Konfigurieren der Zertifikatzuordnung für sichere Client-Authentifizierung auf FTD über FMC

Inhalt

Einleitung

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

Voraussetzungen

Anforderungen

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

- Cisco FirePOWER Management Center (FMC)
- Firewall Threat Defense (FTD) - virtuell
- 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

Die Zertifikatszuordnung ist eine Methode, die in VPN-Verbindungen verwendet wird, bei denen ein Clientzertifikat einem lokalen Benutzerkonto zugeordnet wird oder Attribute innerhalb des Zertifikats für Autorisierungszwecke verwendet werden. Hierbei wird ein digitales Zertifikat als Mittel zur Identifizierung eines Benutzers oder Geräts verwendet. Durch die Verwendung der Zertifikatszuordnung wird das SSL-Protokoll zur Authentifizierung von Benutzern verwendet, ohne dass diese Anmeldeinformationen eingeben müssen.

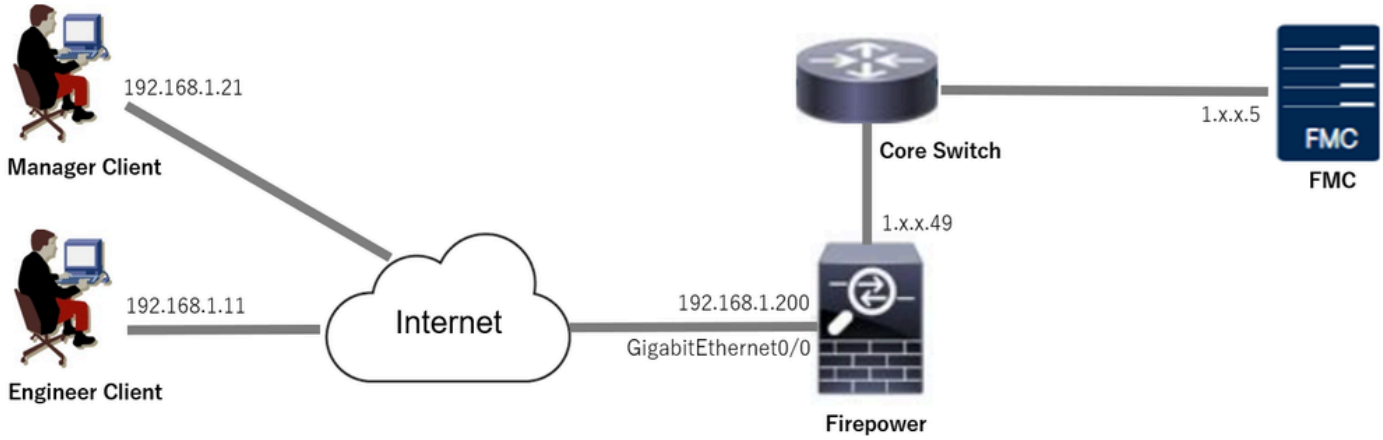
In diesem Dokument wird beschrieben, wie der Cisco Secure Client mithilfe des allgemeinen Namens eines SSL-Zertifikats authentifiziert wird.

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

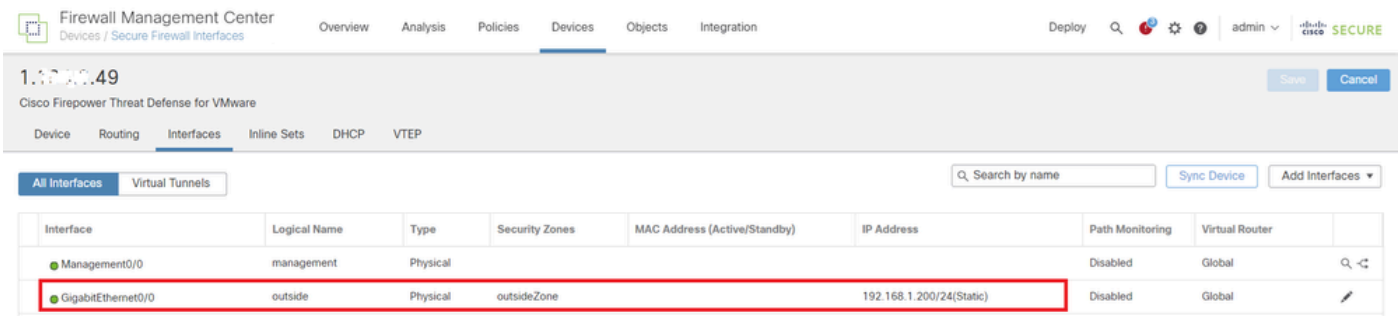
Konfiguration in FMC

Schritt 1: FTD-Schnittstelle konfigurieren

Navigieren Sie zu Devices > Device Management, bearbeiten Sie das FTD-Zielgerät, und konfigurieren Sie die externe Schnittstelle für FTD inInterfacestab.

