Konfigurieren von AAA und Zertifikatauthentifizierung für sicheren Client auf FTD über FMC

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Netzwerkdiagramm

Konfigurationen

- Konfiguration in FMC
  - Schritt 1: FTD-Schnittstelle konfigurieren
  - Schritt 2: Cisco Secure Client-Lizenz bestätigen
  - Schritt 3: Richtlinienzuweisung hinzufügen
  - Schritt 4: Konfigurationsdetails für Verbindungsprofil
  - Schritt 5: Adresspool für Verbindungsprofil hinzufügen
  - Schritt 6: Gruppenrichtlinie für Verbindungsprofil hinzufügen
  - Schritt 7. Sicheres Client-Image für Verbindungsprofil konfigurieren
  - Schritt 8: Konfigurationszugriff und Zertifikat für Verbindungsprofil
  - Schritt 9. Zusammenfassung für Verbindungsprofil bestätigen
- In FTD-CLI bestätigen
- Bestätigung in VPN-Client
  - Schritt 1: Clientzertifikat bestätigen
  - Schritt 2: Zertifizierungsstelle bestätigen

Überprüfung

- Schritt 1: VPN-Verbindung initiieren
- Schritt 2: Aktive Sitzungen in FMC bestätigen
- Schritt 3: VPN-Sitzung in FTD CLI bestätigen
- Schritt 4: Kommunikation mit Server bestätigen

Fehlerbehebung

Referenz

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration von Cisco Secure Client über SSL auf FTDs beschrieben, die von FMC mit AAA- und Zertifikatsauthentifizierung verwaltet werden.

Voraussetzungen

Anforderungen

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

- Cisco FirePOWER Management Center (FMC)
- Firewall Threat Defense Virtual (FTD)
- VPN-Authentifizierungsablauf

Verwendete Komponenten

- Cisco FirePOWER Management Center für VMware 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

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

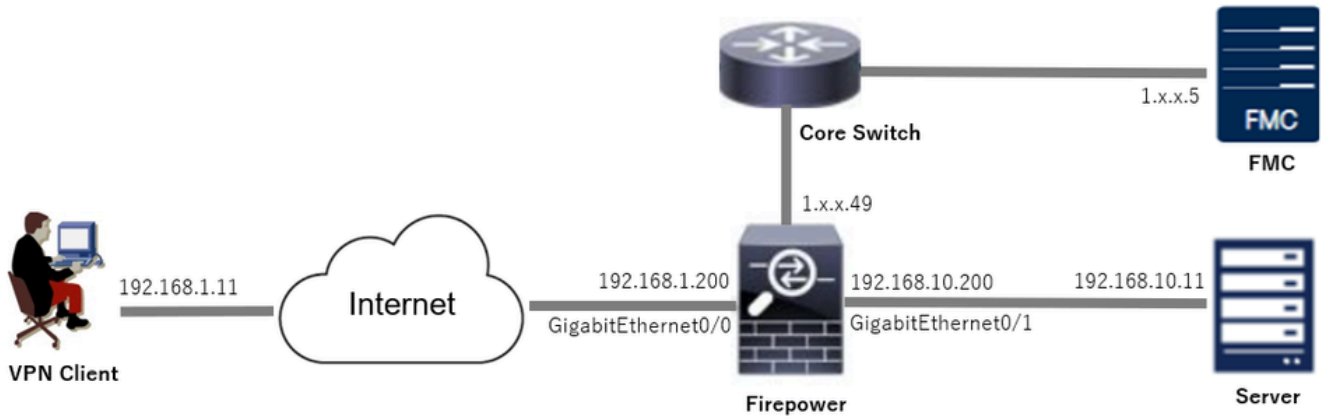
Da Unternehmen strengere Sicherheitsmaßnahmen einführen, ist die Kombination von Zwei-Faktor-Authentifizierung (2FA) mit zertifikatbasierter Authentifizierung zur gängigen Praxis geworden, um die Sicherheit zu verbessern und den Schutz vor nicht autorisiertem Zugriff zu gewährleisten. Eine der Funktionen, die die Benutzererfahrung und die Sicherheit deutlich verbessern können, ist die Möglichkeit, den Benutzernamen im Cisco Secure Client voreinzustellen. Diese Funktion vereinfacht den Anmeldeprozess und erhöht die Gesamteffizienz des Remote-Zugriffs.
In diesem Dokument wird beschrieben, wie Sie einen vordefinierten Benutzernamen in Cisco Secure Client auf FTD integrieren, um sicherzustellen, dass Benutzer schnell und sicher eine Verbindung mit dem Netzwerk herstellen können.

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

- CA: ftd-ra-ca-common-name
- Client-Zertifikat: sslVPNClientCN
- Serverzertifikat: 192.168.1.200

Netzwerkdiagramm

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



Netzwerkdiagramm

Konfigurationen

Konfiguration in FMC

Schritt 1: FTD-Schnittstelle konfigurieren

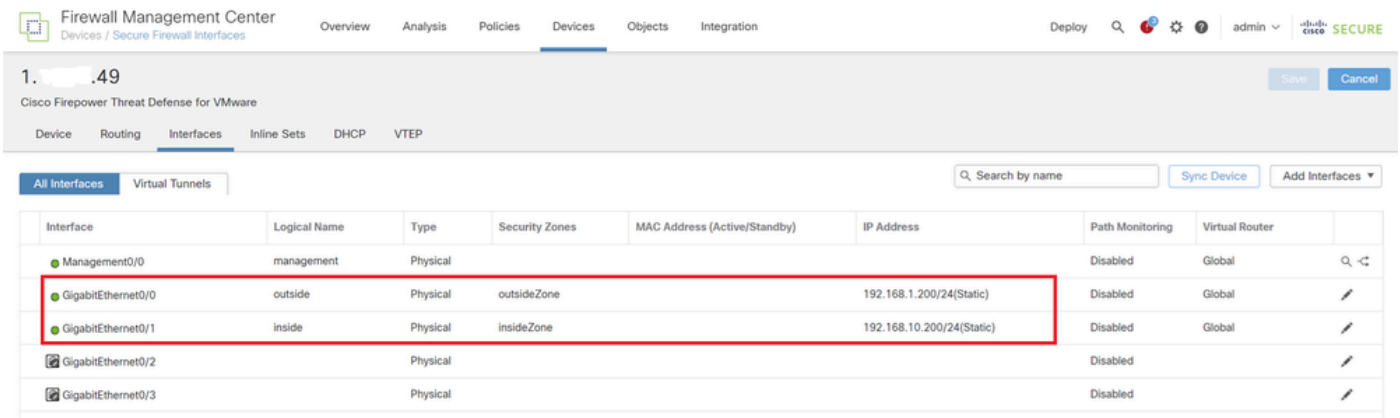
Navigieren Sie zu Devices (Geräte) > Device Management (Geräteverwaltung), bearbeiten Sie das FTD-Zielgerät, und konfigurieren Sie auf der Registerkarte Interfaces (Schnittstellen) die interne und externe FTD-Schnittstelle.

Bei GigabitEthernet0/0

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

Bei GigabitEthernet0/1

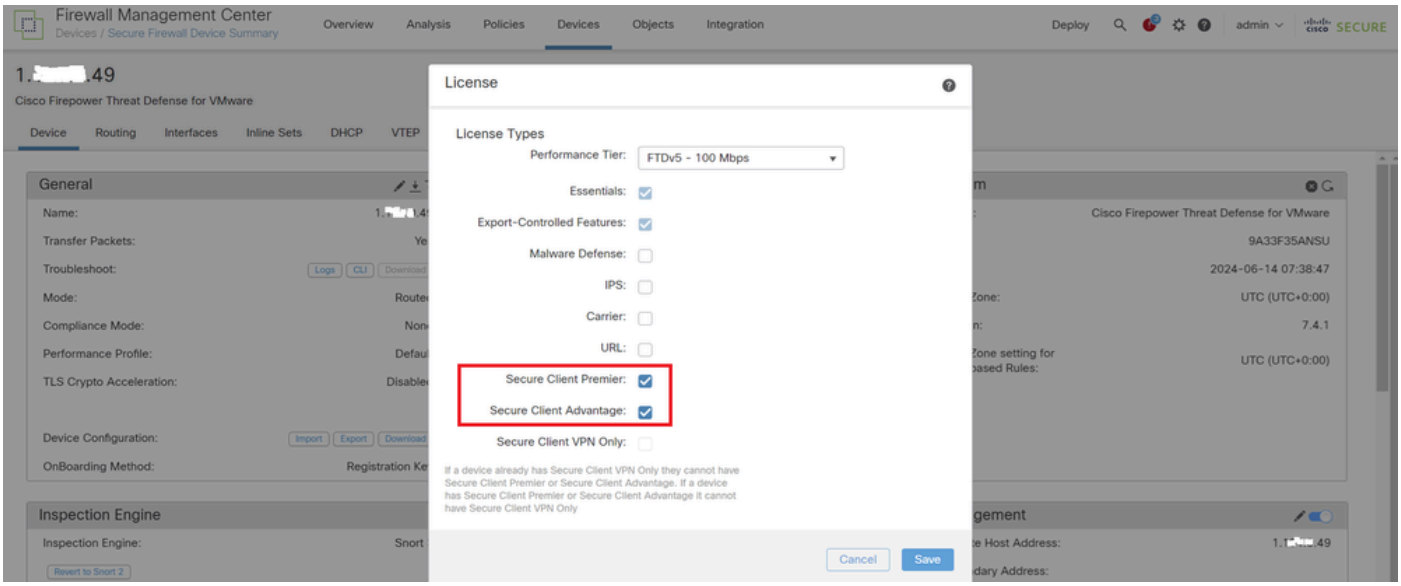
- Name : innen
- Sicherheitszone : insideZone
- IP-Adresse: 192.168.10.200/24



