# Konfigurieren der Zertifikatzuordnung für die sichere Client-Authentifizierung auf FTD über FDM

# Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Netzwerkdiagramm Konfigurationen Konfiguration in FDM Schritt 1: FTD-Schnittstelle konfigurieren Schritt 2: Cisco Secure Client-Lizenz bestätigen Schritt 3: Adresspool hinzufügen Schritt 4: Sicheres Clientprofil erstellen Schritt 5: Hochladen eines sicheren Client-Profils an FDM Schritt 6: Gruppenrichtlinie hinzufügen Schritt 7. FTD-Zertifikat hinzufügen Schritt 8: CA zu FTD hinzufügen Schritt 9. VPN-Verbindungsprofil für Remote-Zugriff hinzufügen Schritt 10. Zusammenfassung für Verbindungsprofil bestätigen In FTD-CLI bestätigen Bestätigung in VPN-Client Schritt 1: Kopieren des sicheren Clientprofils auf den VPN-Client Schritt 2: Clientzertifikat bestätigen Schritt 3: Zertifizierungsstelle bestätigen Überprüfung Schritt 1: VPN-Verbindung initiieren Schritt 2: VPN-Sitzungen in FTD CLI bestätigen Fehlerbehebung Zugehörige Informationen

# Einleitung

In diesem Dokument wird beschrieben, wie der Cisco Secure Client mit SSL auf FTD über FDM mithilfe der Zertifikatzuordnung für die Authentifizierung eingerichtet wird.

## Voraussetzungen

### Anforderungen

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

- Cisco FirePOWER Gerätemanager (FDM) virtuell
- Firewall Threat Defense (FTD) virtuell
- VPN-Authentifizierungsablauf

Verwendete Komponenten

- Cisco FirePOWER Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8
- Cisco Secure Client 5.1.4.74
- Profil-Editor (Windows) 5.1.4.74

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 kennen.

# Hintergrundinformationen

CertificateMatch ist eine Funktion, mit der Administratoren Kriterien konfigurieren können, die der Client verwenden muss, um ein Clientzertifikat für die Authentifizierung mit dem VPN-Server auszuwählen. Diese Konfiguration wird im Clientprofil angegeben. Dabei handelt es sich um eine XML-Datei, die mit dem Profil-Editor verwaltet oder manuell bearbeitet werden kann. Die CertificateMatch-Funktion kann verwendet werden, um die Sicherheit von VPN-Verbindungen zu verbessern, indem sichergestellt wird, dass nur ein Zertifikat mit spezifischen Attributen für die VPN-Verbindung verwendet wird.

In diesem Dokument wird beschrieben, wie der Cisco Secure Client mithilfe des allgemeinen Namens eines SSL-Zertifikats authentifiziert wird.

Diese Zertifikate enthalten einen gemeinsamen Namen, der für Autorisierungszwecke verwendet wird.

- CA: ftd-ra-ca-common-name
- Techniker-VPN-Client-Zertifikat: vpnEngineerClientCN
- Manager VPN Client-Zertifikat: vpnManagerClientCN
- Serverzertifikat: 192.168.1.200

## Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.



Netzwerkdiagramm

# Konfigurationen

### Konfiguration in FDM

Schritt 1: FTD-Schnittstelle konfigurieren

Navigieren Sie zu Device > Interfaces > View All Interfaces (Gerät > Schnittstellen), konfigurieren Sie die interne und externe Schnittstelle für FTD auf der Registerkarte Interfaces (Schnittstellen).

Bei GigabitEthernet0/0

- Name: außen
- IP-Adresse: 192.168.1.200/24

Firewall	Device Manager	Monitoring	Ø Policies	∰E Objects	Device: firepower	r		$(\Sigma_{-})$			?	* ad * Ac	min Iministrator	~ .	SECURE
	Device Summary Interfaces														
	Cisco Firepower Threat	0/3 0/4 0/5	o/6 0/7	MGMT CONSOLE											
	9 Interfaces	unnel internaces						<b></b> ,		T F	ilter				+
	NAME			LO	GICAL NAME ST	TATUS	MODE	IP ADDRESS			STANDBY AD	ORESS	MONITOR	FOR HA	ACTIONS
	> 🗸 GigabitEtherr	net0/0		ou	utside		Routed	192.168.1.200 State	1				Enabled		

FTD-Schnittstelle

Schritt 2: Cisco Secure Client-Lizenz bestätigen

Navigieren Sie zu Device > Smart License > View Configuration, und bestätigen Sie den Artikel Cisco Secure Client License in RA VPN License.



