# Configurazione dell'autenticazione basata sul certificato Anyconnect per l'accesso mobile

# Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Configurazione di Cisco Anyconnect su FTD
Esempio di rete
Aggiungi certificato a FTD
Configurazione Di Cisco Anyconnect
Crea certificato per utenti mobili
Installa nel dispositivo mobile
Verifica
Risoluzione dei problemi
Debug

## Introduzione

Questo documento descrive un esempio di implementazione dell'autenticazione basata su certificati su dispositivi mobili.

# Prerequisiti

Gli strumenti e i dispositivi utilizzati nella guida sono:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Dispositivo Apple iOS (iPhone, iPad)
- CA (Certificate Authority)
- Software Cisco Anyconnect Client

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN di base
- SSL/TLS
- Infrastruttura a chiave pubblica
- Esperienza con FMC

- OpenSSL
- Cisco Anyconnect

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione di Cisco Anyconnect su FTD

In questa sezione viene descritto come configurare Anyconnect tramite FMC. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

### Esempio di rete

	Internal Certificate Authority	Management			
	Internal Lan	Firepower Threat Defense	Internet	- ج ه Mobile	Jsers
, C	ııı ı. Isco				

#### Aggiungi certificato a FTD

Passaggio 1. Creare un certificato per l'FTD sull'accessorio FMC. Passare a Dispositivi > Certificato e scegliere Aggiungi, come mostrato nell'immagine:

Firepower Management Center Devices / Certificates	Overview An	alysis Policies	evices Objects AMP Intelligence	Q. Dep	ioy 💕 🌣 🚯 admin 🔻
	=				
Name	Domain	Enrollment Type	tatus		
V=FTD1					
FTD	Global	Manual (CA & ID)	CA (LD)		₽ Ø C €
✓ IIII Tcoutrie-FTD2					
ħd2	Global	PKCS12 file	(CA) (((10)		₽ ₽ C ¥
			How To		

Passaggio 2. Scegliere l'FTD desiderato per la connessione VPN. Selezionare l'accessorio FTD dal menu a discesa dei dispositivi. Fare clic sull'icona + per aggiungere un nuovo metodo di registrazione dei certificati, come mostrato nell'immagine seguente:

← → C @ O A https:	//tcoutrie-fmc.tcoutrie-s	security301.com/ididi/#F	KiCerificate 🗘	🗢 🛃 lin	□ 0	B 0 -	
Oetting Started C School C Work						C1 00	er Bookmarks
Firepower Management Center Devices / Certificates	Overview Ar	nalysis Policies	Devices Objects AMP Intelligence	٩	Deploy	e o o	admin 🕶
							Add
Name	Domain	Enrollment Type	Status				
∨ em FTD1							
FTD	Global	Manual (CA & ID)	140A (1430)			₽ ₽ C	¥.
✓ IIIII Tcoutrie→FTD2							
ftd2	Global	PKCS12 file	Add New Certificate			₽₽℃	Ŷ.
			Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.				
			Cancel Add				
			How To.				

Passaggio 3. Aggiungere i certificati al dispositivo. Scegliere l'opzione che rappresenta il metodo

preferito per ottenere i certificati nell'ambiente.

Suggerimento: le opzioni disponibili sono: Certificato autofirmato - Genera un nuovo certificato localmente, SCEP - Usa protocollo SCEP (Simple Certificate Enrollment Protocol) per ottenere un certificato da una CA, Manuale - Installa manualmente il certificato radice e identità, PKCS12 - Carica il bundle di certificati crittografati con radice, identità e chiave privata.

Passaggio 4. Caricare il certificato sul dispositivo FTD. Immettere il passcode (solo PKCS12) e fare clic su Save (Salva), come mostrato nell'immagine:

Add Cert Enrollme	nt			•
Name* ftdcert Description				
CA Information	Certificate Parameters K	Key Rev	ocation	
PKCS12 File*:	Tcoutrie-ftd2.p12	<b></b>	Browse PKCS12 File	]
Passphrase:		$\bigcirc$		
	Skip Check for CA flag	in basic co	nstraints of the CA Certif	icate
			Cancel	Save

Nota: una volta salvato il file, la distribuzione dei certificati viene eseguita immediatamente. Per visualizzare i dettagli del certificato, scegliere l'ID.