FTD-Schnittstelle

Schritt 2: Cisco Secure Client-Lizenz bestätigen

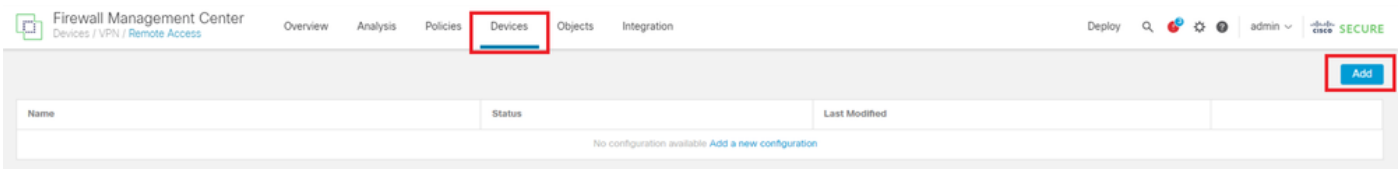
Navigieren Sie zu Devices > Device Management (Geräte > Gerätemanagement), bearbeiten Sie das FTD-Zielgerät, und bestätigen Sie die Cisco Secure Client-Lizenz auf der Registerkarte Device (Gerät).



Secure Client-Lizenz

Schritt 3: Richtlinienzuweisung hinzufügen

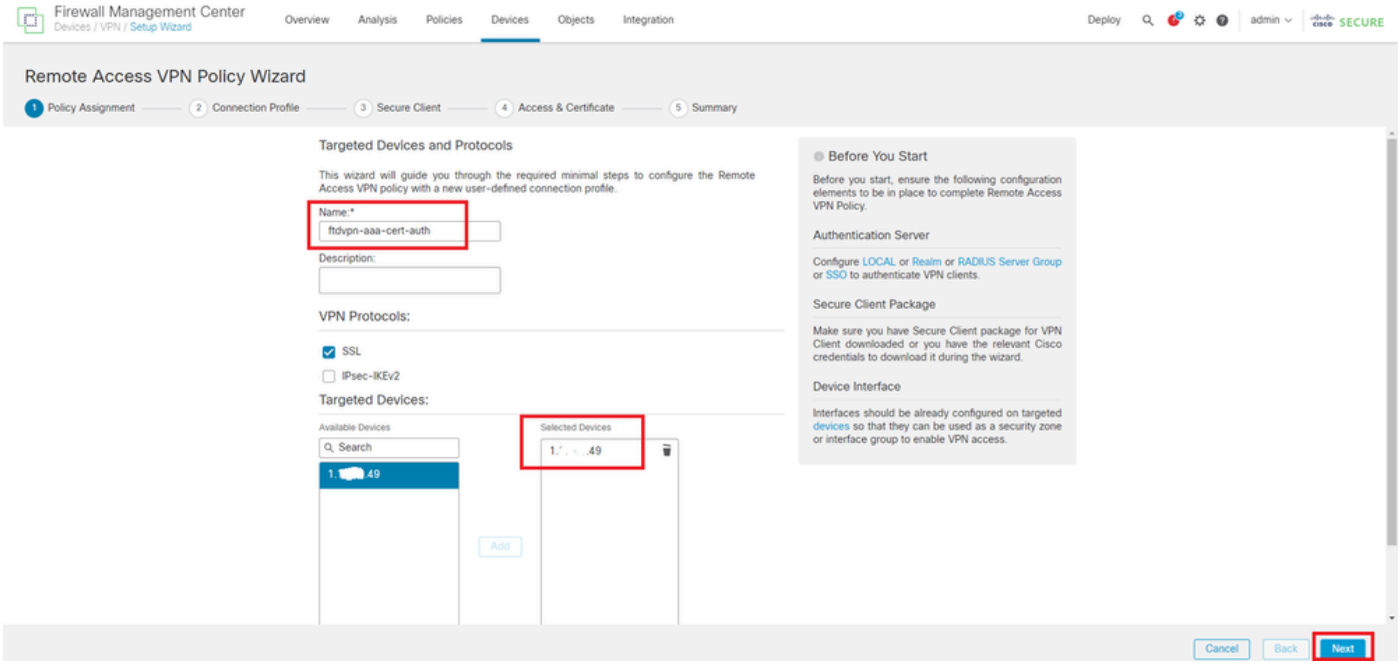
Navigieren Sie zu Devices > VPN > Remote Access, und klicken Sie auf die Schaltfläche Add.



Remote Access-VPN hinzufügen

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

- Name: ftdvpn-aaa-cert-auth
- VPN-Protokolle: SSL
- Zielgeräte: 1.x.x.49

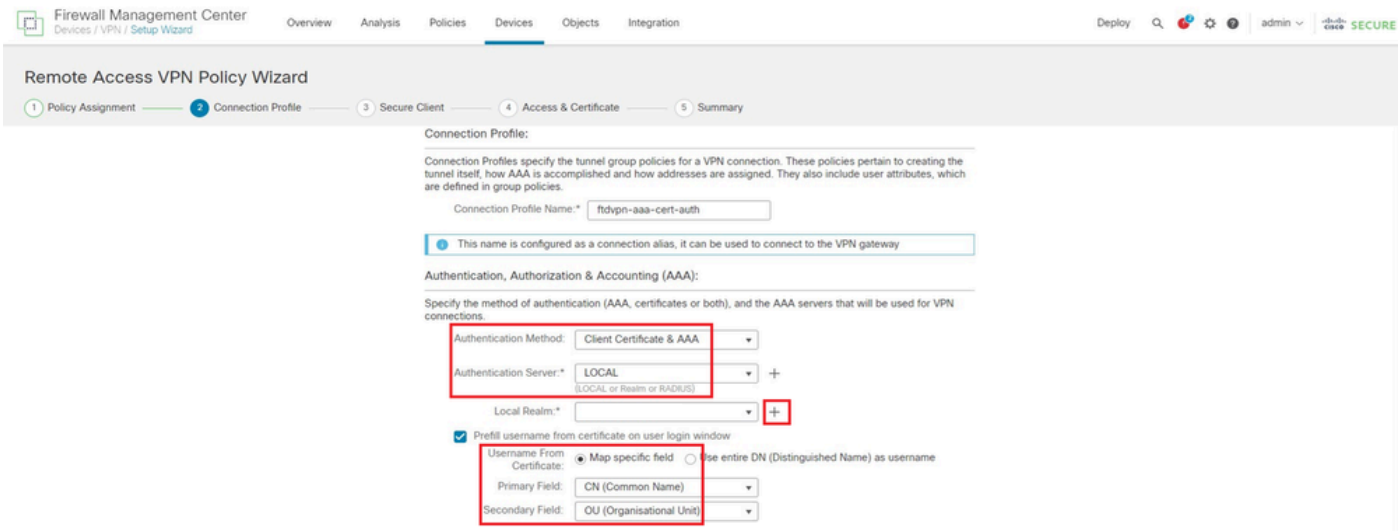


Richtlinienzuweisung

Schritt 4: Konfigurationsdetails für Verbindungsprofil

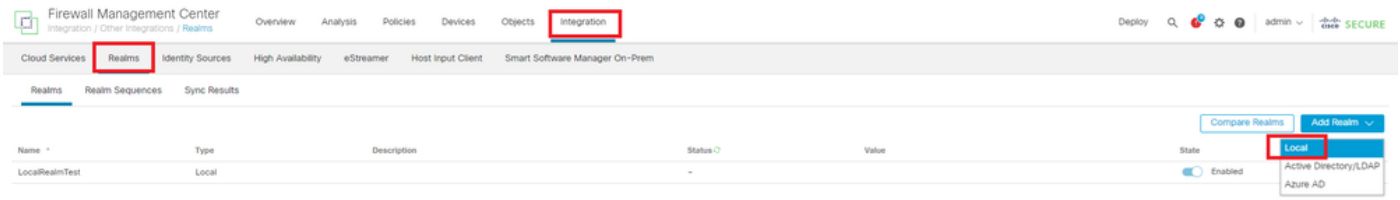
Geben Sie die erforderlichen Informationen für das Verbindungsprofil ein, und klicken Sie neben dem Element Lokaler Bereich auf die Schaltfläche +.