Secure Client-Lizenz

#### Schritt 3: Adresspool hinzufügen

Navigieren Sie zu Objekte > Netzwerke, und klicken Sie auf + Schaltfläche.

Firewall Device Manag	er Monitoring Policies Objects Device:	firepower (	) (admin Administrator v else S	ECURE
Object Types ←	Network Objects and Groups 7 objects		Filter Preset filters: System defined. User defined	•
Security Zones	NAME			ACTIONS
Application Filtere	1 IPV4-Private-10.0.0.0-8	NETWORK 10.0.0/8		

Adresspool hinzufügen

Geben Sie die erforderlichen Informationen ein, um einen neuen IPv4-Adresspool hinzuzufügen. Klicken Sie auf die Schaltfläche OK.

- Name: ftd-cert-match-pool
- Typ: Bereich
- IP-Bereich: 172.16.1.150-172.16.1.160

# Add Network Object

Name
ftd-cert-match-pool
Description
1.
Туре
Network Host FQDN Range
IP Range
172.16.1.150-172.16.1.160
e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100
CANCEL OK

Ø

X

Details zur	n IPv4-Adresspoo	Ы
-------------	------------------	---

Schritt 4: Sicheres Clientprofil erstellen

Laden Sie den Secure Client Profile Editor von der <u>Cisco Software-</u>Website herunter, und installieren Sie ihn. Navigieren Sie zur Serverliste, und klicken Sie auf die Schaltfläche Hinzufügen. Geben Sie die erforderlichen Informationen ein, um einen Server-Listeneintrag hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

- Anzeigename: Zertifikatübereinstimmung
- FQDN oder IP-Adresse: 192.168.1.200
- Primäres Protokoll: SSL

- (9) Preferences (Part 1)	Server List										
Preferences (Part 2)	Profile: Untit	ed									
Certificate Pinning Certificate Matching Certificate Enrollment	Hostname	Host Addr	User Group	Backup Ser	SCEP	Mobile Sett	Certificate				
	Note: it is hi	ghly recommen	ded that at le	ast one server t	be define in	Ad D	el	1			
						Server List	Entry				
						Server Load	Balancing Se	rvers SCEP Mobile C	ertificate Pinning		
						Primary	Server		Connection Inform	ation	
						Display	Name (requir	ed) cert-match	Primary Protocol	SSL 🗸	
						FQDN	or IP A	User Group	ASA gateway	(	
						192.16	0 1 200		Auth Method I	During IKE Negotiation	CAD An Connet
						A PEIAG	0.1.200			burning the negotidation	EAP*AnyConnect ~
						Group	URL		IKE Identity (I	OS gateway only)	EAP-AnyConnect
						Group 192.16	URL 8.1.200		IKE Identity (I	(OS gateway only)	EAP-Anyconnect
						Group 192.16	URL 8.1.200	Backup Servers	IKE Identity (I	(OS gateway only)	EAP-AnyConnect
						Group 192.16	8.1.200 URL 8.1.200	Backup Servers Host Address	IKE Identity (I	(OS gateway only)	EAP-Anyconnet
						Group 192.16	URL 8.1.200	Backup Servers Host Address	IKE Identity (I	IOS gateway only) Add Mount In	[EAP-Anyconnect ]
						Group 192.16	URL 8.1.200	Backup Servers Host Address	IKE Identity (I	IOS gateway only) Add Move Up	EAP-Anyconnect V
						Group 192.16	URL 8.1.200	Backup Servers Host Address	IKE Identity (I	IOS gateway only) Add Move Up Move D	EAP-Anyconnect V
						Group 192.16	URL 8.1.200	Backup Servers Host Address	IKE Identity (I	IOS gateway only) Add Move Up Move D Delete	EAP-AnyConnect V

Navigieren Sie zu Zertifikatzuordnung, und klicken Sie auf die Schaltfläche Hinzufügen. Geben Sie die erforderlichen Informationen ein, um einen Distinguished Name Entry hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

- Name: KN
- Muster: vpnEngineerClientCN
- Operator: Gleich



Hinweis: Aktivieren Sie in diesem Dokument die Option MatchCase.