#### Configurazione Di Cisco Anyconnect

Configurare Anyconnect tramite FMC con la procedura guidata di accesso remoto.

Passaggio 1. Avvia la Configurazione guidata criteri VPN di Accesso remoto per configurare Anyconnect.

Passare a Dispositivi > Accesso remoto e scegliere Aggiungi.



Passaggio 2. Assegnazione criteri.

Completare l'assegnazione dei criteri:

- a. Assegnare un nome al criterio.
- b. Scegliere i protocolli VPN desiderati.
- c. Scegliere il dispositivo di destinazione per applicare la configurazione.

Remote Access VPN Policy Wizard Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 3 Summary	
Policy Assignment Connection Politie   Augeonet   Access & Centracia Summary <b>Cannection Politie</b> Access & Centracia Summary <b>Connection Politie</b> Access & Centracia Summary <b>Connection Politie</b> Access & Centracia Summary <b>Connection Policy Connection Politie Summary Connection Politie Connectio</b>	Perfore You start, measure the following configuration elements be inplace to complete Remote Access VNN Policy.     Authentication Server     Authentication Server     Authentication Server     AngConnect Client Package     Mark sure you have Ap/Connect package for VNN Clientitation to download it during the witard.     Device Interface     More Instruction as a security profile as a security profile of or interface group to enable VMN access.
How To	Cancel Back Next

Passaggio 3. Profilo di connessione.

- a. Assegnare un nome al profilo di connessione.
- b. Impostare il metodo di autenticazione su Solo certificato client.
- c. Assegnare un pool di indirizzi IP e, se necessario, creare un nuovo oggetto Criteri di gruppo.
- d. Fare clic su Next (Avanti).

Remote Access VPN Policy Wizard	
1 Policy Assignment  O Connection Profile  3 AnyOr	anext 4 Access & Certificate 5 Summay
	Connection Profiles specify the funner group policies for a VMX connection. These policies partials to creating the tunner tank of two AAA as accompliated and how addresses are assigned. They also include user attributes, which are defined in group policies."
	The name as configured as a connection size, if calls and obsciences to the VMM galaxies
	Automotivation, noncontrast previous. Specify membra of automotivation (AAA, centricates or both), and the AAA servers that will be used for VPN connections.
	Automication Method. Clean Cardicale Dely +
	Usersana Fran 👻 May spocific field 🔷 Use entries DM (Distriguished Stame) as usersane Contribution Primery Frield: CM (Connors Name) 🔹
	Secondary Relat. Appendix +
	Authorization Server: • + Preserver VACAGO
	Accounting Server: • +
	Client Address Assignment:
	Clear P address can be assigned from AAA server, DICP server and P address pools. When multiple options are selected, P address registered to red in the option of the AAA server, DICP server and P address pool. One AAA Server (Pealm or RADUS on)) •
	the P Advances Note
	libit Address Proze Address Proze
	A group policy is a collection of user-oriented esculor attributes which are assigned to client when a VRN connection is anathinities. Select or orsea a Group Policy object.
	Group Policy* Othoraphatey  + Edit Group Policy

Nota: scegliere il campo Principale da utilizzare per immettere il nome utente per le sessioni di autenticazione. In questa guida viene utilizzato il CN del certificato.

Passaggio 4. AnyConnect.

Aggiungere un'immagine Anyconnect all'accessorio. Caricare la versione preferita di Anyconnect e fare clic su Avanti.

Nota: i pacchetti Cisco Anyconnect possono essere scaricati da Software.Cisco.com.

Passaggio 5. Accesso e certificato.

Applicare il certificato a un'interfaccia e abilitare Anyconnect a livello di interfaccia, come mostrato nell'immagine, e fare clic su Avanti.