- Authentifizierungsmethode: Client-Zertifikat und AAA
- Authentifizierungsserver: LOKAL
- Benutzername aus Zertifikat: Zuordnungsspezifisches Feld
- Primärfeld: CN (Common Name)
- Sekundäres Feld: OU (Organisationseinheit)



Details zum Verbindungsprofil

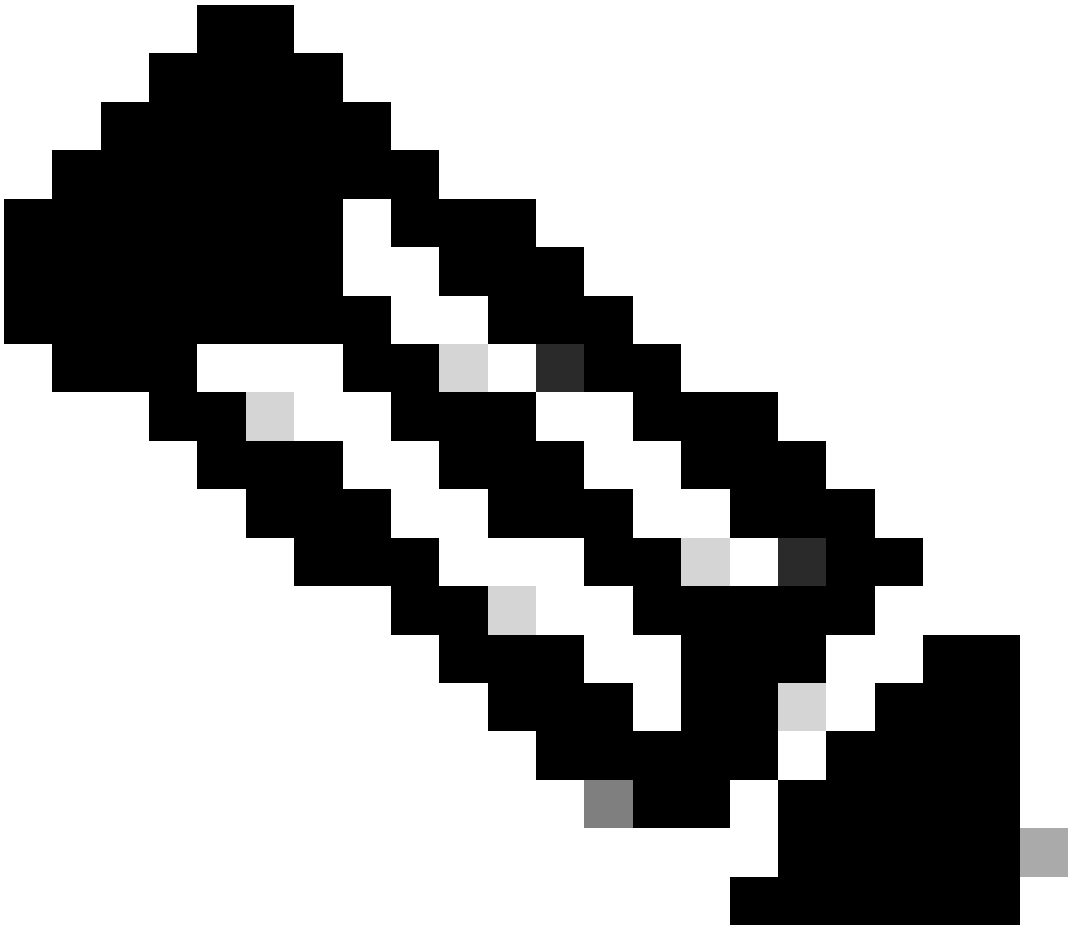
Klicken Sie auf Lokal aus der Dropdown-Liste Bereich hinzufügen, um einen neuen lokalen Bereich hinzuzufügen.



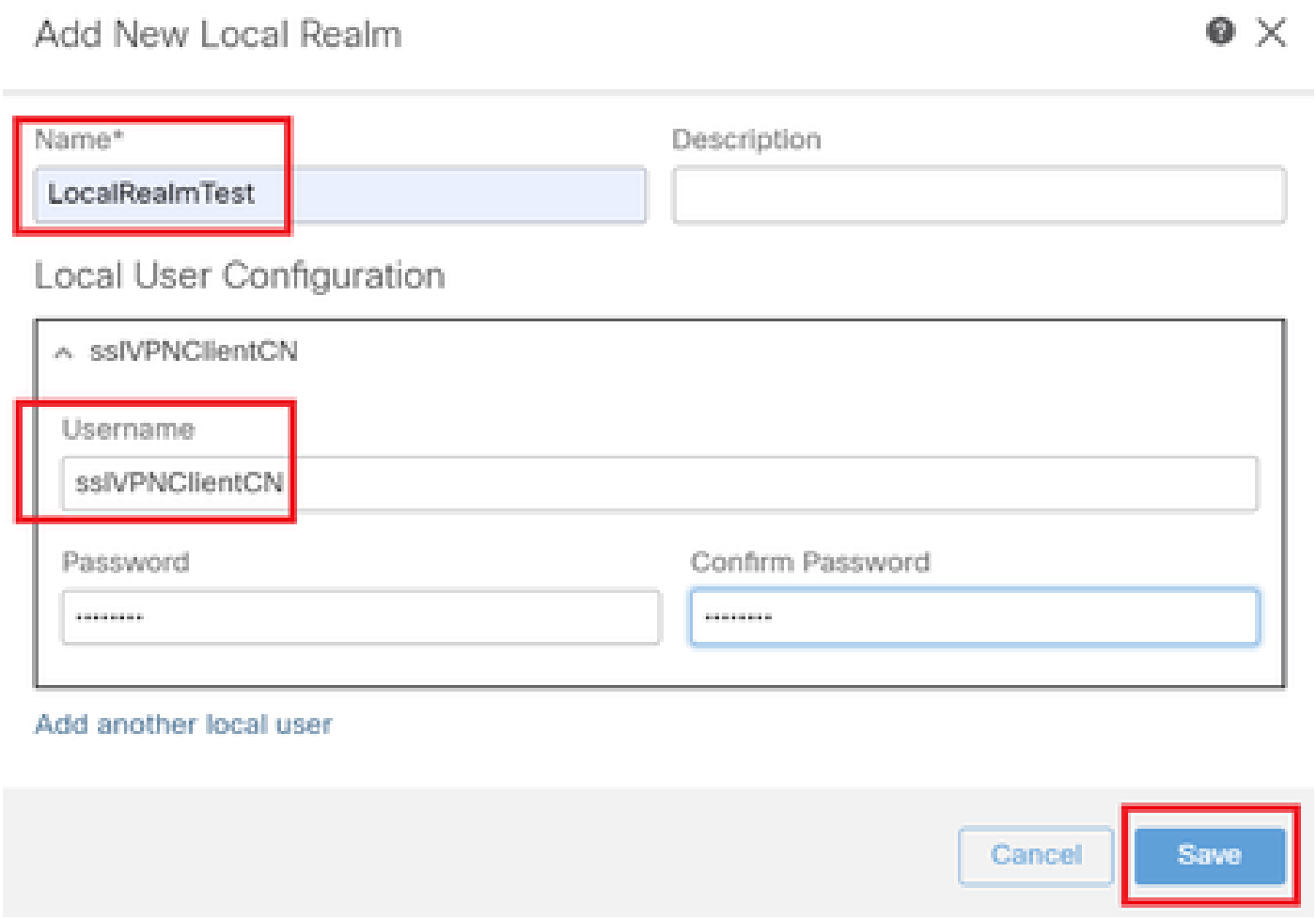
Lokalen Bereich hinzufügen

Geben Sie die erforderlichen Informationen für den lokalen Bereich ein, und klicken Sie auf die Schaltfläche Speichern.

- Name: LocalRealmTest
- Benutzername: sslVPNClientCN



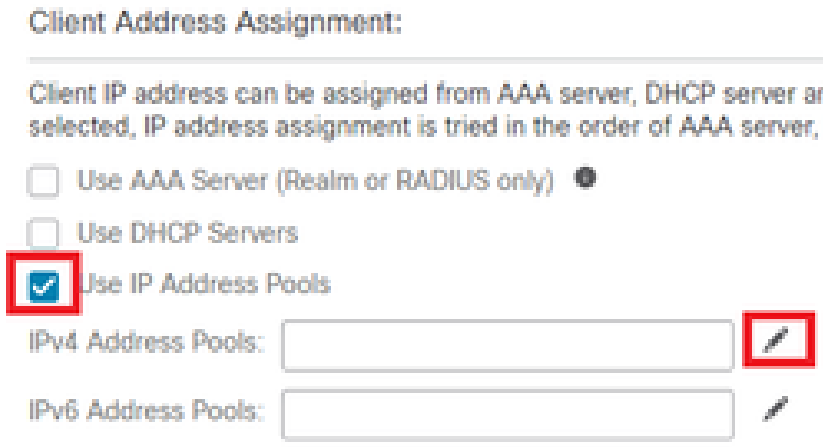
Hinweis: Der Benutzername entspricht dem allgemeinen Namen im Clientzertifikat.



Details zum lokalen Bereich

Schritt 5: Adresspool für Verbindungsprofil hinzufügen

Klicken Sie neben dem Element IPv4-Adresspools auf die Schaltfläche Bearbeiten.