File Help							
VPN Preferences (Part 1) Preferences (Part 2)	Certificate Profile: C:	Matching Users\jianzh	3\OneDrive	- Cisco\Des	ktop\vpnCli	ent.xml	
Backup Servers     Certificate Dinaing     Certificate Matching     Certificate Enrolment     Mobile Policy     Server List	Key Usag Deci Enci CRL Key Data Key Non Digi	e pher_Only _Sign _Cert_Sign _Agreem _Encipher _Encipherm. _Repudiat tal_Signa		xtended Ke Server/ ClientA CodeSi EmailPi IPSecEi IPSecU IPSecU TimeSt OCSPSi	y Us Auth uth gn rotect ndSystem unnel ser amp ign	DVCS	ate
	Custom E	ch only certif	tch Key (Ma. Add Delete	(ey Usage	u Hrann		Distinguished Name Entry     Name     CN     Pattern     VpnEngineerClient     Operator     Operator
	Distinguis	hed Name (	Max	xtended Ke	y Usage		Wildcard
	Name	Pattern	Wildcard	Operator	MatchC	Add	MatchCase
						Delete	OK Cancel

Distinguished Name-Eintrag

Speichern Sie das sichere Clientprofil auf dem lokalen Computer, und bestätigen Sie die Profildetails.



Sicheres Client-Profil

Schritt 5: Hochladen eines sicheren Client-Profils an FDM

Navigieren Sie zu Objekte > Secure Client Profile, und klicken Sie auf CREATE SECURE CLIENT PROFILE (SICHERES CLIENT-PROFIL ERSTELLEN).

Firewall Device Manager Monitoring	Policies Objects Device: firepower	S. 🚔 🗐 ? : admin Administrator	SECURE
Object Types ←	Secure Client Profiles		
C Networks		<b>T</b> Filter	+
S Ports	# NAME	FILE NAME ACTIONS	
G Security Zones			
🐬 Application Filters		There are no Secure Client profile objects yet.	
C <sup>9</sup> URLs		Start by creating the first Secure Client profile object.	
© Geolocations		CREATE SECURE CLIENT PROFILE	
Syslog Servers			
✗ IKE Policies			
🗠 IPSec Proposals			
Secure Client Profil			
Survey Identity Sources			

Sicheres Clientprofil erstellen

Geben Sie die erforderlichen Informationen ein, um ein sicheres Clientprofil hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

- Name: secureClientProfile
- Sicheres Clientprofil: secureClientProfile.xml (Hochladen vom lokalen Computer)

Add Secure Client Profile	0	×
Name secureClientProfile		
Description		
		4
UPLOAD secureClientProfile.xml		
CANCEL	ОК	

### Schritt 6: Gruppenrichtlinie hinzufügen

Navigieren Sie zu Gerät > Remotezugriff-VPN > Konfiguration anzeigen > Gruppenrichtlinien, und klicken Sie auf +.

Firewall Device M	anager Monitoring Policies Objects	Device: firepower	$(\Sigma_{-})$	🚔 🗐 ? :	admin Administrator	SECURE
RA VPN ←	Device Summary Group Policies					
Connection Profiles	2 objects			<b>T</b> Filter		+
SAML Server	# NAME	DNS SERVER	IPV4 SPLIT TUNNELING	IPV6 SPLIT TUNNELING	SECURE CLIENT PROFILES	ACTIONS
	1 DfltGrpPolicy		Allow all traffic	Allow all traffic		

Gruppenrichtlinie hinzufügen

Geben Sie die erforderlichen Informationen ein, um eine Gruppenrichtlinie hinzuzufügen, und klicken Sie auf die Schaltfläche OK.

- Name: ftd-cert-match-grp
- Profile für sichere Clients: secureClientProfile

Add Group Policy		0	×
Q, Search for attribute	Name		_
Basic	ftd-cert-match-grp Description		
Session Settings			11
Advanced Address Assignment	DNS Server	,	,
Split Tunneling Secure Client	Banner Text for Authenticated Clients		
Traffic Filters	Secure Client profiles		
This biomaci Proxy	▼ Filter		
	SecureClientProfile     Create new Secure Client Prof     CANCEL     OK		
	CANCEL	ОК	

Details zur Gruppenrichtlinie

Schritt 7. FTD-Zertifikat hinzufügen

Navigieren Sie zu Objekte > Zertifikate, und klicken Sie auf Internes Zertifikat hinzufügen aus + Element.