Bei GigabitEthernet0/0

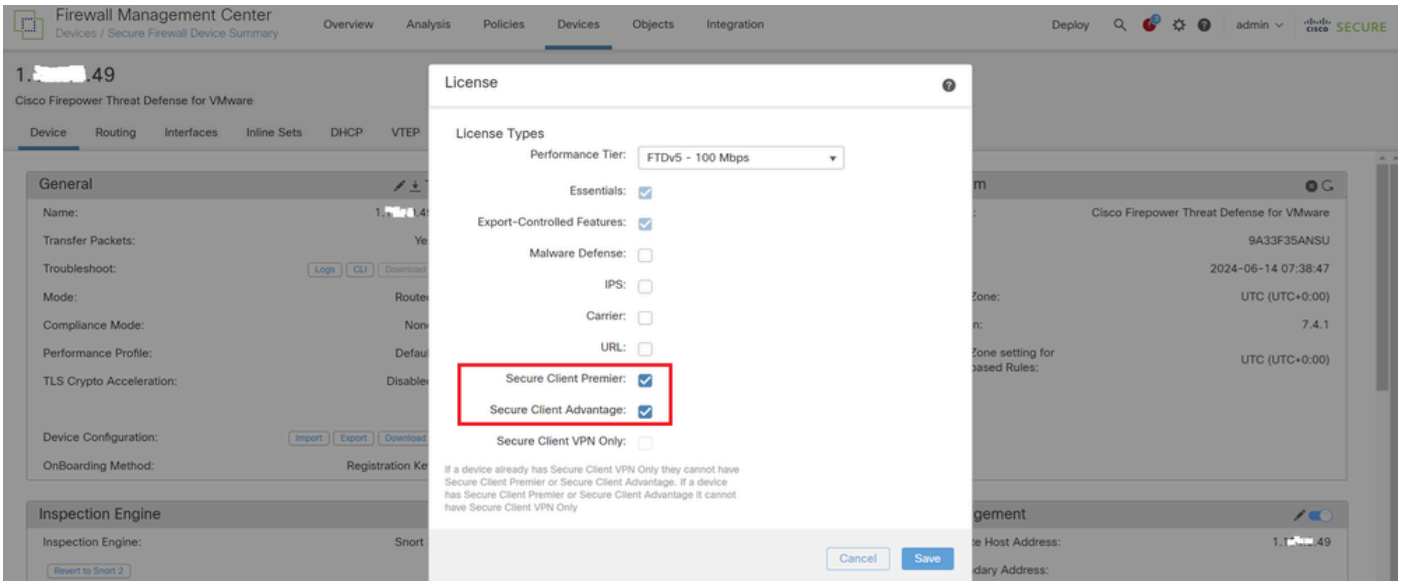
- Name: außen
- Sicherheitszone: outsideZone
- IP-Adresse: 192.168.1.200/24



FTD-Schnittstelle

Schritt 2: Cisco Secure Client-Lizenz bestätigen

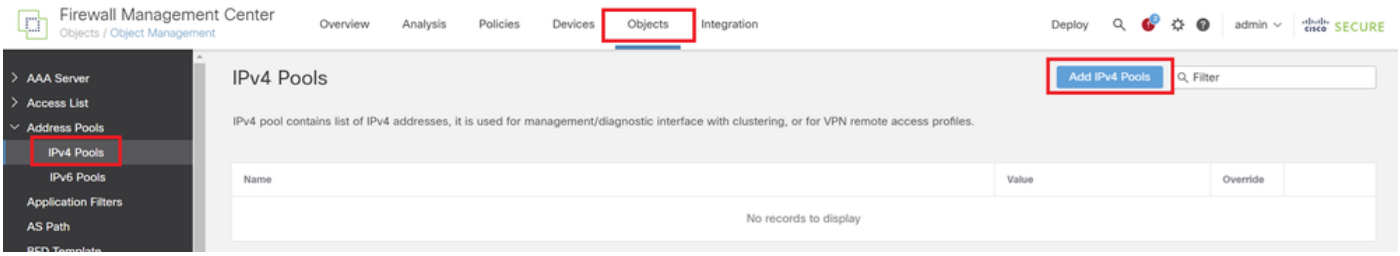
Navigieren Sie zuGeräte > Geräteverwaltung, bearbeiten Sie das FTD-Zielgerät, und bestätigen Sie die Cisco Secure Client-Lizenz auf der Registerkarte Gerät.