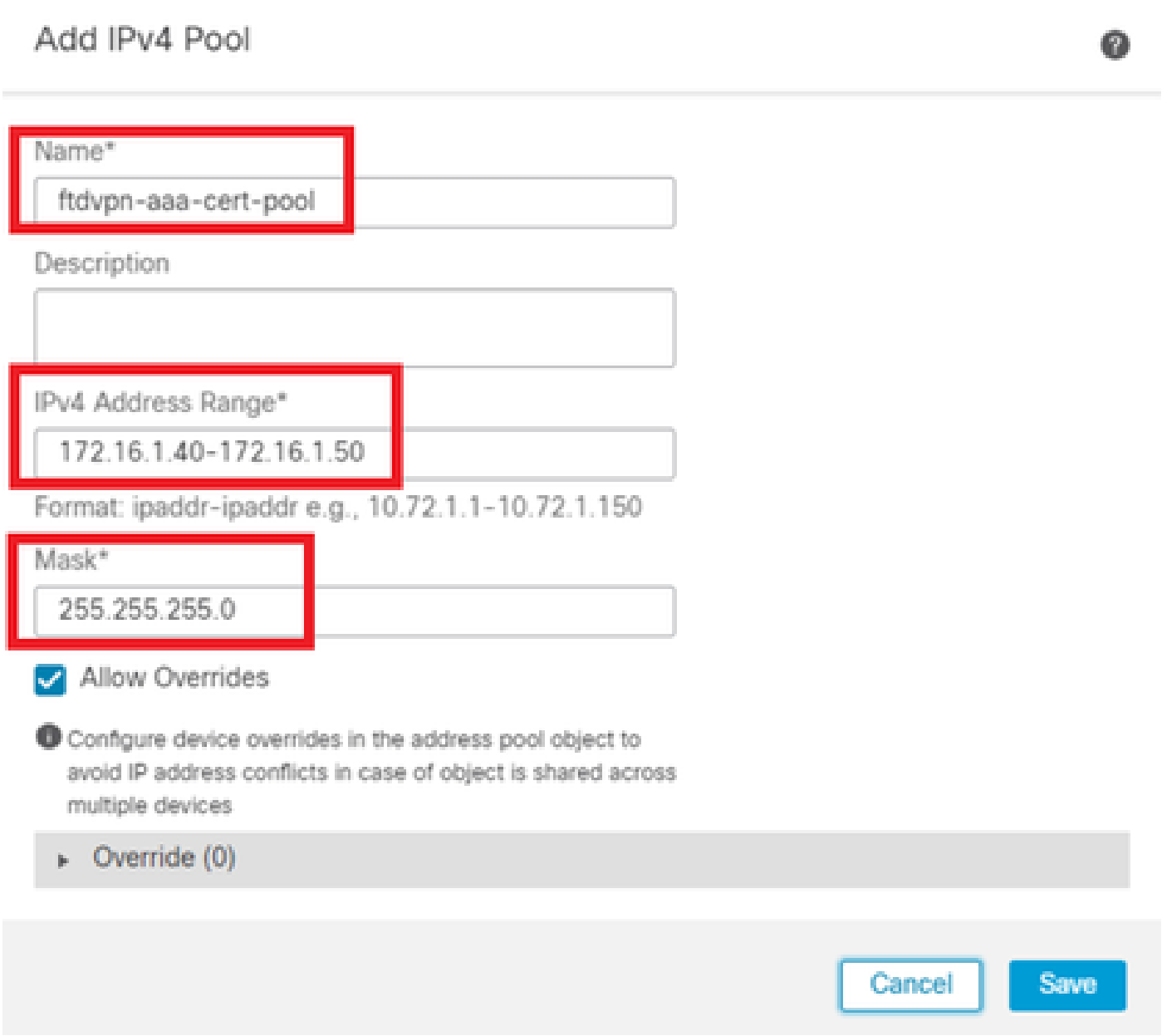


IPv4-Adresspool hinzufügen

Geben Sie die erforderlichen Informationen ein, um einen neuen IPv4-Adresspool hinzuzufügen. Wählen Sie den neuen IPv4-Adresspool für das Verbindungsprofil aus.

- Name: ftdvpn-aaa-cert-pool
- IPv4-Adressbereich: 172.16.1.40-172.16.1.50

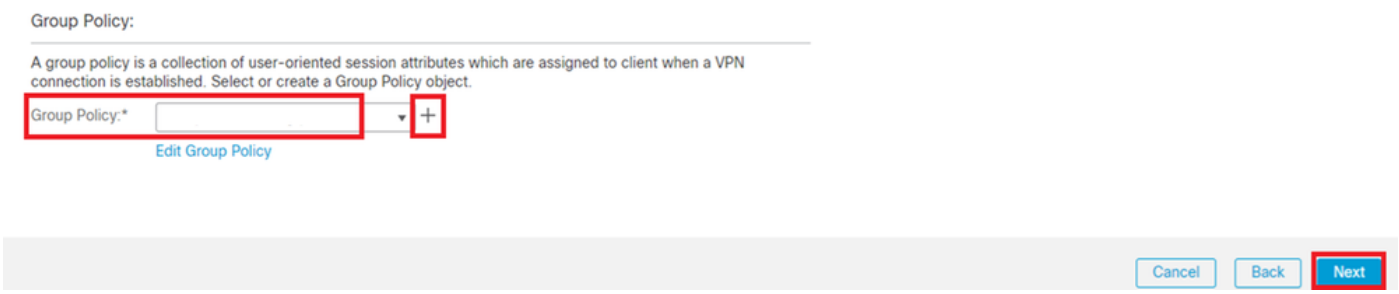
- Maske: 255.255.255.0



Details zum IPv4-Adresspool

Schritt 6: Gruppenrichtlinie für Verbindungsprofil hinzufügen

Klicken Sie neben dem Element Gruppenrichtlinie auf die Schaltfläche+.

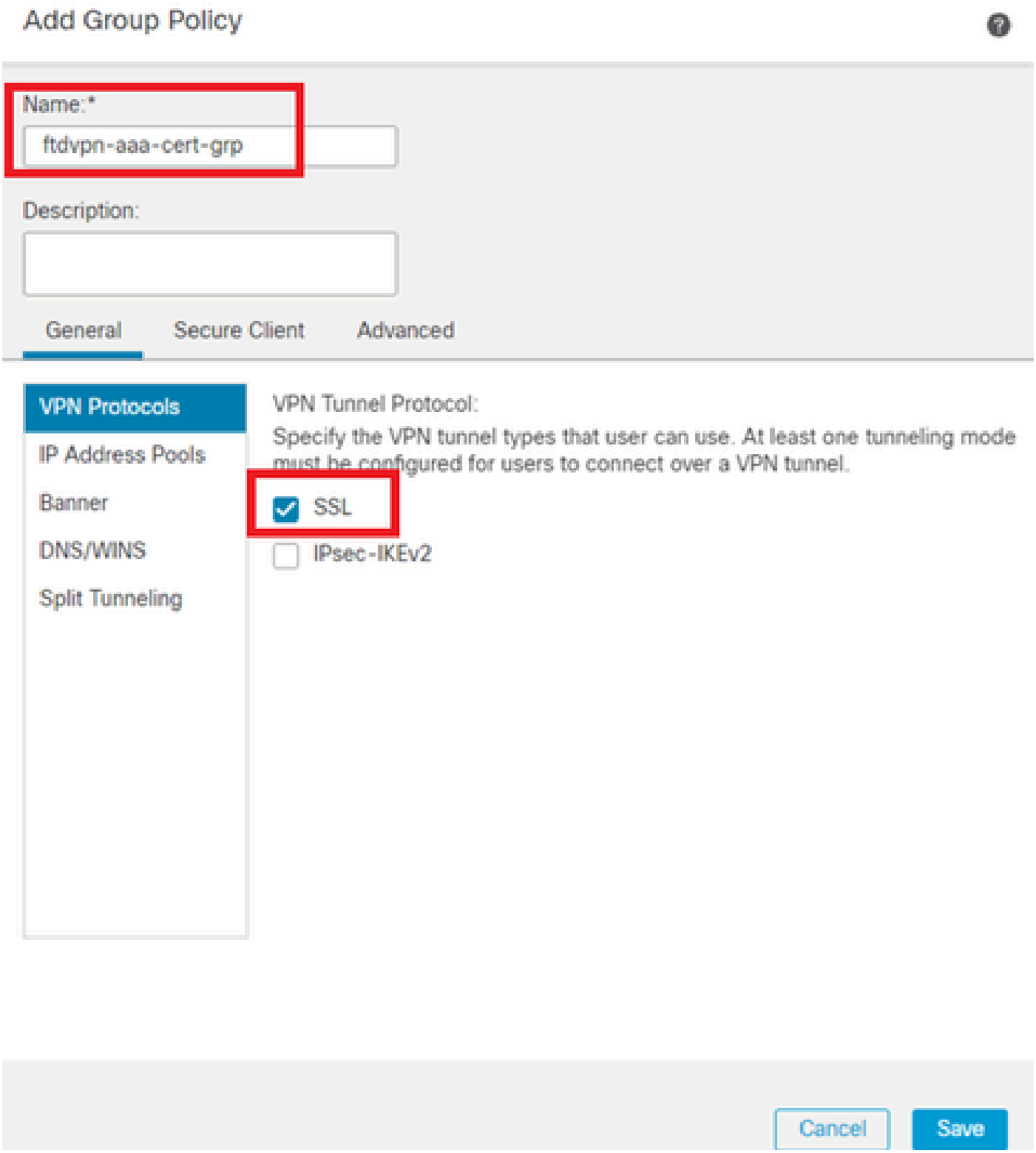


Gruppenrichtlinie hinzufügen

Geben Sie die erforderlichen Informationen zum Hinzufügen einer neuen Gruppenrichtlinie ein.

Wählen Sie die neue Gruppenrichtlinie für das Verbindungsprofil aus.