Firewall Device Man	ager Monitoring Policies Objects Device	i: firepower		dmin Idministrator
Object Types ←	Certificates			
C Networks	121 objects		T Filter	+ · 🔊
🕏 Ports			Preset filters: System defined, User defined	Add Internal CA
Security Zones	H NAME	туре		Add Internal Certificate ACTIONS
🐬 Application Filters	1 AAA-Certificate-Services	Trusted CA Certificate		Add Trusted CA Certificate
🖉 URLs	2 ACCVRAIZ1	Trusted CA Certificate		
Geolocations	3 Actalis-Authentication-Root-CA	Trusted CA Certificate		
Geolocations	4 AffirmTrust-Commercial	Trusted CA Certificate		
Syslog Servers	5 AffirmTrust-Networking	Trusted CA Certificate		
🔏 IKE Policies	6 AffirmTrust-Premium	Trusted CA Certificate		
🐴 IPSec Proposals	7 AffirmTrust-Premium-ECC	Trusted CA Certificate		
Secure Client Profiles	8 Amazon-Root-CA-1	Trusted CA Certificate		
s Identity Sources	9 Amazon-Root-CA-2	Trusted CA Certificate		
1 Users	10 Amazon-Root-CA-3	Trusted CA Certificate		
	11 DefaultInternalCertificate	Internal Certificate		
X Certificates	12 DefaultWebserverCertificate	Internal Certificate		

Internes Zertifikat hinzufügen

#### Klicken Sie auf Zertifikat und Schlüssel hochladen.



Zertifikat und Schlüssel hochladen

Geben Sie die erforderlichen Informationen für das FTD-Zertifikat ein, importieren Sie ein Zertifikat und einen Zertifikatschlüssel vom lokalen Computer, und klicken Sie dann auf die Schaltfläche

OK.

- Name: ftd-vpn-Zertifikat
- Validierungsverwendung für spezielle Services: SSL-Server



Schritt 8: CA zu FTD hinzufügen

Navigieren Sie zu Objekte > Zertifikate, und klicken Sie auf Vertrauenswürdiges Zertifizierungsstellenzertifikat hinzufügen aus + Element.

Ę	Firewall Device Manager	Monitoring	Policies	Objects	Device: firepow	ver	$(\Sigma)$		0	?	:	admin Administrator	<ul> <li>→ uluulu cisco</li> </ul>	SECURE
7	Application Filters	Cortific	otoo											
Ø	URLs	Certino	ales											
Ŷ	Geolocations	120 objects	6				<b>T</b> 1	Filter					+~	<b>R</b> ~
	Outlos Contra						Preset fi	ilters: Sys	tem defin	ed. User.o	defined	Add Interna	I CA	
	Syslog Servers	# NAME				туре						Add Interna	al Certificate	ACTIONS
ß	IKE Policies	1 NGF	W-Default-Inter	nalCA		Internal CA						Add Truste	d CA Certificate	1
-	IPSec Proposals	2 AAA-	Certificate-Ser	vices		Trusted CA Certificate								
-	Secure Client Profiles	3 ACC	VRAIZ1			Trusted CA Certificate								
5	Identity Sources	4 Acta	lis-Authenticati	on-Root-CA		Trusted CA Certificate								
1	Users	5 Affin	mTrust-Comme	rcial		Trusted CA Certificate								
Q	Certificates	6 Affin	mTrust-Network	king		Trusted CA Certificate								
<u>م</u>	Control Varia	7 Affin	mTrust-Premiur	n		Trusted CA Certificate								
	Secret Keys					T								

Vertrauenswürdiges Zertifizierungsstellenzertifikat hinzufügen

Geben Sie die erforderlichen Informationen für die Zertifizierungsstelle ein, und importieren Sie ein Zertifikat vom lokalen Computer.

- Name: ftdvpn-ca-cert
- · Validierung und Verwendung für spezielle Services: SSL-Client

# Add Trusted CA Certificate

Name		
ftdvpn-ca-cert		
Certificate Paste certificate, or choose a file (DER, PEM, CR	RT, CER)	ftd-ra-ca.crt Upload.Certificate
BEGIN CERTIFICATE MIIDbDCCA1SgAwIBAgIIUkKgLg229/8wDQYJKo BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQ	ZIhvcNAQELBQAwbTELMAkGA1UE QHEwVUb2t5bzEOMAwGA1UEChMF	- - 
Skip CA Certificate Check 🕕		
Validation Usage for Special Services SSL Client ×		~
	CANCEL	ОК
Details zum vertrauenswürdigen Zertifizierungsstellenzertifikat		

2

### Schritt 9. VPN-Verbindungsprofil für Remote-Zugriff hinzufügen

Navigieren Sie zu Gerät > Remotezugriff-VPN > Konfiguration anzeigen > Verbindungsprofile, und klicken Sie auf die Schaltfläche VERBINDUNGSPROFIL ERSTELLEN.