Secure Client-Lizenz

Schritt 3: IPv4-Adresspool hinzufügen

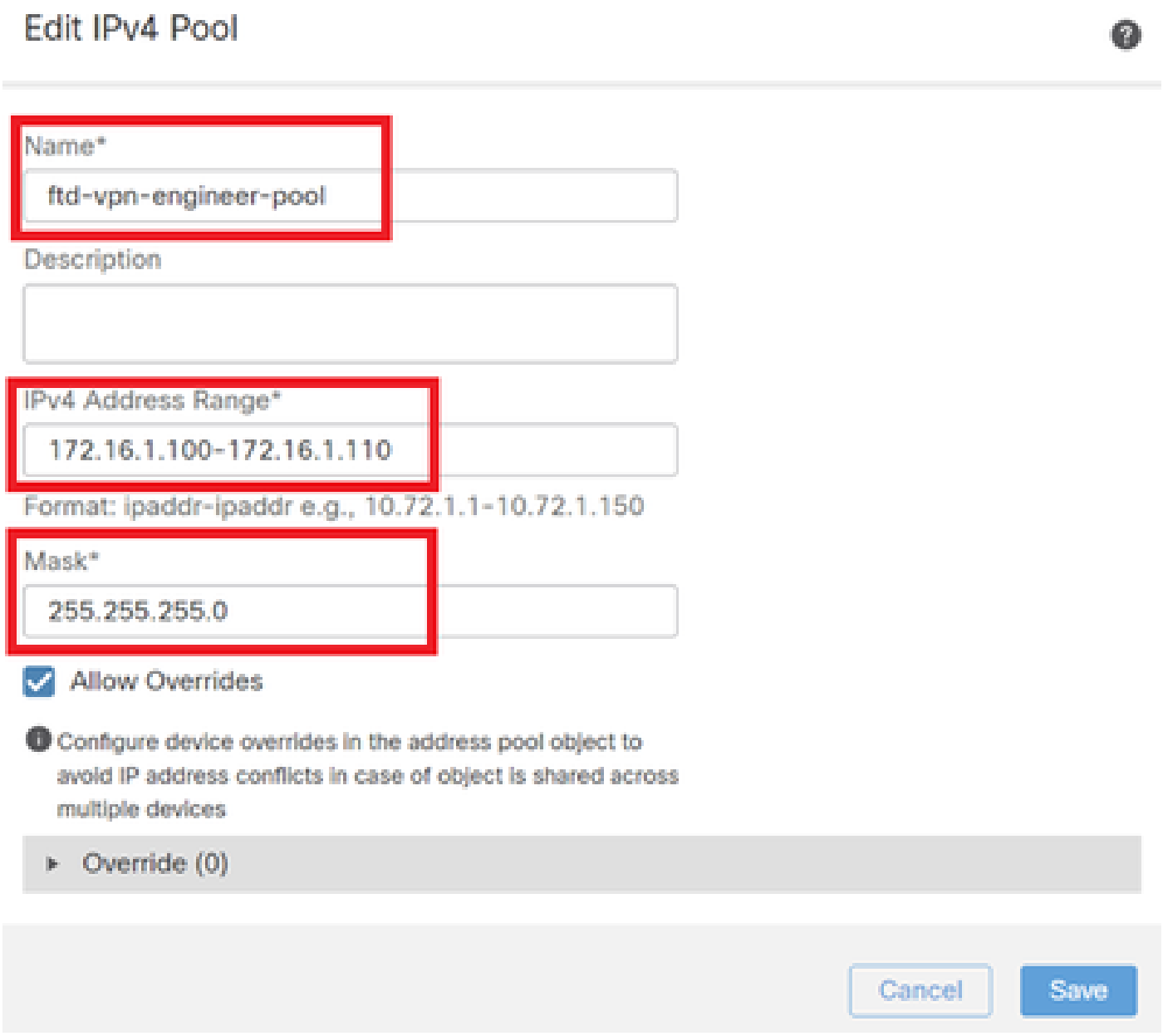
Navigieren Sie zuObject > Object Management > Address Pools > IPv4 Pools, und klicken Sie auf Add IPv4 Pools (IPv4-Pools hinzufügen).



IPv4-Adresspool hinzufügen

Geben Sie die erforderlichen Informationen ein, um einen IPv4-Adresspool für den VPN-Client des Technikers zu erstellen.