💼 Firefox File Edit View History Bookmarks Tools Window Help			0 🛳 🛳 💷 📼	💲 📷 🗢 🕤 Q 🚍 🥔 Fri Jul 30 10:40 AM
O      O     Cisco Firepower Management C      +				
← → C @ https://tcoutrie-fmc.tcoutrie-security301.co	n/ddd/#RAVpnSetupWizard		\$	S 7 1V 10 8 8 9 5 1 1
Getting Started 🗅 School 🗅 Work				C Other Bookmarks
-It-th: Firepower Management Center Overview Analysis Process / VPN / Setup Wizard	licies Devices Objects AMP Intelligence			् Deploy 💕 🌣 🕲 admin 🔻
Remote Access VPN Policy Wizard				
1 Policy Assignment 2 Connection Profile 3 AnyConnect	Access & Certificate 5 Summary			
Remote User	Network Interface for Incoming VPN Access Select or create an Interface Group or a Security Zone that conto	VIN biside Cor Device Res		
	Interface group/Security Zone:* outside	+ +		
	All the devices must have interfaces as part of the Interface	Group/Security Zone selected.		
	Device Certificates Device certificate (also called identity certificate) identifies the V	PN gateway to the remote access		
	clients. Select a certificate which is used to authenticate the VPM Certificate Enrollment:* fed2	l gateway.		
	Enroll the selected certif	cate object on the target devices		
	Access Control for VPN Traffic			
	All decrypted traffic in the VPN tunnel is subjected to the Access this option to bypass decrypted traffic from the Access Control F	Control Policy by default. Select olicy.		
			How To	Cancel

Passaggio 6. Riepilogo.

Esaminare le configurazioni. Se tutte le estrazioni sono state eseguite, fare clic su fine, quindi su distribuisci.

## Crea certificato per utenti mobili

Creare un certificato da aggiungere al dispositivo mobile utilizzato nella connessione.

Passaggio 1. XCA

a. Apri XCA

b. Avvia un nuovo database

Passaggio 2. Creare CSR.

a. Scegliere Richiesta firma certificato (CSR)

- b. Scegli nuova richiesta
- c. Inserire il valore con tutte le informazioni necessarie per il certificato
- d. Genera una nuova chiave
- e. Al termine, fare clic su OK

	•	Í	X Certificate a	and Key management		
Crea	ate Certificate signing req	luest				(a) (Persiade Truckano 744
	Sourc	е	Extensions	Key usage Netscape	Advanced	
	Distinguished name					
	Internal name			organizationName		
	countryName			organizationalUnitName		
	stateOrProvinceName			commonName	Cisco Test	
	localityName			emailAddress	cisco_irest	
	localityName			emainAudress		
	Туре			Content		Add
						Add
						Delete
	Private key					
	Ciaco Test 1 (DCA:20	40 hit)				ata a namelani
	CISCO_TEST_T (RSA-20	46 DIL)		Used key	Gener	ate a new key
						Cancel

Nota: questo documento utilizza il CN del certificato.

Passaggio 3. Inviare CSR.

- a. Esportazione del CSR
- b. Inviare CSR a CA per ottenere un nuovo certificato

		đ	X Certificate and Key manager	nent		
		Private Keys	Certificates	Templates	Revocation lists	
	Internal name A commonName Signed					New Request
						Export
						Import
						Show Details
						Delete
						2 Farminecta Minshoo Fine
D	atabase: /Users/tcoutrie/cisco.xdb		Search			

Nota: utilizzare il formato PEM del CSR.

Installa nel dispositivo mobile

Passaggio 1. Aggiungere il certificato del dispositivo al dispositivo mobile. Passaggio 2. Condividere il certificato con l'applicazione Anyconnect per aggiungere la nuova applicazione di certificato.

Attenzione: l'installazione manuale richiede la condivisione del certificato con l'applicazione. Ciò non si applica ai certificati sottoposti a push tramite MDM.

<b>〈</b> Documents		certs	Ē	9 🔡 Select
Q Search				Ŷ
Cisco_Test.p1	DMChain.p7b	DMS	Certificate Personal Control	Certificate Personal Control
Copy Duplicate	ڻ ب	4/25/21, 1:50 1 KB	driod.p12 5/13/21, 7:04 4 KB	driod_1.p12 5/13/21, 7:05 4 KB
Move Delete		Certificate Perional	Certificate Personal	Certificate Perionat
Info Quick Look	() ()	Noblesse_IPA D_2.p12 4/25/21, 11:18 4 KB	Noblesse_IPh one.p12 4/25/21, 10:31 3 KB	Noblesse_IPh one_1.p12 4/25/21, 11:01 4 KB
Tags	0			
Rename	1	Certificate Personal	Certificate Perional	Certificate Perional
Compress		Noblesse_MA C_2.p12 4/25/21, 11:19 4 KB	Noblesse_Wi ndows.p12 4/25/21, 12:56 3 KB	Noblesse_Wi ndowsIKE.p12 5/12/21, 12:42 4 KB

Passaggio 3. Immettere la password del certificato per il file PKCS12.