Firewall Device M	anager Monitoring	Policies Object	s Device: firepower	۵. 🗳	admi	n v divili SECURE
RA VPN ←		Device Summary Remote Access	s VPN Connection Profiles			
Group Policies					<b>Y</b> Filter	+
SAML Server		# NAME	АЛА	GROUP POLICY	ACT	nons
			Ther	are no Remote Access Connectio	ons yet.	
			Г	Start by creating the first Connection	n.	
			L	CREATE CONNECTION PROFILE		

VPN-Verbindungsprofil für Remote-Zugriff hinzufügen

Geben Sie die erforderlichen Informationen für das Verbindungsprofil ein, und klicken Sie auf die

Schaltfläche Weiter.

- · Name des Verbindungsprofils: ftd-cert-match-vpn
- Authentifizierungstyp: Nur Client-Zertifikat
- Benutzername vom Zertifikat: Zuordnungsspezifisches Feld
- Primärfeld: CN (Common Name)
- Sekundäres Feld: OU (Organisationseinheit)
- IPv4-Adresspools: ftd-cert-match-pool

Firewall Device Manager Monitoring Policies	Cobjects Device: firepower	(admin Administrator admin SECURE
Remote Access VPN	Connection and Client (2) Remote User Experience	3 Global Settings 4 Summary
Remote Users Gi	ents — Internet	PREPOVER
	Connection and Client Config Specify how to authenticate remote users and the secure clients inside network.	guration they can use to connect to the
	Connection Profile Name This name is configured as a connection alias, it can be used to connect to the ftd-cert-match-vpn	VPN gateway
	Group Alias (one per line, up to 5) Group URL (one ftd-cert-match-vpn	e per line, up to 5)
	Primary Identity Source Authentication Type Client Certificate Only	
	Username from Certificate  Map Specific Field  Primary Field  CN (Common Name)  V  OU (Organisat	i ional Unit) ~
	<ul> <li>Use entire DN (distinguished name) as username</li> <li>Advanced</li> </ul>	
	Authorization Server Accounting Serve Please select V Please select	r V
	Client Address Pool Assignment IPv6 Address Pool Endpoints are provided an address from this pool Cndpoints are provided Cndpoints are provided C	I ed an address from this pool
	DHCP Servers  CANCEL	

Details zum VPN-Verbindungsprofil

Geben Sie die erforderlichen Informationen für die Gruppenrichtlinie ein, und klicken Sie auf die Schaltfläche Weiter.

• Gruppenrichtlinie anzeigen: ftd-cert-match-grp

Firewall Device Manager Monitoring Policies Objects	Device: firepower	() () () () () () () () () () () () () (	min v viluele SECURE
Remote Access VPN	Connection and Client     Configuration     Remote User Experience	3 Global Settings 4	Summary
Ramote Users	ents — Internet — R Client Certificate — BIESNACE	REPOWER INTEGRACES	orate Resources
	Remote User Experience A group policy is a collection of user-oriented session attributes whi VPN connection is established. Select or create a Grou View Group Policy Itd-cert-match-grp Policy Group Brief Details	For the second secon	
	Banner Text for Authentic BACK		

Gruppenrichtlinie auswählen

Wählen Sie Certificate of Device Identity, Outside Interface, Secure Client Package für die VPN-Verbindung aus.

- Zertifikat für die Geräteidentität: ftd-vpn-cert
- Externe Schnittstelle: außen (GigabitEthernet0/0)
- Secure Client-Paket: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



Hinweis: Deaktivieren der Funktion zum Ausschließen von NAT in diesem Dokument.

