# Konfigurieren der auf AnyConnect-Zertifikaten basierenden Authentifizierung für den mobilen Zugriff

# Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren von Cisco AnyConnect auf FTD Netzwerkdiagramm Zertifikat zu FTD hinzufügen Konfigurieren von Cisco AnyConnect Zertifikat für mobile Benutzer erstellen Installation auf Mobilgeräten Überprüfung Fehlerbehebung Debugger

### Einleitung

Dieses Dokument beschreibt ein Beispiel für die Implementierung einer zertifikatsbasierten Authentifizierung auf Mobilgeräten.

### Voraussetzungen

Die im Leitfaden verwendeten Tools und Geräte sind:

- Cisco FirePOWER Threat Defense (FTD)
- Firepower Management Center (FMC)
- Apple iOS-Gerät (iPhone, iPad)
- Zertifizierungsstelle (Certificate Authority, CA)
- Cisco AnyConnect Client-Software

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Basis-VPN
- SSL/TLS
- Public Key-Infrastruktur
- Erfahrung mit FMC

- OpenSSL
- Cisco AnyConnect

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTD von Cisco
- Cisco FMC
- Microsoft CA-Server
- XCA
- Cisco AnyConnect
- Apple-iPad

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

# Konfigurieren von Cisco AnyConnect auf FTD

In diesem Abschnitt werden die Schritte zur Konfiguration von AnyConnect über FMC beschrieben. Bevor Sie beginnen, stellen Sie sicher, dass Sie alle Konfigurationen bereitstellen.

### Netzwerkdiagramm

	Internal Firepower Certificate Center Authority	 Management			
	Internal Lan	Firepower Threat Defense	Internet	ر ج س Mobile Users	
ا، ا د	ı.ı]ı. ISCO				

Zertifikat zu FTD hinzufügen

Schritt 1: Erstellen Sie ein Zertifikat für die FTD auf der FMC-Appliance. Navigieren Sie zu **Devices > Certificate**, und wählen Sie **Add (Hinzufügen)** aus, wie in diesem Bild gezeigt:

Firepower Management Center Devices / Certificates	C Overview A	nalysis Policies	Devices Objects	AMP	Intelligence		م	Deploy	¢ 😵	admi	in •
	-	3								Ad	
Name	Domain	Enrollment Type	Status								
V=FTD1											
FTD	Global	Manual (CA & ID)	CA ID						B• 💰	C 🖥	
V IIII Tcoutrie-FTD2											
ħd2	Global	PKCS12 file	CA ID						G• 💰	Cì	
					How To						
											4

Schritt 2: Wählen Sie die für die VPN-Verbindung gewünschte FTD aus. Wählen Sie die **FTD-Appliance** aus der Dropdown-Liste aus. Klicken Sie auf das + Symbol, um eine neue Methode zur Zertifikatsregistrierung hinzuzufügen, wie in diesem Bild gezeigt:

← → C @ O A https://	tcoutrie-fmc.tcoutrie-s	ecurity301.com/ddd/#P	KICerificate \$\$	S ኛ IV ED 🕹 🛅 ڬ 🚍 🔝 🗮
Setting Started C School C Work				C Other Bookmarks
CISCO Firepower Management Center Devices / Certificates	Overview Ar	nalysis Policies	Devices Objects AMP Intelligence	् Deploy 🗳 🌣 🥥 admin 🔻
				Add
Name	Domain	Enrollment Type	Status	
V=FTD1				
FTD	Global	Manual (CA & ID)	(LCA) (LLD)	B• 12° C° च
V = Tcoutrie-FTD2				
ftd2	Global	PKCS12 file	Add New Certificate	₽₽С₩
			Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.	
			How To	

Schritt 3: Fügen Sie dem Gerät die Zertifikate hinzu. Wählen Sie die Option aus, die die bevorzugte Methode zum Abrufen von Zertifikaten in der Umgebung ist.

**Tipp:** Folgende Optionen stehen zur Verfügung: **Selbstsigniertes Zertifikat** - Erstellen Sie lokal ein neues Zertifikat, **SCEP** - Verwenden Sie das Simple Certificate Enrollment Protocol, um ein Zertifikat von einer Zertifizierungsstelle zu erhalten. **Manuell**- Installieren Sie das

Root- und Identitätszertifikat manuell, **PKCS12** - Hochladen eines verschlüsselten Zertifikatspakets mit Stamm, Identität und privatem Schlüssel.

Schritt 4: Laden Sie das Zertifikat auf das FTD-Gerät hoch. Geben Sie den Passcode ein (nur PKCS12), und klicken Sie auf **Speichern**, wie in diesem Bild gezeigt:

Add Cert Enrollme	nt			?
Name* ftdcert Description				
CA Information C Enrollment Type: PKCS12 File*: Passphrase:	Certificate Parameters Ker PKCS12 File Tcoutrie-ftd2.p12  Skip Check for CA flag in	y Rev	Browse PKCS12 File	icate
			Cancel	Save

**Anmerkung:** Nachdem Sie die Datei gespeichert haben, erfolgt die Bereitstellung der Zertifikate sofort. Wählen Sie die ID aus, um die Zertifikatdetails anzuzeigen.