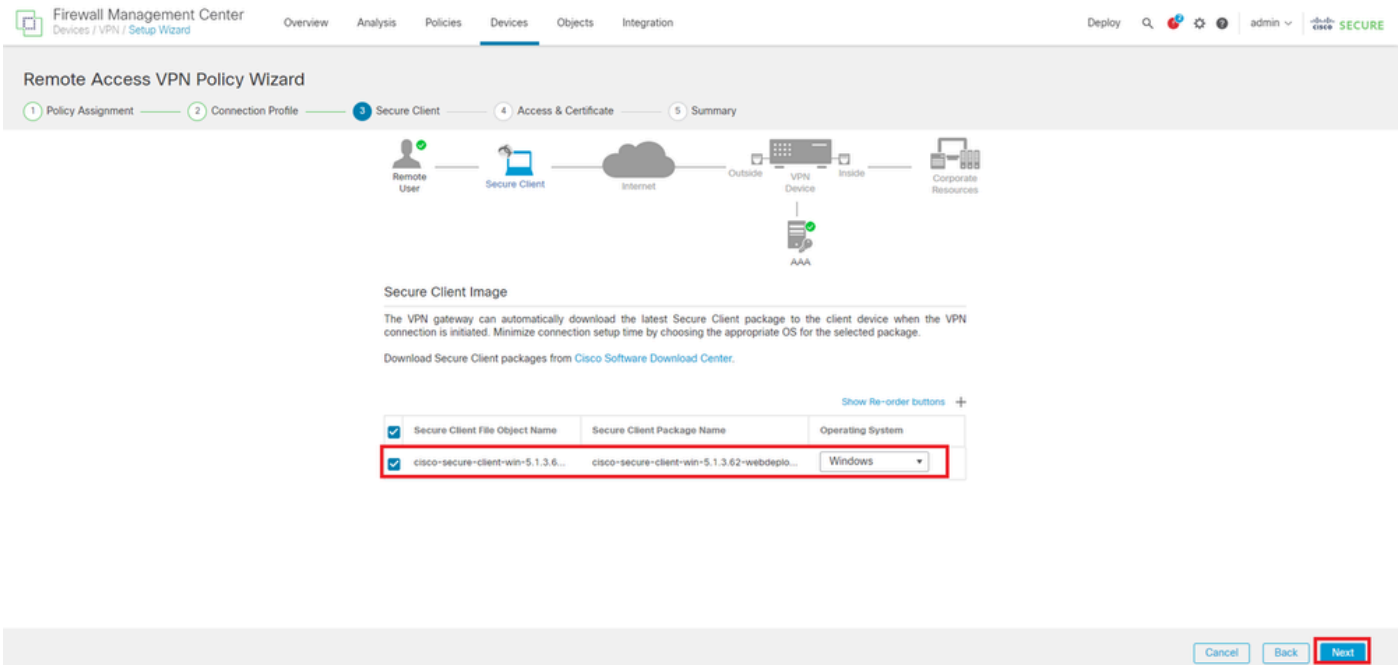
- Name: ftdvpn-aaa-cert-grp
- VPN-Protokolle: SSL



Details zur Gruppenrichtlinie

Schritt 7. Sicheres Client-Image für Verbindungsprofil konfigurieren

Wählen Sie die sichere Client-Image-Datei aus, und klicken Sie auf die Schaltfläche Weiter.

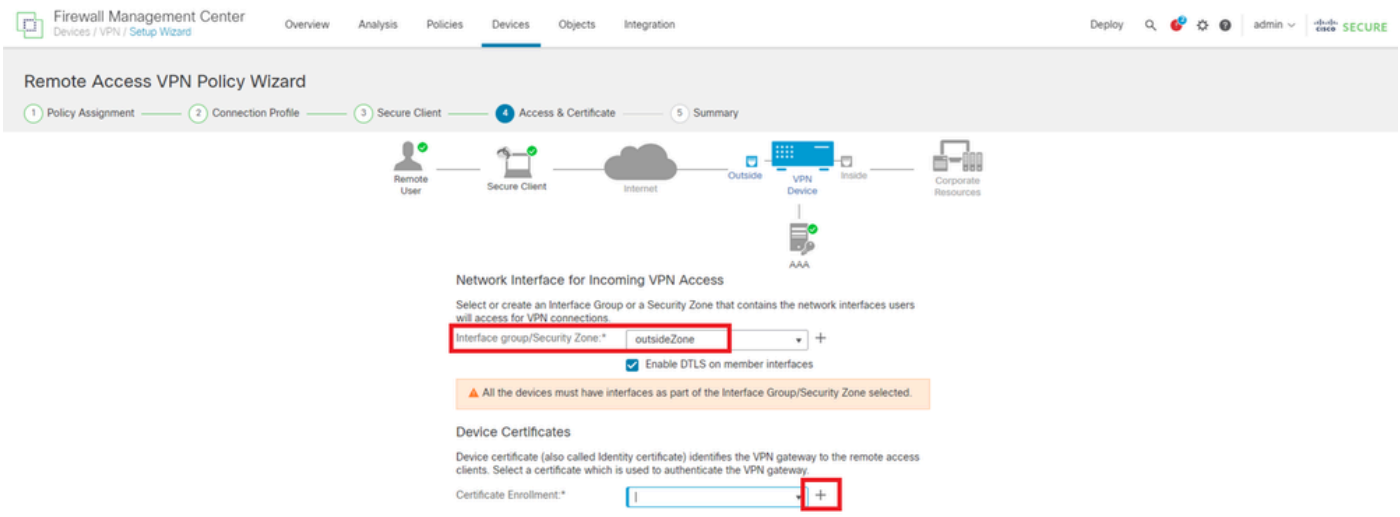


Sicheres Client-Image auswählen

Schritt 8: Konfigurationszugriff und Zertifikat für Verbindungsprofil

Wählen Sie Sicherheitszone für die VPN-Verbindung aus, und klicken Sie neben dem Element Zertifikatregistrierung auf die +-Schaltfläche.

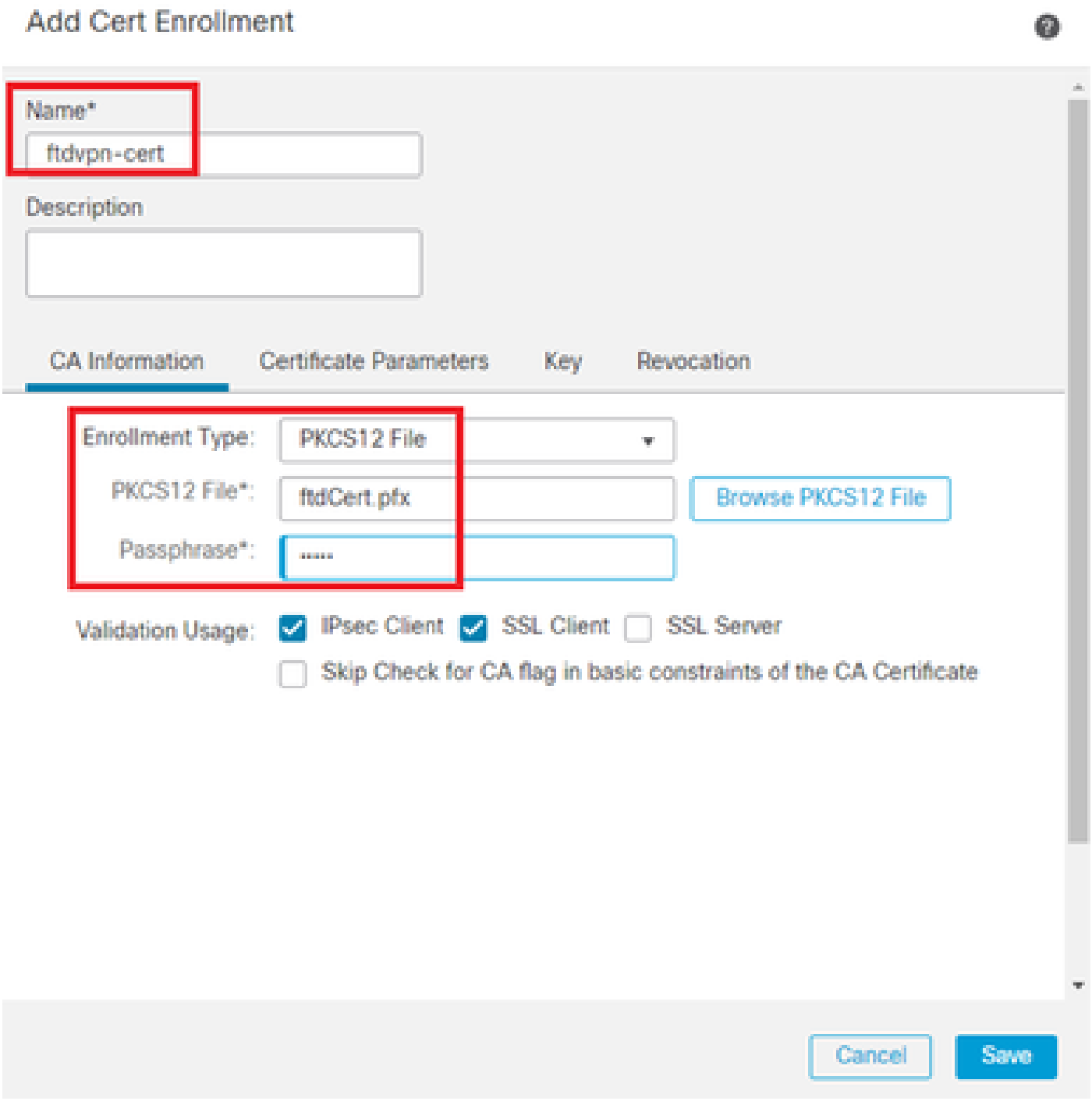
- Schnittstellengruppe/Sicherheitszone : outsideZone