Firewall Device Manager 例 中 Monitoring Policies Objects D	evice: firepower
Remote Users 🗖 Secure Clients - Internet	Client Certificate
	Global Settings
These settings apply to all c	control the basic functioning of the connection. Changes to any of these options onnection profiles; you cannot configure different settings in different profiles.
Certificate of Devia ftd-vpn-cert (M Fully-qualified Dor e.g. rayon.example.c Access Control for Decrysted VPN traffic policy for decrysted t and the autorization Bypass Access NAT Exempt () () () () () () () () () () () () () (	e Identity ilidation Us ge: SSL Se V Outside Interface outside (GigabitEthernet0/0) V nain Name for the Outside Interface Port 443 m e.g. 8080 VPN Traffic Is subjected to access control policy inspection by default. Enabling the Bypass Access Control raffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL. ACL downloaded from the AAA server are still applied to VPN traffic s Control policy for decrypted traffic (sysopt permit-vpn)
Secure Client	Package
in a day doop in the end installer when the clip You can download se	nt authenticates for the first time. The user can then install the package from the system. zure client packages from software.cisco.com (2.
You must have the ne	tessary secure client somware isoense.
UPLOAD PACK	AGE 🗸
Windows: cisco	-secure-client-win-5.1.4.74-webdeploy-k9.pkg
	BACK

Details der globalen Einstellungen

Schritt 10. Zusammenfassung für Verbindungsprofil bestätigen

Bestätigen Sie die für die VPN-Verbindung eingegebenen Informationen, und klicken Sie auf die Schaltfläche FERTIG stellen.

þ	Firewall Device Manager	Monitoring	Ø Policies	Dbjects	Device: firepower	$\odot$	۲	?	÷	admin Administrator	Ý	cisco SECURE

#### Summary

Review the summary of the Remote Access VPN configuration.

STEP 1: CONNECTION AND CLIENT CONFIGURATION	N	
Primary Identity Source		
Authentication Type	Client Certificate Only	
Primary Identity Source	-	
Fallback Local Identity Source	-	
Username from Certificate	Map Specific Field	
Primary Field	CN (Common Name)	
Secondary Field	OU (Organisational Unit)	
Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		
IPv4 Address Pool	G ftd-cert-match-pool	
IPv6 Address Pool	- G	
DHCP Servers	-	
STEP 2: GROUP POLICY		
Group Policy Name	ថ្មឹ⊕ ftd-cert-match-grp	
Banner + DNS Server		
DNS Server	8 -	
Banner text for authenticated clients	-	
Session Settings		
Maximum Connection Time / Alert Interval	Unlimited / 1 minutes	
Idle Timeout / Alert Interval	30 / 1 minutes	
Simultaneous Login per User	3	
Split Tunneling		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling	Allow all traffic over tunnel	
Secure Client		
Secure Client Profiles	General secureClientProfile	
STEP 3: GLOBAL SETTINGS		
Certificate of Device Identity		
Outside Interface	GigabitEthemet0/0 (outside)	
Fully-qualified Domain Name for the Outside	-	
Interface		
Port	443	
Access Control for VPN Traffic	No	
NAT Exempt		
NAT Exempt	NO	
Inside Interfaces	-	
Inside Networks	-	
Secure Client Package		
	Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg	1

Zusammenfassung für Verbindungsprofil bestätigen

### In FTD-CLI bestätigen

Bestätigen Sie die VPN-Verbindungseinstellungen in der FTD-CLI nach der Bereitstellung vom FDM.

// Defines IP of interface interface GigabitEthernet0/0 speed auto nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.1.200 255.255.255.0 // Defines a pool of addresses ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftd-vpn-cert enrollment terminal keypair ftd-vpn-cert crl configure // Server Certificate crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 . . . . . . quit // Defines Trustpoint for CA crypto ca trustpoint ftdvpn-ca-cert enrollment terminal validation-usage ssl-client crl configure // CA crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 . . . . . . quit // Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2 anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml anyconnect enable tunnel-group-list enable cache disable error-recovery disable

// Configures the group-policy to allow SSL connections group-policy ftd-cert-match-grp internal group-policy ftd-cert-match-grp attributes dhcp-network-scope none vpn-simultaneous-logins 3 vpn-idle-timeout 30 vpn-idle-timeout alert-interval 1 vpn-session-timeout none vpn-session-timeout alert-interval 1 vpn-filter none vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelall ipv6-split-tunnel-policy tunnelall split-dns none split-tunnel-all-dns disable client-bypass-protocol disable msie-proxy method no-modify vlan none address-pools none ipv6-address-pools none webvpn anyconnect ssl dtls none anyconnect mtu 1406 anyconnect ssl keepalive none anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client none anyconnect dpd-interval gateway none anyconnect ssl compression none anyconnect dtls compression none anyconnect modules none anyconnect profiles value secureClientProfile type user anyconnect ssl df-bit-ignore disable always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication tunnel-group ftd-cert-match-vpn type remote-access tunnel-group ftd-cert-match-vpn general-attributes address-pool ftd-cert-match-pool default-group-policy ftd-cert-match-grp tunnel-group ftd-cert-match-vpn webvpn-attributes authentication certificate group-alias ftd-cert-match-vpn enable

#### Bestätigung in VPN-Client

Schritt 1: Kopieren des sicheren Clientprofils auf den VPN-Client

Kopieren Sie ein sicheres Client-Profil in einen technischen VPN-Client und einen Manager-VPN-Client.