#### Konfigurieren von Cisco AnyConnect

Konfigurieren Sie AnyConnect über FMC mit dem Remote-Zugriffs-Assistenten.

Verfahren:

Schritt 1: Starten Sie den Remote Access VPN Policy Wizard, um AnyConnect zu konfigurieren.

Navigieren Sie zu Geräte > Remotezugriff, und wählen Sie Hinzufügen aus.

cisco Devices / VPN / Remote Access Overview Analysis Policies	Devices Objects AMP Intelligence		Q Dep	oloy 🔮 🌣	😫 admin 🔻
			-		Add
Name	Status	Last Modified			
RAVPN	Targeting 1 devices Up-to-date on all targeted devices	2021-07-09 17:10:31 Modified by "admin"		ί Ψ	
	How To				

Schritt 2: Richtlinienzuweisung.

Führen Sie die Richtlinienzuweisung aus: antwort: Policy benennen

- b. Wählen Sie die gewünschten VPN-Protokolle
- c. Wählen Sie das Zielgerät aus, um die Konfiguration anzuwenden.

Remote Access VPN Policy Vilzara     AnyConnect Access & Certificate 6     Summary

Schritt 3: Verbindungsprofil.

antwort: Benennen Sie das Verbindungsprofil.

b. Legen Sie die Authentifizierungsmethode auf Nur Clientzertifikat fest.

- c. Zuweisen eines IP-Adresspools und ggf. Erstellen einer neuen Gruppenrichtlinie
- d. Klicken Sie auf Weiter

Remote Access VPN Policy Wizard
Patric Assessed Connection Profile 2 And/Careed 1 Ansesse & Control an 2 Supervay
Connection Profiles specify the turned processing for a VPN connection. These policies pertain to creating the turned fact, from AAA is accomplicated and those addresses are assigned. They also include user attributes, which are defined in group Address. Connection Profile Teams <sup>1</sup> RoBH1
This name is configured as a convection axis, I can be used to convect to the VPN general
Authentication, Authoritation & Accounting (AAA):
Specify the method of admentation (AAA, conficience or biot); and the AAA assume that all be used for VMs connections.
Authenticution Method Deper Cardicate Dely +
Usersander Form 🤞 Map speeche teel 🔿 Use erste DK (Detropatived Name) is usersanse
Primay Falst CK (Connean Name) •
Secondary Pest Name •
Authorization Shrine (Marine Halling)
Accounting Sometric +
Client Address Assignment:
Cline IP athless carbo examples from AAA saves, CEPC Parver and D Adobins provide Value multitude quintum are instructed, P athless and provide a Value in the ord of AAA saves, CEPC Coll saver and B athless provide and and
Use AAA Storee (Regime of RAEOUS or A)
C toe Poster Post
IPv4 Address Posts: BAKPN
I'vd Addens Poots
Gray Poloy:
A group policy is a collection of unamoviented session ambustes which are assigned to cleant where a VMN connection is established. Select or create a Group Policy object.
uniter may interpreted in T

**Anmerkung:** Wählen Sie das primäre Feld aus, um den Benutzernamen für Authentifizierungssitzungen einzugeben. In diesem Leitfaden wird der CN des Zertifikats verwendet.

Schritt 4: AnyConnect.

Fügen Sie der Appliance ein AnyConnect-Image hinzu. Laden Sie die bevorzugte Version von AnyConnect hoch, und klicken Sie auf **Weiter**.

Anmerkung: Cisco AnyConnect-Pakete können unter Software.Cisco.com heruntergeladen werden.

Schritt 5: Zugriff und Zertifikat.

Wenden Sie das Zertifikat auf eine Schnittstelle an, und aktivieren Sie Anyconnect auf Schnittstellenebene, wie in diesem Bild gezeigt, und klicken Sie auf **Weiter**.



Schritt 6: Zusammenfassung.

Überprüfen Sie die Konfigurationen. Wenn alle Auscheckvorgänge ausgeführt werden, klicken Sie auf **Fertig stellen** und dann **bereitstellen**.

### Zertifikat für mobile Benutzer erstellen

Erstellen Sie ein Zertifikat, das dem Mobilgerät hinzugefügt werden soll, das in der Verbindung verwendet wird.

Schritt 1: XCA

antwort: Öffnen von XCA

- b. Neue Datenbank starten
- Schritt 2: CSR erstellen

antwort: Wählen Sie Certificate Signing Request (CSR) aus.

- b. Neue Anforderung auswählen
- c. Geben Sie den Wert zusammen mit allen für das Zertifikat erforderlichen Informationen ein.
- d. Erstellen eines neuen Schlüssels
- e. Klicken Sie abschließend auf OK

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

Anmerkung: In diesem Dokument wird der CN des Zertifikats verwendet.

