload het certificaat naar het FTD-apparaat. Voer de wachtcode in (alleen PKCS12) en klik op **Opslaan**, zoals in deze afbeelding:

Add Cert Enrollmer	nt	?
Name* ftdcert Description		
CA Information C Enrollment Type: PKCS12 File*: Passphrase:	ertificate Parameters       Key       Revocation         PKCS12 File <ul> <li>Tcoutrie-ftd2.p12</li> <li>Browse PKCS12 File</li> <li>Skip Check for CA flag in basic constraints of the CA Certificate</li> </ul> Skip Check for CA flag in basic constraints of the CA Certificate	
	Cancel	/e

**Opmerking:** Zodra u het bestand hebt opgeslagen, vindt de implementatie van de certificaten onmiddellijk plaats. Selecteer de gewenste ID voor de certificeringsgegevens.

#### Cisco AnyConnect configureren

Elke verbinding via FMC configureren met de wizard Toegang op afstand.

Procedure: Initiatief

Stap 1. Start de wizard Remote Access VPN om AnyConnect te configureren.

Navigeren in op Apparaten > Externe Toegang en kiezen Toevoegen.

cisco	Firepower Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence			٩	Deploy 6	° • •	admin •
													<b>→</b> (	Add
Name					Status				Last Modified					
RAVP	4				Targeting 1 de Up-to-date or	vices all targeted d	evices		2021-07-09 17: Modified by *adm	10:31 nin*		/ 1		
								How To						

Stap 2. Beleidstoewijzing.

Voltooi de beleidstaak:

- a. Geef het beleid een naam
- b. Kies de gewenste VPN-protocollen
- c. Kies het doelapparaat om de configuratie toe te passen

Remote Access VPN Policy Wizard         Policy Assignment       2 Connection Profile       3 AnyConnect       6 Access & Cettificate       5 Summary         Targeted Devices and Protocols         Tripe devices and Protocols         Tripe devices and Protocols         UPN Protocols:         VPN Protocols:         Description:         Philes (KDg)       Targeted Devices         Salt         Philes (KDg)       Targeted Devices:         Connection Protocols:	Before You Start Before You Start Before You Start elements to be in place to complete Remote Access VPN Policy.  Authentication Server Configure Realm or RADIUS Server Group or 550 to authenticate VPN clients.  AnyConnect Client Package Main sure you have AnyConnect package for VPN Client downloaded or you have the relevant Clisco credentials to download it during 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 VPI acces.
Available Devices Stetcted Devices	

Stap 3. Connection-profiel.

- a. Naam van het verbindingsprofiel
- b. Stel de verificatiemethode alleen in op clientcertificaat

- c. Pas een IP-adrespool aan en indien nodig een nieuw groepsbeleid.
- d. Klik op Volgende

ante Annese VPN Policy Wizard
nue nuesa erit rong intend
stoy Assymment Connection Profile 3 AnyConnect 4 Access & Certificate 5 Burninary
Connection Holme:
Connection Private specify the tower groups paticiants for a VMS connection. These paticities periods and the set of the connection to be patient to be addresses and water patients to be addresses and water patients and other of the patient patient to be addresses and water patients. They also include user antibutes, which is and other of the patient beams of the latter of the
Toy survey is configured as a connection align it can be used to connect to the VPC connece
Automatication, Automatication (AAA)
Specify the method of authentication (AAA, earthquares or body), and the AAA answers that will be used for VPN
connectiona. Automatication Mathematication Mathematication (Copert CepterSpace Only) •
Utermane From 🐂 tape specific Head 🕤 Use errise TMI (Distriguished Name) as username
Annual Concentration Concentra
Society Field Remain
Authoritation Server: to the server is the s
Accounting Soviet:
Clast Address Assignment:
Clear P actions can be assigned from AAA savery, EPCF array en early P address pords. When many and a savery and a saver
🗌 ble AAA Server (Basim or RADUS sing) 🔴
Discher Steres
WA ADDREN TOTAL
A group particy is a collection of user-internal session ambures which are assigned to coller when a VML
correction is instantinue, added of colling a shore process data. Group Process - Marcinette

**Opmerking:** Kies het Primaire veld dat gebruikt moet worden om de gebruikersnaam voor de verificatiesessie in te voeren. De GN van het certificaat wordt in deze handleiding gebruikt.

Stap 4. Verbinding.

Voeg een AnyConnect-afbeelding aan het apparaat toe. Upload de gewenste versie van AnyConnect en klik op **Volgende**.

**Opmerking:** Cisco AnyConnect-pakketten kunnen worden gedownload van **Software.Cisco.com**.

Stap 5. Toegang en certificaat.

Pas het certificaat op een interface toe en schakelt AnyConnect op interfaceniveau in zoals in deze afbeelding, en klik op **Volgende.** 



Stap 6. Samenvatting

Bekijk de configuraties. Als alle controles zijn uitgevoerd, klik op Voltooien en stel dan in.

## Certificaat voor mobiele gebruikers maken

Maak een certificaat dat wordt toegevoegd aan het mobiele apparaat dat in de verbinding wordt gebruikt.

Stap 1. XCA.

a. Open XCA

b. Een nieuwe database starten

Stap 2. Maak CSR.