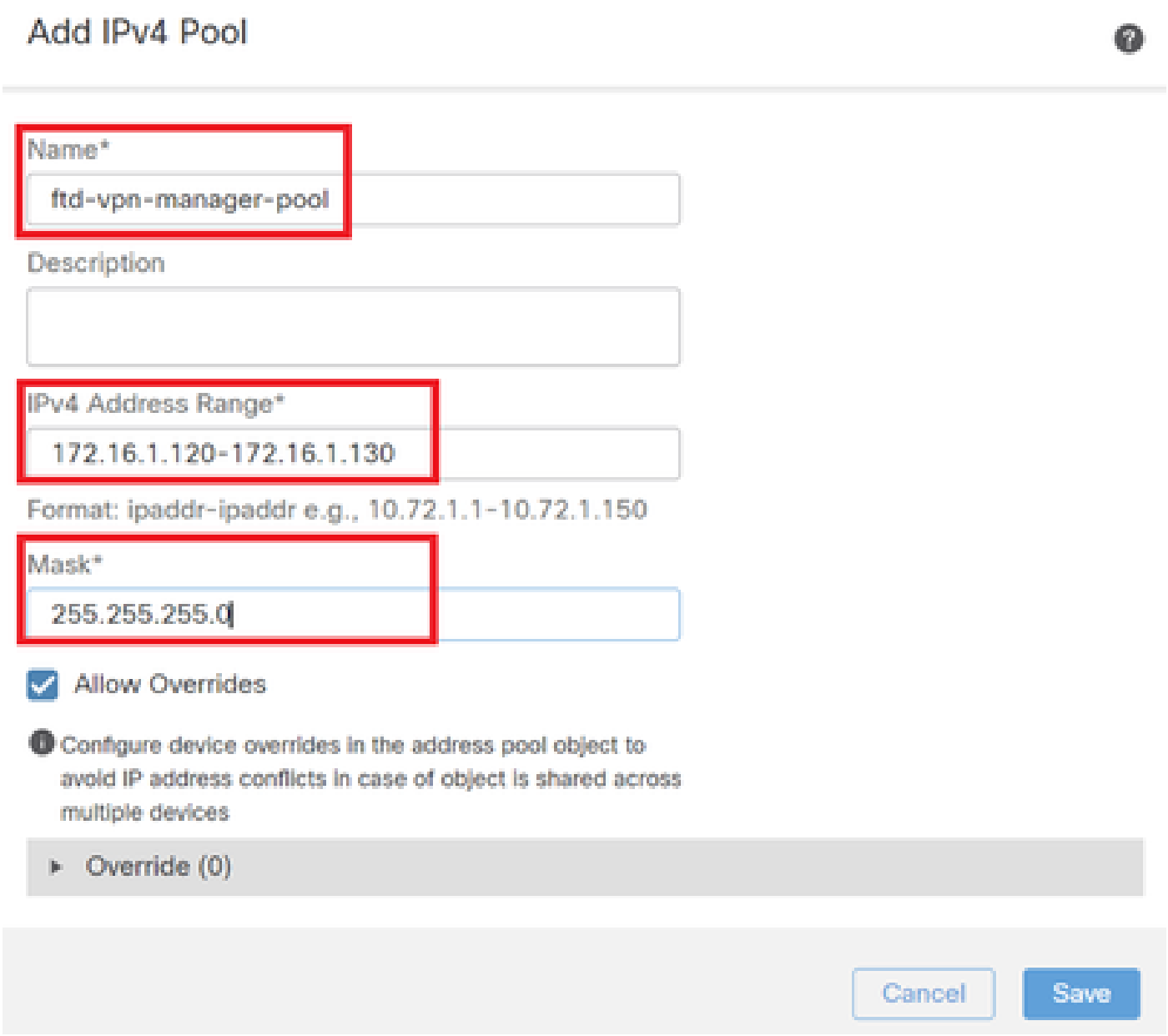
- Name: ftd-vpn-engineer-pool
- IPv4-Adressbereich: 172.16.1.100-172.16.1.110
- Maske: 255.255.255.0



IPv4-Adresspool für Techniker-VPN-Client

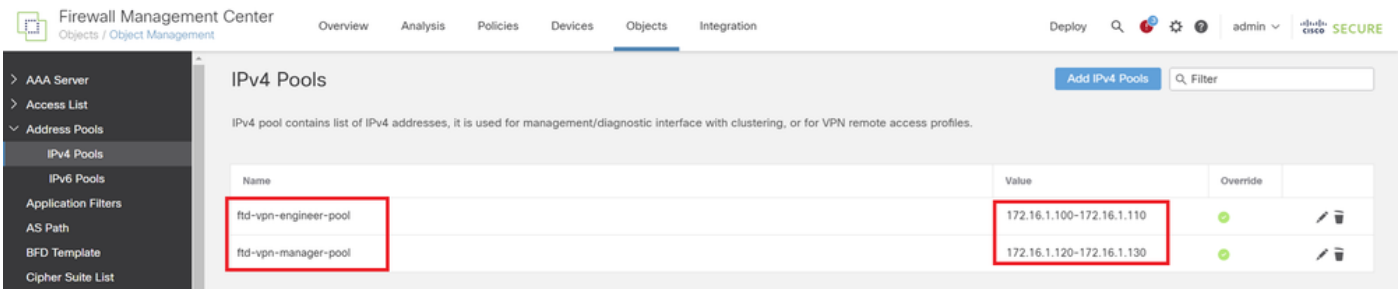
Geben Sie die erforderlichen Informationen ein, um einen IPv4-Adresspool für den Manager-VPN-Client zu erstellen.

- Name: ftd-vpn-manager-pool
- IPv4-Adressbereich: 172.16.1.120-172.16.1.130
- Maske: 255.255.255.0