Sicherheitszone auswählen

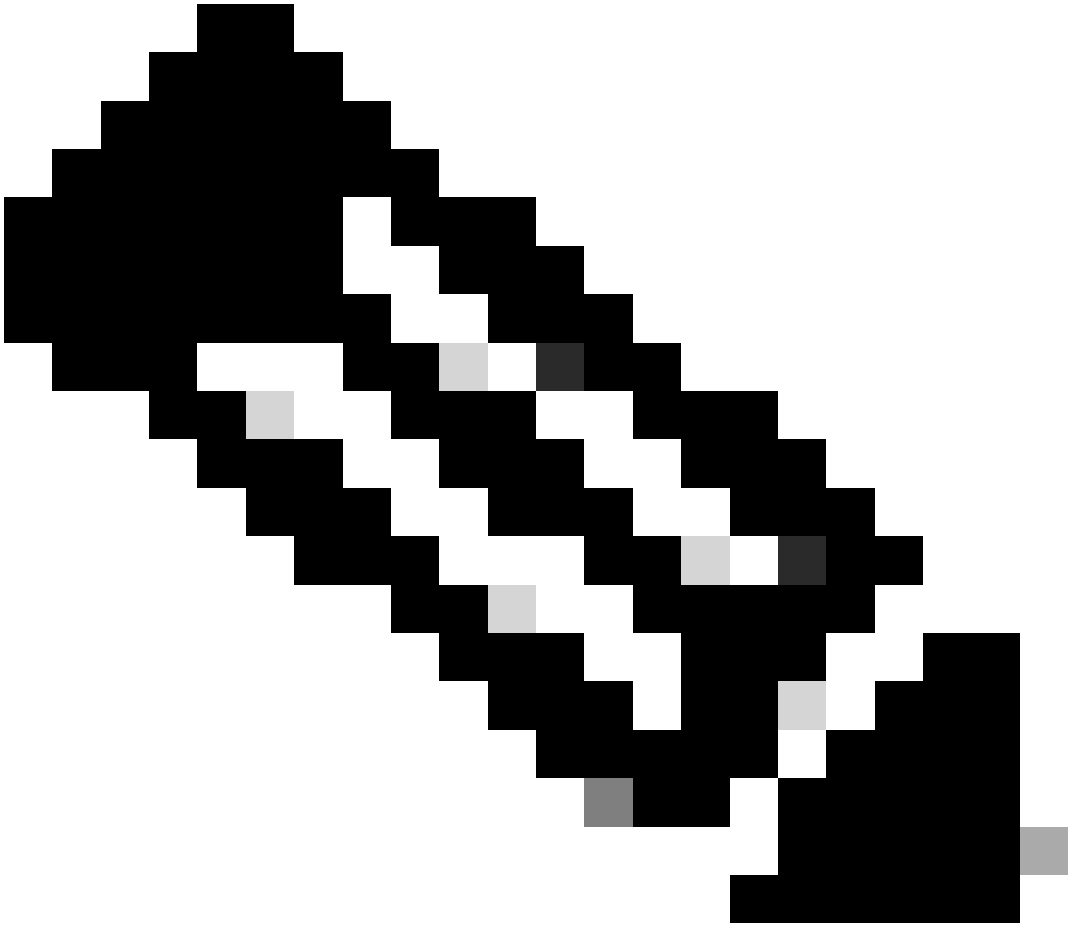
Geben Sie die erforderlichen Informationen für das FTD-Zertifikat ein, und importieren Sie eine PKCS12-Datei vom lokalen Computer.

- Name: ftdvpn-cert
- Registrierungstyp: PKCS12-Datei

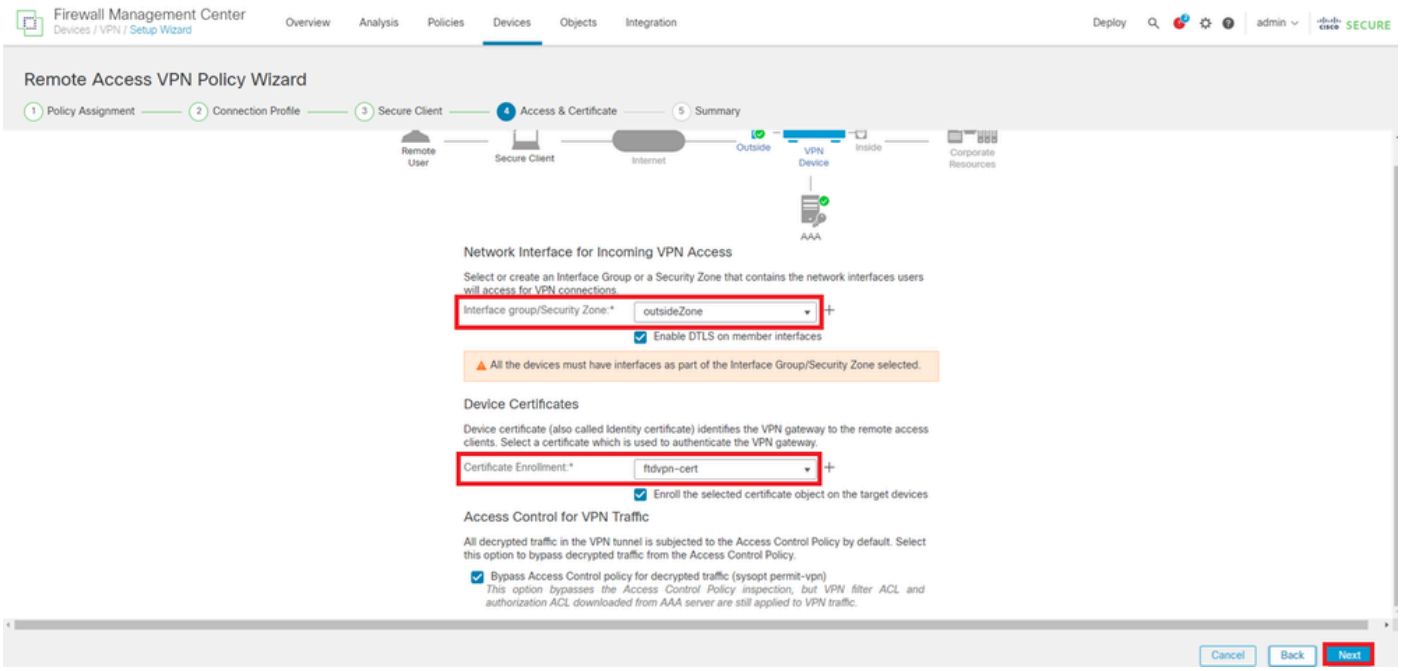


FTD-Zertifikat hinzufügen

Bestätigen Sie die im Zugriffs- und Zertifikat-Assistenten eingegebenen Informationen, und klicken Sie auf die Schaltfläche Weiter.



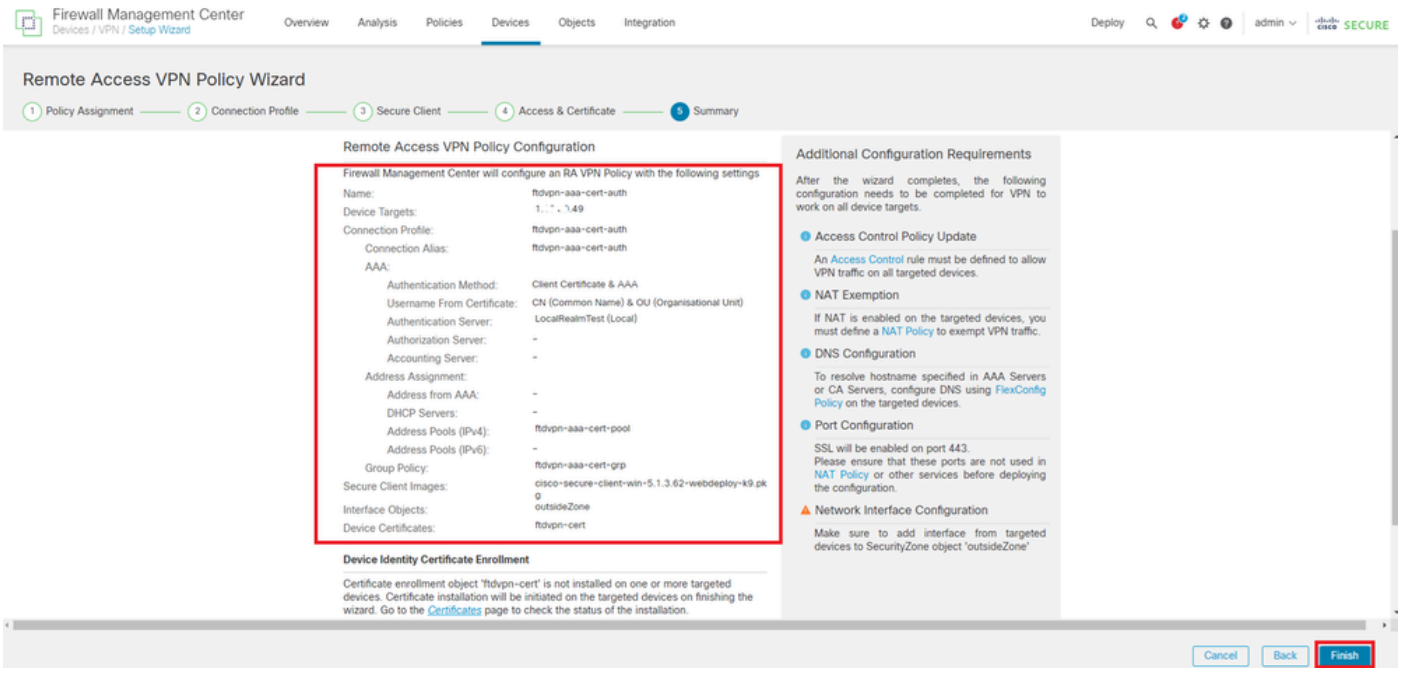
Hinweis: Aktivieren Sie die Richtlinie zur Zugriffskontrolle auf Umgehung für entschlüsselten Datenverkehr (sysopt permit-vpn), damit der entschlüsselte VPN-Datenverkehr nicht der Richtlinienprüfung zur Zugriffskontrolle unterzogen wird.