- a. Kies certificaataanvraag (CSR)
- b. Kies nieuwe aanvraag
- c. Voer de waarde in met alle informatie die voor het certificaat nodig is
- d. Een nieuwe sleutel genereren
- e. Klik na voltooiing op OK

	💞 X Certificate and Key management
Create Certificate signing request	3) Mariade The
Source	Extensions Key usage Netscape Advanced
Distinguished name	
Internal name	organizationName
countryName	organizationalUnitName
stateOrProvinceName	commonName Cisco_Test
localityName	emailAddress
Туре	Content Add
	Delete
Private kev	
Cines Test 1 (DSA:20.49 bit)	
Cisco_Test_T (RSA-2048 bit)	Used keys too Generate a new key
	Cancel OK

**Opmerking:** In dit document wordt de GN van het certificaat gebruikt.

Stap 3. Vermeld CSR.

- a. CSR exporteren
- b. CSR aan CA indienen om een nieuw certificaat te verkrijgen

	I X	Certificate and Key management	
	Private Keys	Certificates   Templates   Revocation lists	
Internal name A commonName Signed			New Request
			Export
			Import
			Show Details
			Delete
-			
			Jarminecta.
			2 Diverso Time
[[			
Database: /Users/tcoutrie/cisco.xdb		Search	

**Opmerking:** Gebruik het PEM-formaat van de CSR.

### Installatie op mobiel apparaat

Stap 1. Voeg het apparaatcertificaat toe aan het mobiele apparaat.

Stap 2. Deel het certificaat met de AnyConnect-toepassing om de nieuwe certificaattoepassing toe te voegen.

**Voorzichtig:** De handmatige installatie vereist dat de gebruiker het certificaat met de toepassing deelt. Dit is niet van toepassing op certificaten die via MDM's worden geduwd.

Cocuments		certs	Ē	Select
Q Search				Ŷ
Certificate	DMChain.p7b	DMS	Certificate Period Display	Certificate Personal
Сору	மூ	4/25/21, 1:50 1 KB	driod.p12 5/13/21, 7:04	driod_1.p12 5/13/21, 7:05
Duplicate	Đ		4 KB	4 KB
Move	8	(Contraction of the second sec	( Contraction of the contraction	(P)
Delete	<b> </b>	Certificate Perional	Certificate Perional	Certificate Perionat
Info	(1)	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	0			
Rename	1	Certificate Perional	Certificate Personal	Certificate Perional
, Share	Û	Noblesse_MA	Noblesse_Wi	Noblesse_Wi
Compress		<b>C_2.p12</b> 4/25/21, 11:19 4 KB	ndows.p12 4/25/21, 12:56 3 KB	ndowsIKE.p12 5/12/21, 12:42 4 KB

- Stap 3. Voer het certificaatwachtwoord in voor het bestand PKCS12.
- Stap 4. Maak een nieuwe verbinding op AnyConnect.
- Stap 5. Navigeer naar nieuwe verbindingen; **Aansluitingen > VPN-verbinding toevoegen**.

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

Stap 6. Voer de informatie in voor de nieuwe verbinding.

Beschrijving: Geef de connectie een naam

Serveradres: IP-adres voor FQDN-exemplaar van FTD

Geavanceerd: Aanvullende configuraties

Stap 7. Kies Geavanceerd.

Stap 8. Kies Certificaat en kies uw nieuwe certificaat.

AnyConnect	VPN Connections	VPN Connections				
PRIMARY VIRTUAL PRIVATE NETWO	RK					
AnyConnect VPN	Advanced Select Certificate	(j)				
Connections FT		(i)				
Details Disconnecte	Disabled					
	Selecting this option will disable certificate authentication.	í				
	Automatic	(i)				
GENERAL	This will automatically select a certificate for authentication.	$\odot$				
Settings	Noblesse_IPAD	(i)				
	Issuer: DMsliders-TCOUTRIE-SRV-CA	(i)				
Diagnostics	Expiration Date: Apr 25, 2022 11:00:36	Ŭ				
About	Cisco_Test	í				
	Issuer: DMsliders-TCOUTRIE-SRV-CA      Eveloptics Date: Aug 02, 2022 09:12:47	()				
	Noblesse IPAD					
	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						

Stap 9. Navigeer terug naar verbindingen en test.

Zodra dit gelukt is, blijft de draaiknop ingeschakeld en tonen de gegevens de verbinding in de status.



## Verifiëren

De opdracht toont vpn-sessionedetails Any toont alle informatie over de aangesloten host.

**Tip**: De optie om deze opdracht verder te filteren is de 'filter' of 'type'-sleutelwoorden die aan de opdracht worden toegevoegd.

#### Voorbeeld:

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

## Problemen oplossen

### Debugs

Debugs die nodig zijn om een oplossing voor dit probleem te vinden, zijn:

Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255 Als de verbinding IPSEC en niet SSL is:

Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14 Logs van de mobiele applicatie AnyConnect:

#### Navigeren in naar diagnostiek > VPN Debug Logs > Share logs.

AnyConnect	Diagnostics
AnyConnect VPN	VPN Debug Logs
Connections Asa1	Logs
Details Disconnected	> System Information >
	Share Logs
GENERAL	Customize Debug Logs
Settings	>
Diagnostics	Certificates
About	> Profile >
	Localization
cisco	

Voer de informatie in:

- Probleem
- Stappen om te reproduceren

Navigeer dan om **te verzenden > Delen met**.

3:49 PM Wed Sep 29		•••		중 47% ■
AnyConnect			Diagnostics	
AnyConnect VPN		Cancel Share Log	s Send	
Connections	Asa	Please describe the problem and steps following fields.	s to r Email logs to	>
Details Disconn	ecte	PROBLEM	Administrator	>
	Те	est	Cisco	
GENERAL			Share with	>
Settings		STEPS TO REPRODUCE		
Diagnostics	Те	est		>
About				>
				>
սիսիս		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				

Dit biedt de optie om een e-mailclient te gebruiken om de logbestanden te verzenden.