Hinweis: Verzeichnis des sicheren Clientprofils auf dem Windows-Computer: C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

🔒 🛛 🛃 🚽 🕴 Profil	le				
File Home	Share	View			
← → • ↑ 📘	> Thi	s PC > Local Disk (C:) > Program	nData > Cisco > Cisco Secure Clie	ent > VPN > Profile	ري م م
		Name	Date modified	Туре	Size
Quick access		MgmtTun	£, _3/2024 20:15	File folder	
	- <sup>-</sup>	AnvConnectProfile vsd	6/., 2024 21:44	XSD File	97 KB
Downloads	*	secureClientProfile	712, 2024 10:48	XML Document	4 KB

Kopieren des sicheren Clientprofils auf den VPN-Client

#### Schritt 2: Clientzertifikat bestätigen

Navigieren Sie im VPN-Client des Technikers zu Certificates - Current User > Personal > Certificates (Zertifikate - Aktueller Benutzer > Persönlich), und überprüfen Sie das Client-Zertifikat,

das für die Authentifizierung verwendet wird.



Zertifikat für Techniker-VPN-Client bestätigen

Doppelklicken Sie auf das Client-Zertifikat, navigieren Sie zu Details, überprüfen Sie die Details des Betreffs.

• Betreff: CN = vpnEngineerClientCN

Certificate	×
General Details Certification	Path
Show: <all></all>	$\sim$
Field	Value ^
Subject	vpnEngineerClientCN, vpnEngi
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher
Enhanced Key Usage	Client Authentication (1.3.6.1
Thumborint algorithm	cha1
CN = vpnEngineerClientCN O = Cisco L = Tokyo S = Tokyo C = JP	
	Edit Properties Copy to File
	OK

Details zum Techniker-Client-Zertifikat

Navigieren Sie im VPN-Client des Managers zu Certificates - Current User > Personal > Certificates, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.



Zertifikat für Manager VPN Client bestätigen

Doppelklicken Sie auf das Client-Zertifikat, navigieren Sie zu Details, überprüfen Sie die Details des Betreffs.

• Betreff: CN = vpnManagerClientCN

how: <all></all>	$\sim$
Field Subject	Value Thursday, June 19, 2025 9:41 vpnManagerClientCN, vpnMan
Public key Public key parameters Key Usage Enhanced Key Usage	RSA (2048 Bits) 05 00 Digital Signature, Key Encipher Client Authentication (1.3.6.1
Netscape Comment	xca certificate sha 1
D = Cisco = Tokyo S = Tokyo C = JP	]
	Edit Properties Copy to File

×

Details zum Manager-Clientzertifikat

🔊 Certificate

Schritt 3: Zertifizierungsstelle bestätigen

Navigieren Sie im VPN-Client des Technikers und im VPN-Client des Managers zu Certificates -Current User > Trusted Root Certification Authorities > Certificates, und überprüfen Sie die für die Authentifizierung verwendete Zertifizierungsstelle.