Passaggio 4. Creare una nuova connessione su Anyconnect.

Passaggio 5. Passare a nuove connessioni; Connessioni > Aggiungi connessione VPN.

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 >	HomeIPEC-IN	í
Diagnostics >	HomeIPSEC	í
About >	HomeSSL	í
	rtp-vpn-cluster.cisco.com	í
	Add VPN Connection	>
cisco		

Passaggio 6. Immettere le informazioni per la nuova connessione.

Descrizione: assegnare un nome alla connessione

Indirizzo server: indirizzo IP o FQDN FTD

Avanzate: configurazioni aggiuntive

Passaggio 7. Scegliere Avanzate.

Passaggio 8. Scegliere Certificato e scegliere il certificato appena aggiunto.

AnyConnect		VPN Connections		
PRIMARY VIRTUAL PRIVATE NETWORK				
AnyConnect VPN		Advanced Select Certificate		(j)
Connections	FT			(i)
Details	Disconnecte	Disabled		0
Details	Disconnecte	Selecting this option will disable certificate authenticatio	n.	í
		Automatic		(j)
GENERAL		This will automatically select a certificate for authenticat	ion.	٢
Settings		Noblesse_IPAD		í
Discussion		Issuer: DMsliders-TCOUTRIE-SRV-CA	(i) >	(i)
Diagnostics		Expiration Date: Apr 25. 2022 11:00:36		
About		Cisco_Test Issuer: DMsliders-TCOUTRIE-SRV-CA	(i) >	(i)
		Expiration Date: Aug 02, 2022 08:12:47	<b>U</b>	(i)
	_	Noblesse_IPAD	-	
		Issuer: DMsliders-TCOUTRIE-SRV-CA	(i) >	(i)
E N Is E		Expiration Date: Apr 25, 2022 11:04:38		
		Noblesse_IPAD	() >	
		Issuer: DMsliders-TCOUTRIE-SRV-CA		
		Expiration Date: Apr 25, 2022 00:42:05	_	
CIS	sco			

Passaggio 9. Tornare a Connessioni e verificare.

Se l'operazione ha esito positivo, l'interruttore rimane acceso e i dettagli mostrano la connessione nello stato.



## Verifica

Il comando show vpn-sessiondb detail Anyconnect permette di visualizzare tutte le informazioni sull'host connesso.

Suggerimento: l'opzione per filtrare ulteriormente il comando è rappresentata dalle parole chiave 'filter' o 'sort' aggiunte al comando.

Ad esempio:

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

# Risoluzione dei problemi

#### Debug

I debug necessari per risolvere il problema sono:

Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255

Se la connessione è IPSEC e non SSL:

Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14

Registri dall'applicazione Anyconnect per dispositivi mobili:

Selezionare Diagnostica > Log di debug VPN > Log di condivisione.

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	

Immettere le informazioni:

- Problema
- Passi da riprodurre

Passare quindi a Invia > Condividi con.

3:49 PM Wed Sep 29		•••		중 47% ■	
AnyConnect		Diagnostics			
PRIMARY VIRTUAL PRIVATE NETWO		K			
AnyConnect VPN	Cai	ncel Share Log	gs Send		
Connections As	e Plea follo	ase describe the problem and step owing fields.	es to r Email logs	; to >	
Details Disconnecte	PRO	PROBLEM			
GENERAL	Test		Cisco		
Settings	STEP	PS TO REPRODUCE	Share w	rith	
Diagnostics	Test				
About				>	
				>	
	The abou addr addr purp	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					

In questo documento viene presentata l'opzione per l'utilizzo di un client di posta elettronica per l'invio dei log.

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).