IPv4-Adresspool für Manager-VPN-Client

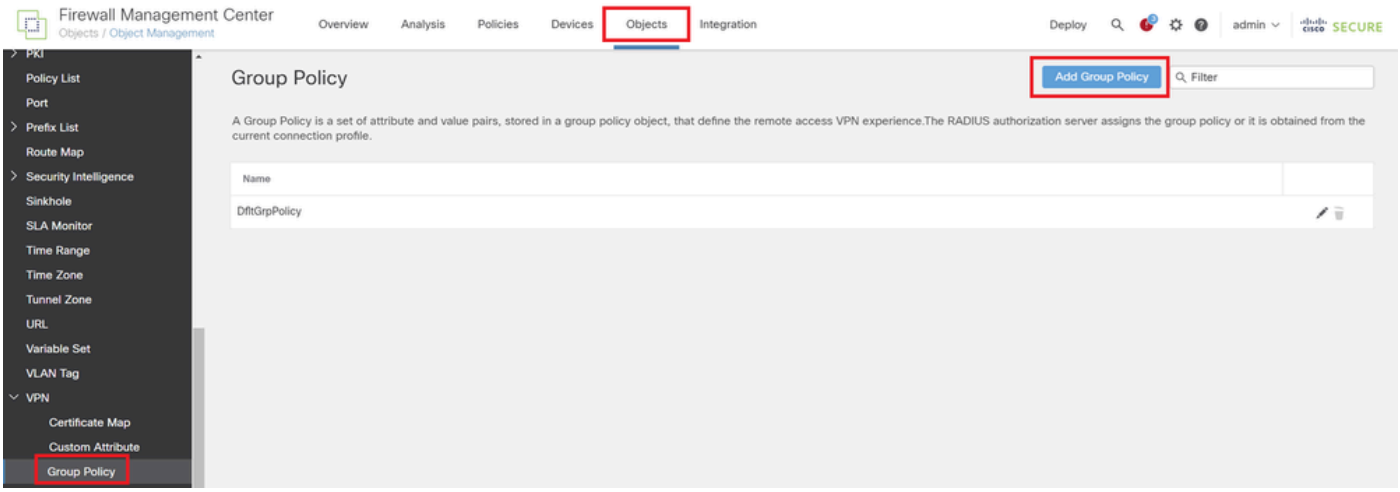
Bestätigen Sie die neuen IPv4-Adresspools.



Neue IPv4-Adresspools

Schritt 4: Gruppenrichtlinie hinzufügen

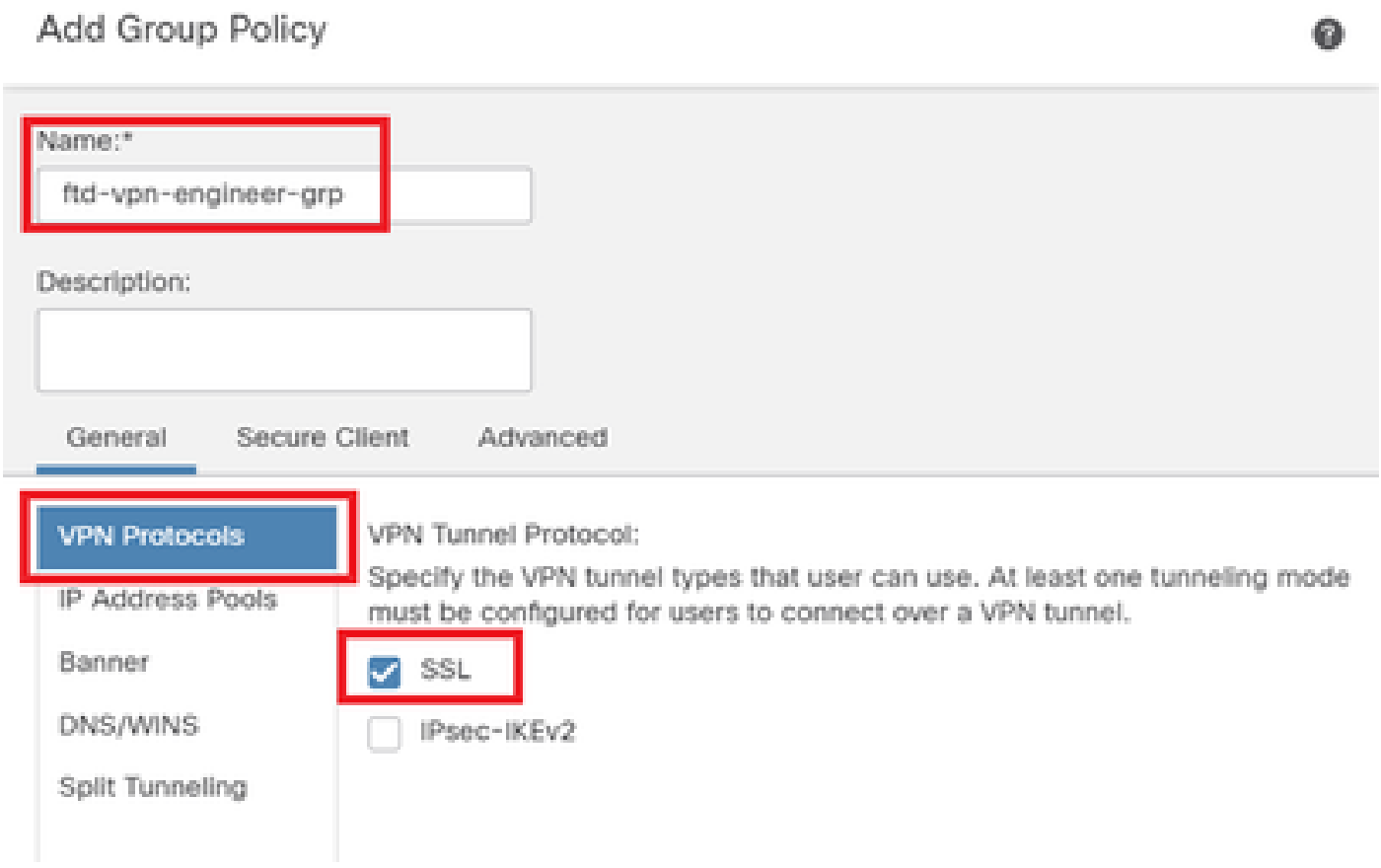
Navigieren Sie zuObject > Object Management > VPN > Group Policy, und klicken Sie auf Add Group Policy (Gruppenrichtlinie hinzufügen).