Ausgestellt von: ftd-ra-ca-common-name

🚡 Cons	ole1 - [Console Root\Certificates - Current	User\Trusted Root Certification A	Authorities\Certificates]			1-1	o ×	
🚡 <u>F</u> ile	Action View Favorites Window	Help					- 8 3	к
<b>(</b>	2 🗊 🤞 🐂 🖼 👔							
Con:	sole Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan ^	Actions	
~ 🗟 🤆	Certificates - Current User	2127.0.0.1	127.0.0.1	5/17/2027	Server Authenticati	duo-endpoir	Certificates	
~	Personal Personal	AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati	Sectigo (AAJ	More	
	Trusted Root Cartification Authorities	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati	DigiCert Balt		1
Ť	Certificates	🔄 Class 3 Public Primary Cer	Class 3 Public Primary Cer	8/1/2028	Client Authenticati	VeriSign Clas	ftd-ra-ca 🔺	•
		COMODO RSA Certificati	COMODO RSA Certificati	1/18/2038	Client Authenticati	Sectigo (forr	More )	,
5	Intermediate Certification Authorities	Copyright (c) 1997 Micros	Copyright (c) 1997 Micros	12/30/1999	Time Stamping	Microsoft Tii		
>	Active Directory User Object	STATEST DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati	www.infraey		
>	Trusted Publishers	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	<all></all>	<none></none>		
>	Untrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root	11/9/2031	Client Authenticati	DigiCert		
>	Third-Party Root Certification Authoriti	🔄 DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati	DigiCert		
>	Trusted People	🔄 DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati	DigiCert Glol		
>	Client Authentication Issuers	DigiCert High Assurance	DigiCert High Assurance	11/9/2031	<all></all>	<none></none>		
>	Smart Card Trusted Roots	🔄 DigiCert High Assurance	DigiCert High Assurance	11/9/2031	Client Authenticati	DigiCert		
> 📮 🤇	Certificates (Local Computer)	DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati	DigiCert Trus		
			DCT D CA YO	2/30/2021	Client Authenticati	DST Root CA		
		📴 ftd-ra-ca-common-name	ftd-ra-ca-common-name	/16/2029	<all></all>	<none></none>		
			olooabign	3/18/2029	Client Authenticati	GlobalSign R		
Zertifiz	zierungsstelle bestätigen							

```
Überprüfung
```

Schritt 1: VPN-Verbindung initiieren

Initiieren Sie im Techniker-VPN-Client die Verbindung zum Cisco Secure Client. Der Benutzername und das Kennwort müssen nicht eingegeben werden, da die VPN-Verbindung erfolgreich hergestellt wurde.

Sisco Secure Client -		$\times$	S Cisco Secure Client   cert-match X S Cisco Secure Client		- 0,	×
AnyConnect VPIE Your clent certificate will be used for authority cert-match	entication Connect		Your clent certificate will be used for authentication Group: ftd-cert-match-upn Connected to cert-match	/PII: ert-match.	Disconnec	t
			OK Cancel 00:00:06			IPv4
<b>\$</b> ①		-de-de- 0/900	¢ ()			-shide- cisco

VPN-Verbindung für Techniker-VPN-Client erfolgreich

Initiieren Sie im Manager-VPN-Client die Verbindung mit dem Cisco Secure Client. Die Verbindung mit dem VPN ist aufgrund eines Fehlers bei der Zertifikatsvalidierung fehlgeschlagen.



Fehler bei der VPN-Verbindung für Manager VPN-Client

#### Schritt 2: VPN-Sitzungen in FTD CLI bestätigen

Führen Sie in der FTD (Lina) CLI den Befehl ausshow vpn-sessiondb detail anyconnect, um die VPN-Sitzungen des Technikers zu bestätigen.

firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32 Assigned IP: 172.16.1.150 Public IP: 192.168.1.11 Protocol : AnyConnect-Parent SSL-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 Bytes Tx : 14718 Bytes Rx : 12919 Pkts Tx : 2 Pkts Rx : 51 Pkts Tx Drop: 0 Pkts Rx Drop: 0 Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn Login Time : 05:42:03 UTC Tue Jul 2 2024 Duration: 0h:00m:11s Inactivity: 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0000000000200006683932b Security Grp: none Tunnel Zone: 0

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1

AnyConnect-Parent: Tunnel ID : 32.1 Public IP : 192.168.1.11 Encryption : none Hashing : none TCP Src Port : 50170 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.17763 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel: Tunnel ID : 32.2 Assigned IP : 172.16.1.150 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 50177 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 12919 Pkts Tx : 1 Pkts Rx : 51 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Fehlerbehebung

Informationen zur VPN-Authentifizierung finden Sie im Debug-Syslog des Lina-Moduls und in der DART-Datei auf dem Windows-Computer.

Dies ist ein Beispiel für Debug-Protokolle in der Lina-Engine während der VPN-Verbindung vom Engineering-Client.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClient Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

Zugehörige Informationen

Konfiguration des FDM On-Box Management Service für FirePOWER 2100 Konfiguration eines Remote Access-VPN auf einem von FDM verwalteten FTD Konfiguration und Überprüfung des Syslog im FirePOWER Geräte-Manager

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.