Einstellungen in Zugriff und Zertifikat bestätigen

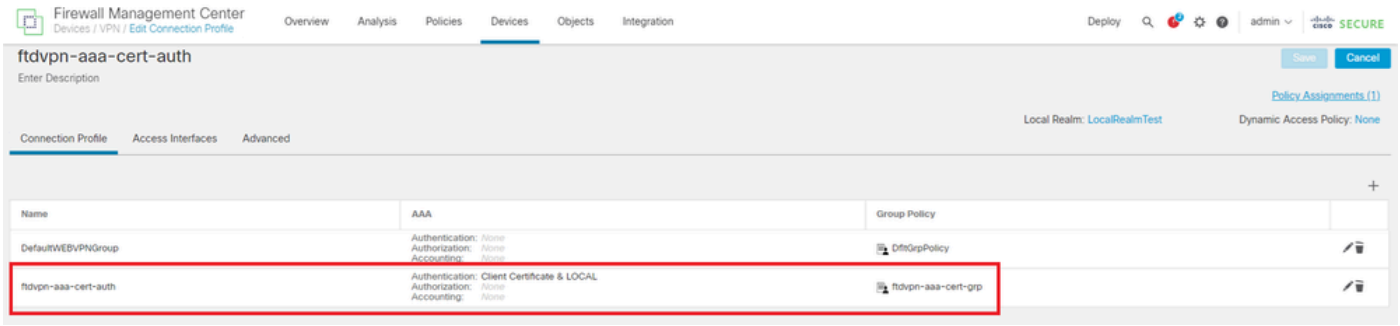
Schritt 9. Zusammenfassung für Verbindungsprofil bestätigen

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



Einstellungen für VPN-Verbindung bestätigen

Bestätigung der Zusammenfassung der VPN-Richtlinie für den Remote-Zugriff und Bereitstellung der Einstellungen für FTD



Zusammenfassung der VPN-Richtlinie für den Remote-Zugriff

In FTD-CLI bestätigen

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

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0

// Defines a local user
username sslVPNClientCN password ***** encrypted

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
crl configure

// Server Certificate Chain
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit
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
```

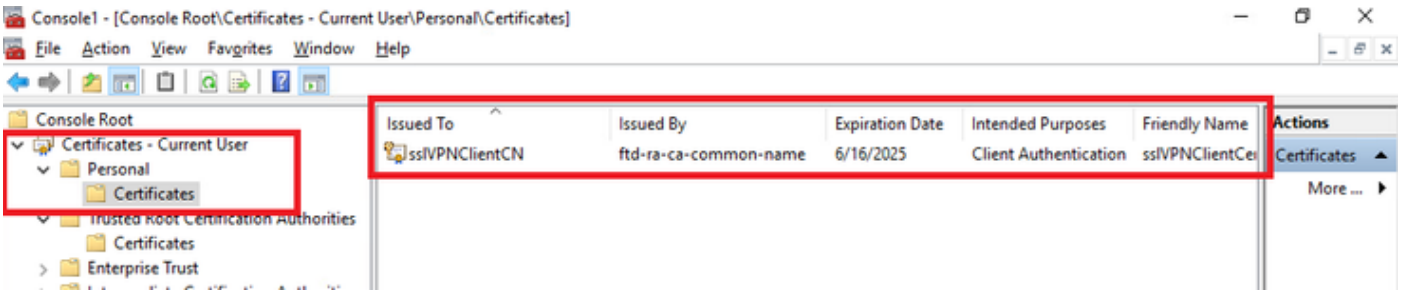
```
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
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-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
```

```
authentication-server-group LOCAL
secondary-authentication-server-group none
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

Bestätigung in VPN-Client

Schritt 1: Clientzertifikat bestätigen

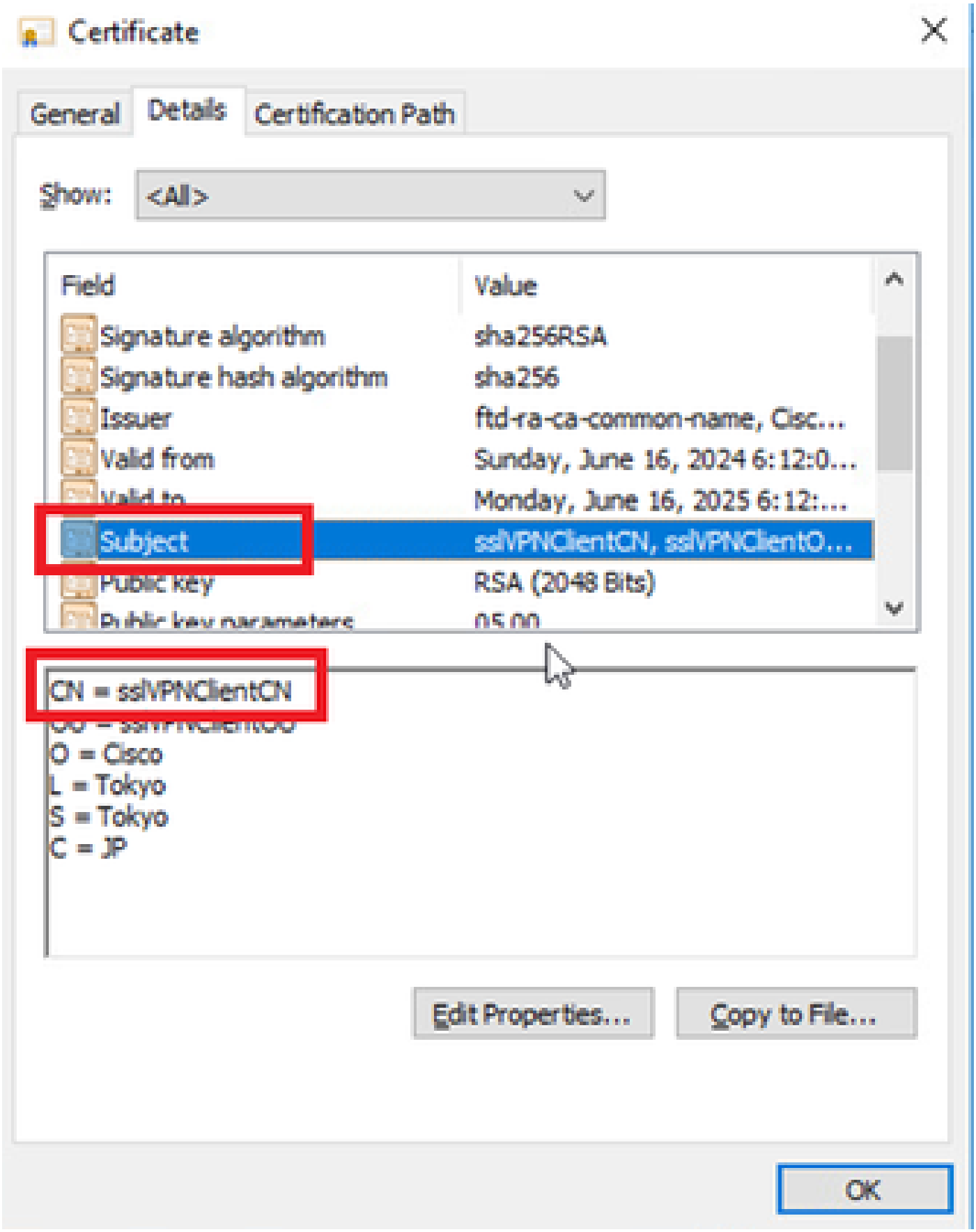
Navigieren Sie zu Zertifikate - Aktueller Benutzer > Persönlich > Zertifikate, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.