Gruppenrichtlinie hinzufügen

Geben Sie die erforderlichen Informationen ein, um eine Gruppenrichtlinie für den Techniker-VPN-Client zu erstellen.

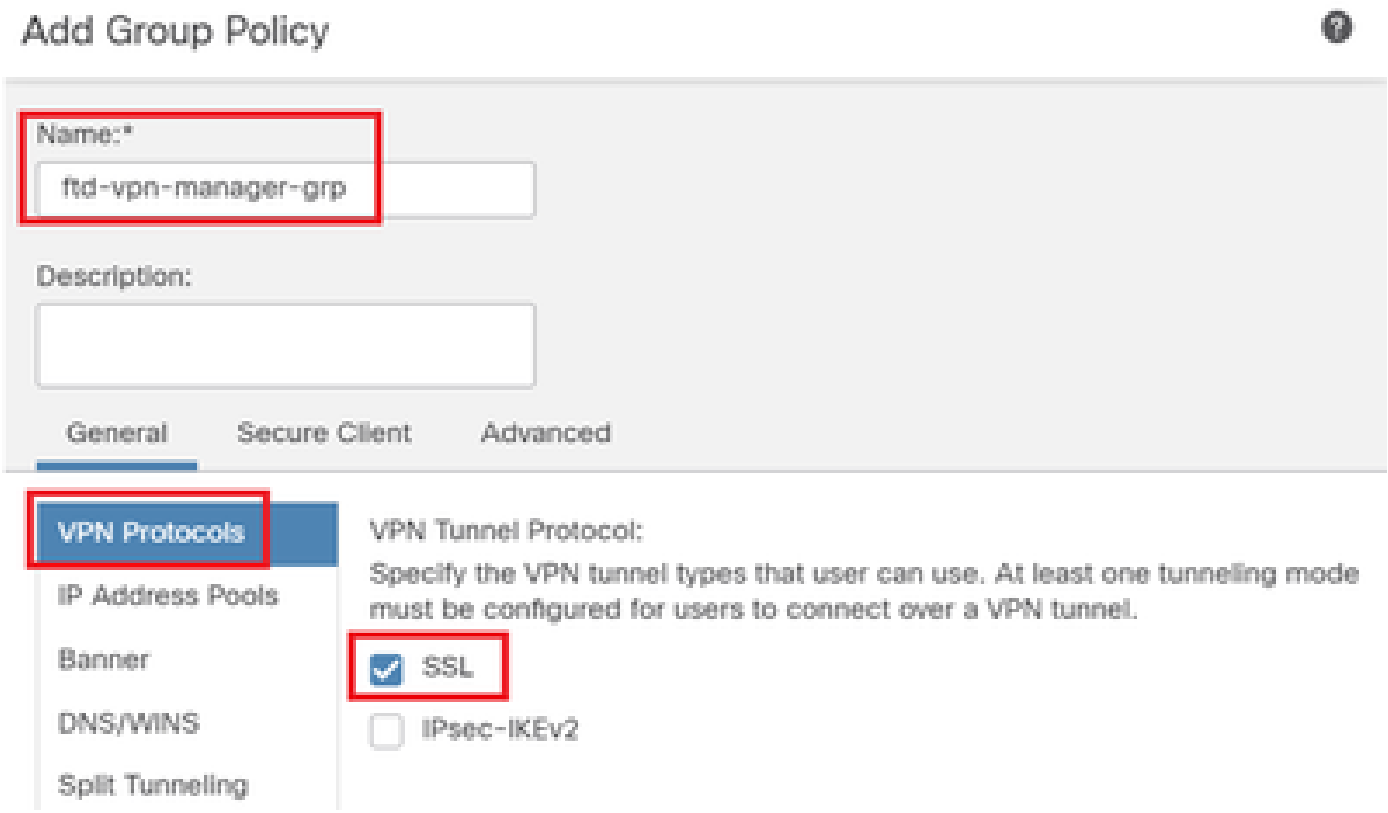
- Name: ftd-vpn-engineer-grp
- VPN-Protokolle: SSL