Schritt 3: CSR senden

antwort: CSR exportieren

b. CSR an CA senden, um ein neues Zertifikat zu erhalten

	d'	X Certificate and Key management	
	Private Keys	Certificates Templates Revocation lists	
Internal name A commonName Signed			New Request
			Export
			Import
			Show Details
			Delete
			Jarminecta Discharbo Fine
Database: /Users/tcoutrie/cisco.xdb		Search	

Anmerkung: Verwenden Sie das PEM-Format der CSR.

#### Installation auf Mobilgeräten

Schritt 1: Fügen Sie das Gerätezertifikat dem Mobilgerät hinzu. Schritt 2: Freigeben des Zertifikats an die AnyConnect-Anwendung, um die neue Zertifikatsanwendung hinzuzufügen

**Vorsicht:** Bei der manuellen Installation muss der Benutzer das Zertifikat für die Anwendung freigeben. Dies gilt nicht für Zertifikate, die über MDMs gesendet werden.

Cocuments		certs	Ē	Select
Q Search				Ŷ
Certificate Personal	DMChain.p7b	DMS	Certificate Personal Solution	Certificate Perional
Сору	Ф	4/25/21, 1:50 1 KB	<b>driod.p12</b> 5/13/21, 7:04	driod_1.p12 5/13/21, 7:05
Duplicate	Œ		4 KB	4 KB
Move			Part P	P
Delete	乛	Certificate Perional	Perional Perional	Perisonal
t Info	<b>i</b>	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 Personal	Certificate Perional	Certificate Perional
, Share	٢	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	<b>ndowsIKE.p12</b> 5/12/21, 12:42 4 KB

Schritt 3: Geben Sie das Zertifikatskennwort für die PKCS12-Datei ein.

Schritt 4: Erstellen Sie eine neue Verbindung auf AnyConnect.

Schritt 5: Navigieren zu neuen Verbindungen Verbindungen > VPN-Verbindung hinzufügen.

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

Schritt 6: Geben Sie die Informationen für die neue Verbindung ein.

Beschreibung: Benennen Sie die Verbindung.

Serveradresse: IP-Adresse oder FQDN FTD

Erweitert: Zusätzliche Konfigurationen

Schritt 7. Wählen Sie Erweitert aus.

Schritt 8: Wählen Sie Zertifikat und wählen Sie das neu hinzugefügte Zertifikat aus.

AnyConnect	VPN Connections	VPN Connections			
PRIMARY VIRTUAL PRIVATE NETWO	RK				
AnyConnect VPN	Advanced Select Certificate	<u>(</u> )			
Connections FT		(j)			
Details Disconnecto	Disabled	0			
Disconnect	Selecting this option will disable certificate authentication.	i			
	Automatic				
GENERAL	This will automatically select a certificate for authentication.				
Settings	Noblesse_IPAD	i			
	Issuer: DMsliders-TCOUTRIE-SRV-CA	(i)			
Diagnostics	Expiration Date: Apr 25, 2022 11:00:36	U			
About	Cisco_Test	í			
	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					

Schritt 9. Navigieren Sie zurück zu Verbindungen, und testen Sie.

Nach dem erfolgreichen Wechsel bleibt der Umschalter eingeschaltet und Details werden im Status als verbunden angezeigt.



### Überprüfung

Der Befehl **show vpn-sessiondb detail Anyconnect** zeigt alle Informationen über den angeschlossenen Host.

**Tipp:** Die Option zum weiteren Filtern dieses Befehls sind die dem Befehl hinzugefügten Schlüsselwörter 'filter' oder 'sort'.

#### Beispiele:

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

### Fehlerbehebung

#### Debugger

Folgende Debugger sind zur Behebung dieses Problems erforderlich:

Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255 Wenn die Verbindung IPSEC und nicht SSL ist:

Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14 Protokolle der mobilen Anwendung AnyConnect:

#### Navigieren Sie zu Diagnostic > VPN Debug Logs > Share logs.

AnyConnect	Diagnostics	
PRIMARY VIRTUAL PRIVATE NETWORK		
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		

- Problem
- Schritte zur Reproduktion

Navigieren Sie dann zu Senden > Freigeben mit.

3:49 PM Wed Sep 29		•	•••		중 47% ■
AnyConnect				Diagnostics	
AnyConnect VPN	Ca	ancel Share	e Logs	Send	
Connections	Asa Ple	ease describe the problem and lowing fields.	d steps to n	Email logs to	>
Details Disconr	PRO	DBLEM		Administrator	>
GENERAL	Test			Cisco	
Settings	ST	EPS TO REPRODUCE		Share with	>
Diagnostics	Test				>
About					>
					>
	Th ab ad ad	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					

Dadurch wird die Option zum Senden der Protokolle mithilfe eines E-Mail-Clients angezeigt.