Clientzertifikat bestätigen

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

- Betreff: CN = sslVPNClientCN



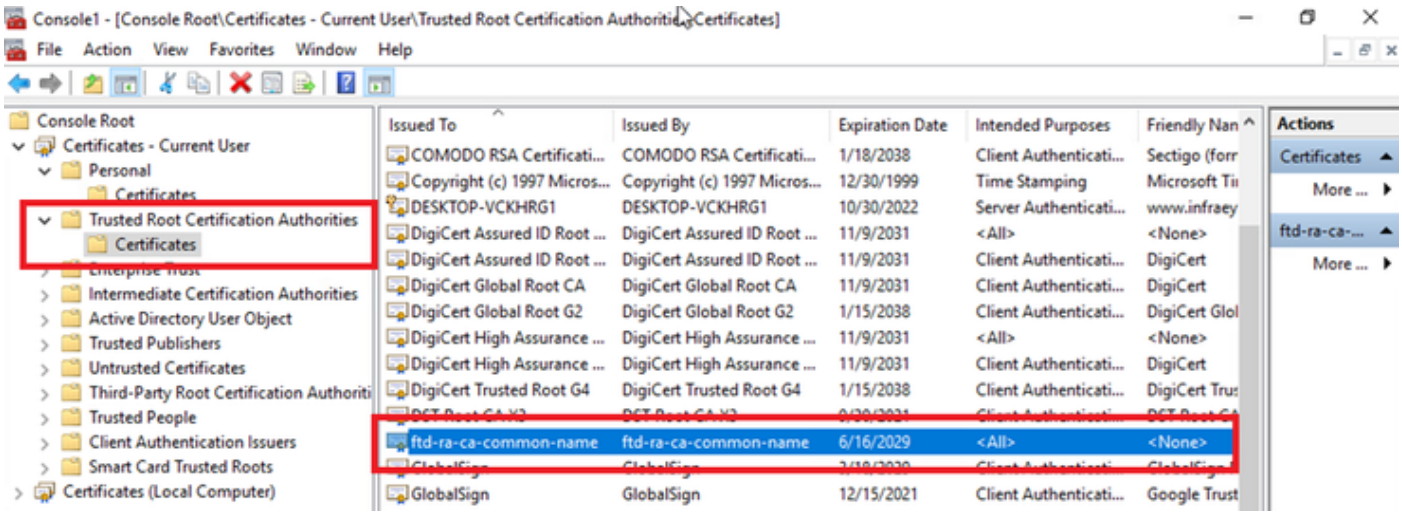
Details zum Clientzertifikat

Schritt 2: Zertifizierungsstelle bestätigen

Navigieren Sie 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



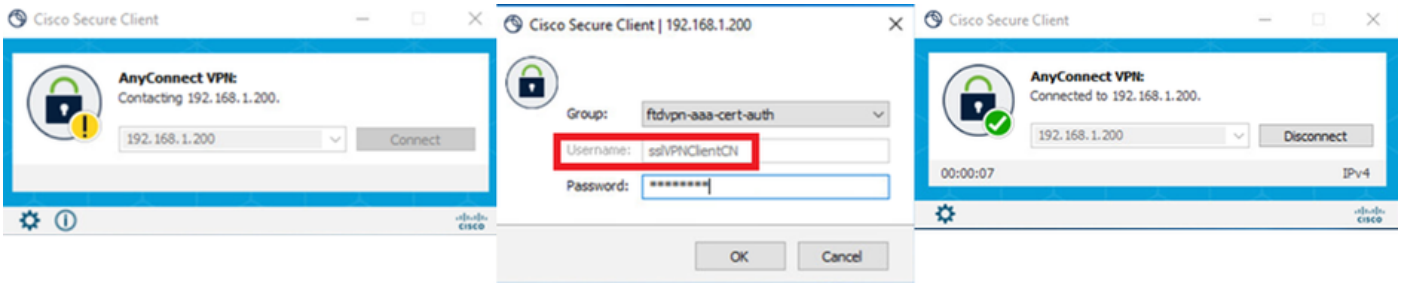
Zertifizierungsstelle bestätigen

Überprüfung

Schritt 1: VPN-Verbindung initiieren

Initiieren Sie auf dem Endgerät die Cisco Secure Client-Verbindung. Der Benutzername wird aus dem Client-Zertifikat extrahiert. Sie müssen das Kennwort für die VPN-Authentifizierung eingeben.

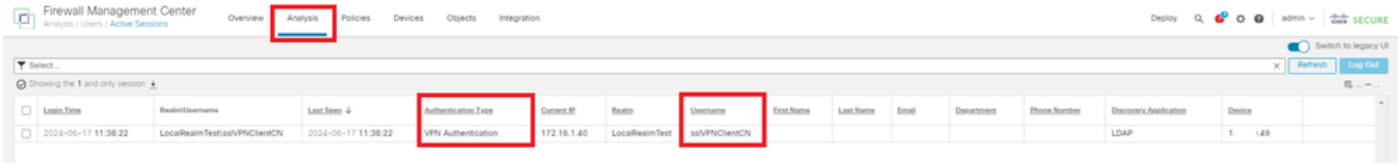
Hinweis: Der Benutzername wird aus dem CN-Feld (Common Name) des Client-Zertifikats in diesem Dokument extrahiert.



VPN-Verbindung initiieren

Schritt 2: Aktive Sitzungen in FMC bestätigen

Navigieren Sie zu Analyse > Benutzer > Aktive Sitzungen, und überprüfen Sie die aktive Sitzung auf VPN-Authentifizierung.



Aktive Sitzung bestätigen

Schritt 3: VPN-Sitzung in FTD CLI bestätigen

Führen Sieshow vpn-sessiondb detail anyconnect den Befehl in der FTD (Lina) CLI aus, um die VPN-Sitzung zu bestätigen.

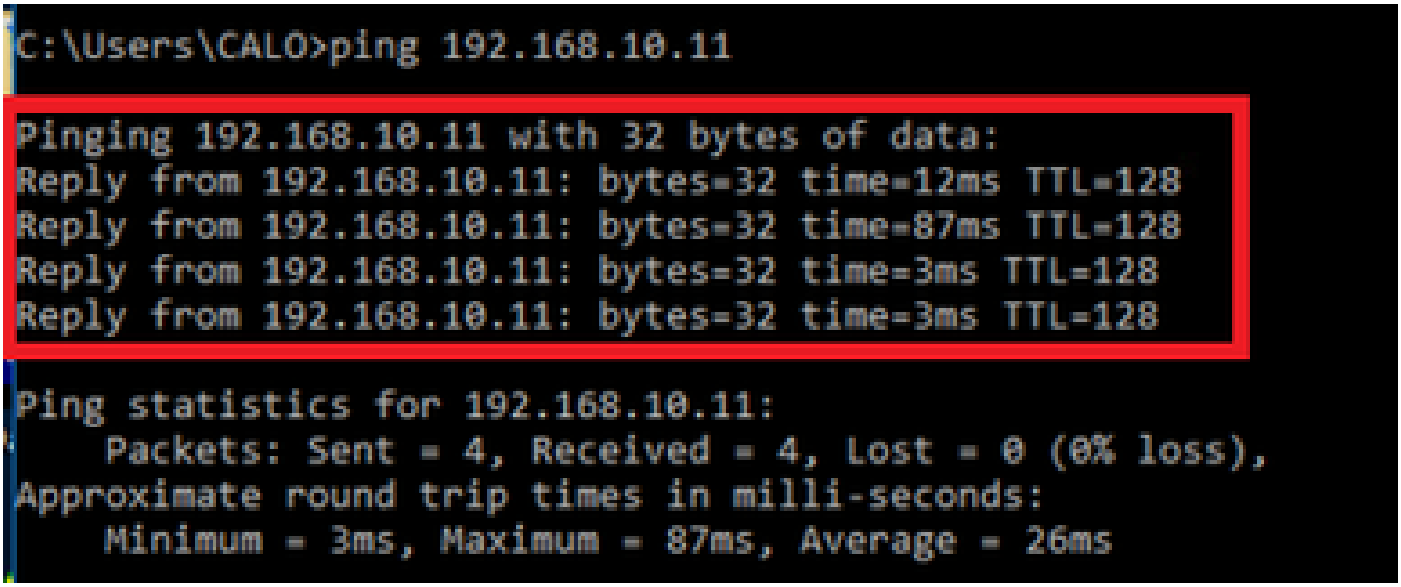
```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
```

Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Schritt 4: Kommunikation mit Server bestätigen

Initiieren Sie ein Ping vom VPN-Client zum Server, und bestätigen Sie, dass die Kommunikation zwischen dem VPN-Client und dem Server erfolgreich ist.



Ping erfolgreich

capture in interface inside real-time Führen Sie den Befehl in der FTD (Lina) CLI aus, um die Paketerfassung zu bestätigen.

ftd702#

```
capture in interface inside real-time


Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

Fehlerbehebung

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

Dies ist ein Beispiel für Debug-Protokolle im Lina-Modul.

```
// Certificate Authentication
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name:  CN=sslVPNClientCl

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested.  [Request 5]
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.  [Request 5]

// AAA Authentication
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

Diese Fehlerbehebungen können über die Diagnose-CLI des FTD durchgeführt werden. Dort finden Sie Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

- debug crypto ca 14
- debug webvpn anyconnect 25
- debug crypto ike-common 255

Referenz

Konfiguration von AnyConnect Remote Access VPN auf FTD

Konfigurieren der zertifikatbasierten AnyConnect-Authentifizierung für den mobilen Zugriff

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.