Gruppenrichtlinie für Techniker-VPN-Client

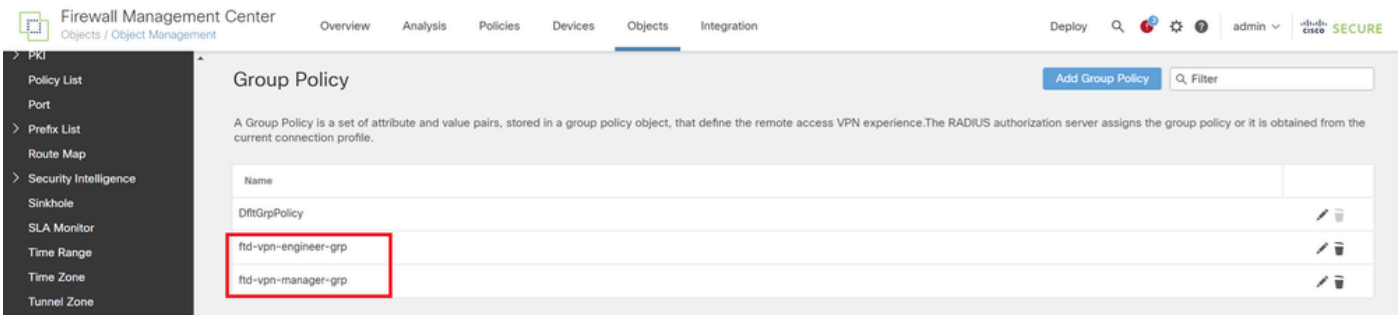
Geben Sie die erforderlichen Informationen ein, um eine Gruppenrichtlinie für den Manager-VPN-Client zu erstellen.

- Name: ftd-vpn-manager-grp
- VPN-Protokolle: SSL



Gruppenrichtlinie für Manager-VPN-Client

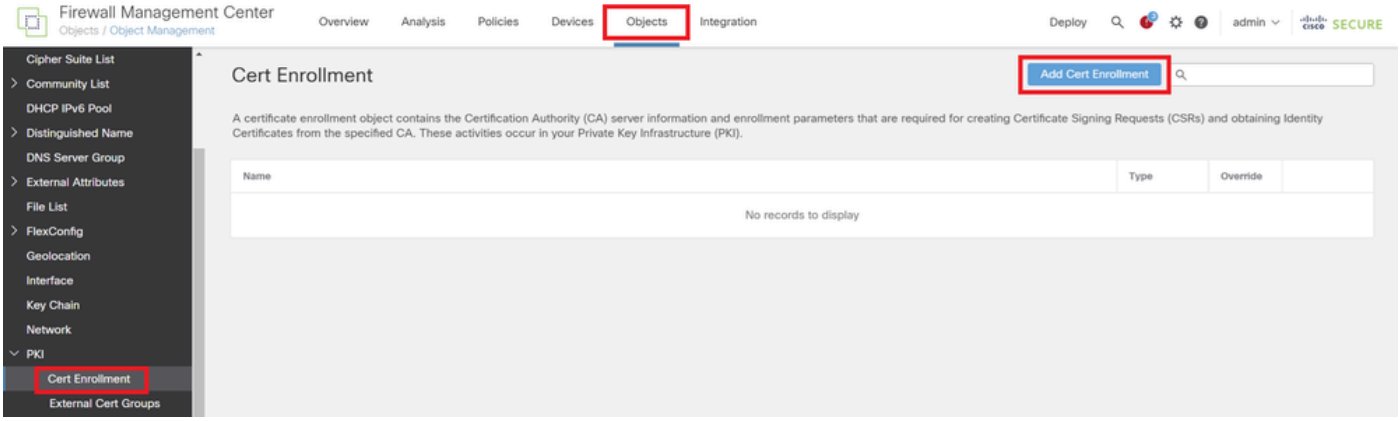
Die neuen Gruppenrichtlinien bestätigen.



Neue Gruppenrichtlinien

Schritt 5: FTD-Zertifikat hinzufügen

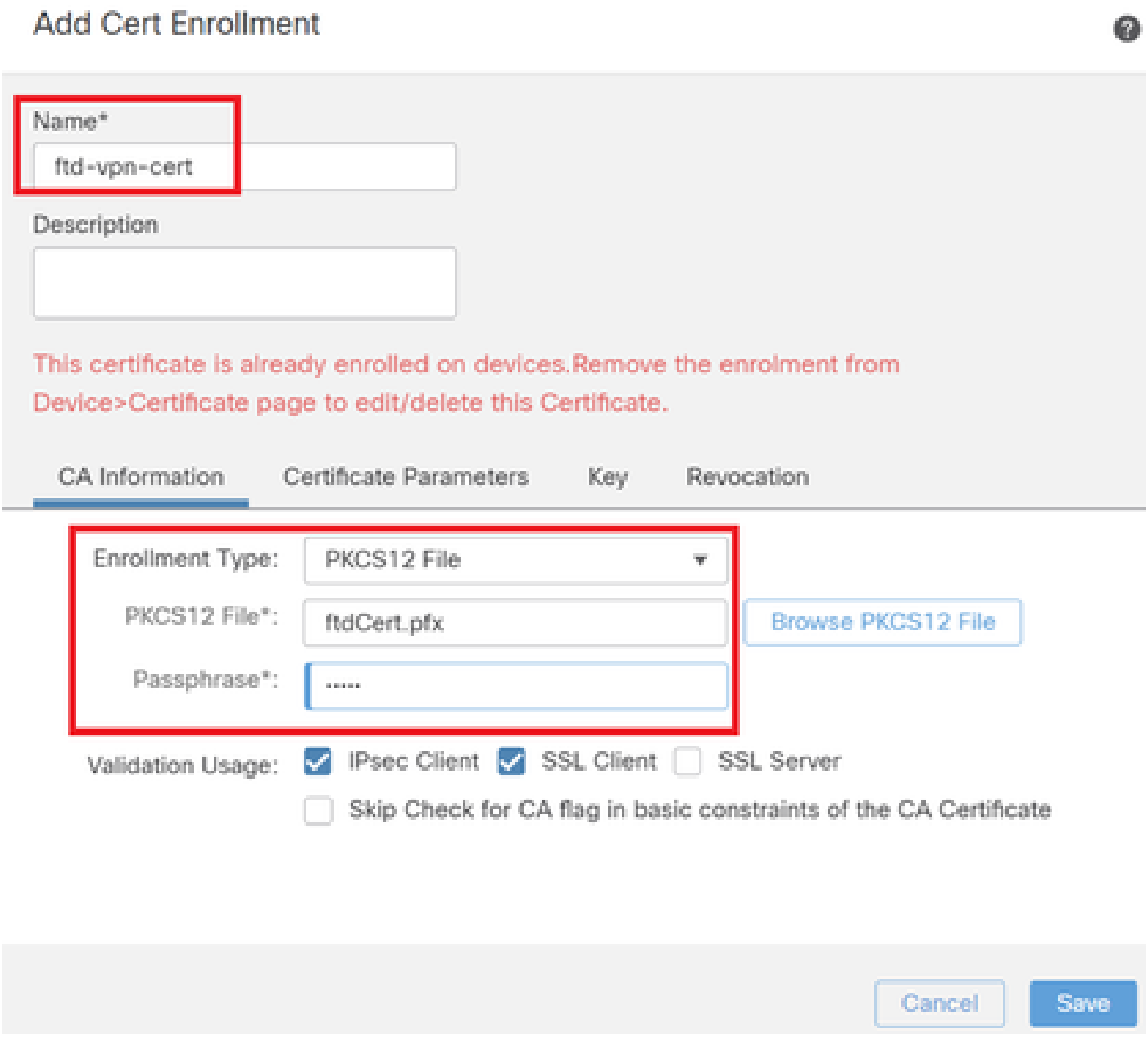
Navigieren Sie zuObject > Object Management > PKI > Cert Enrollment, und klicken Sie auf Add Cert Enrollment (Zertifikatregistrierung hinzufügen).



Zertifikatregistrierung hinzufügen

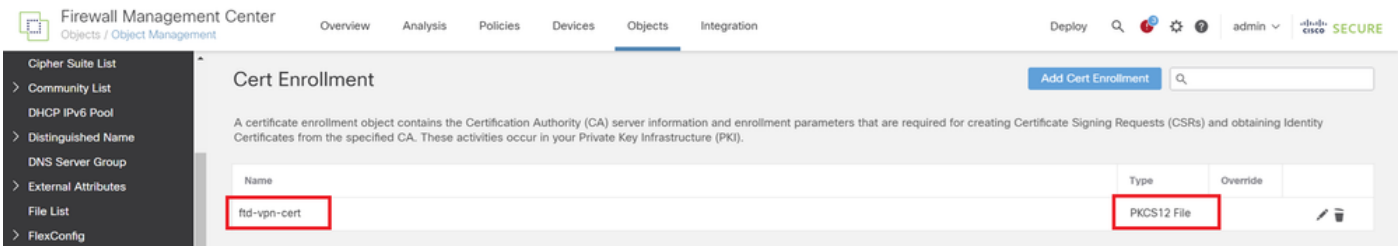
Geben Sie die erforderlichen Informationen für das FTD-Zertifikat ein, und importieren Sie eine PKCS12-Datei vom lokalen Computer.

- Name: ftd-vpn-Zertifikat
- Registrierungstyp: PKCS12-Datei



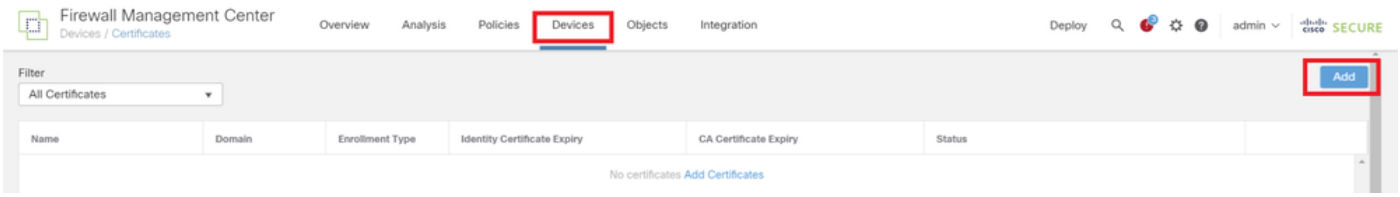
Details zur Zertifikatregistrierung

Bestätigen Sie die neue Zertifikatregistrierung.



Neue Zertifikatregistrierung

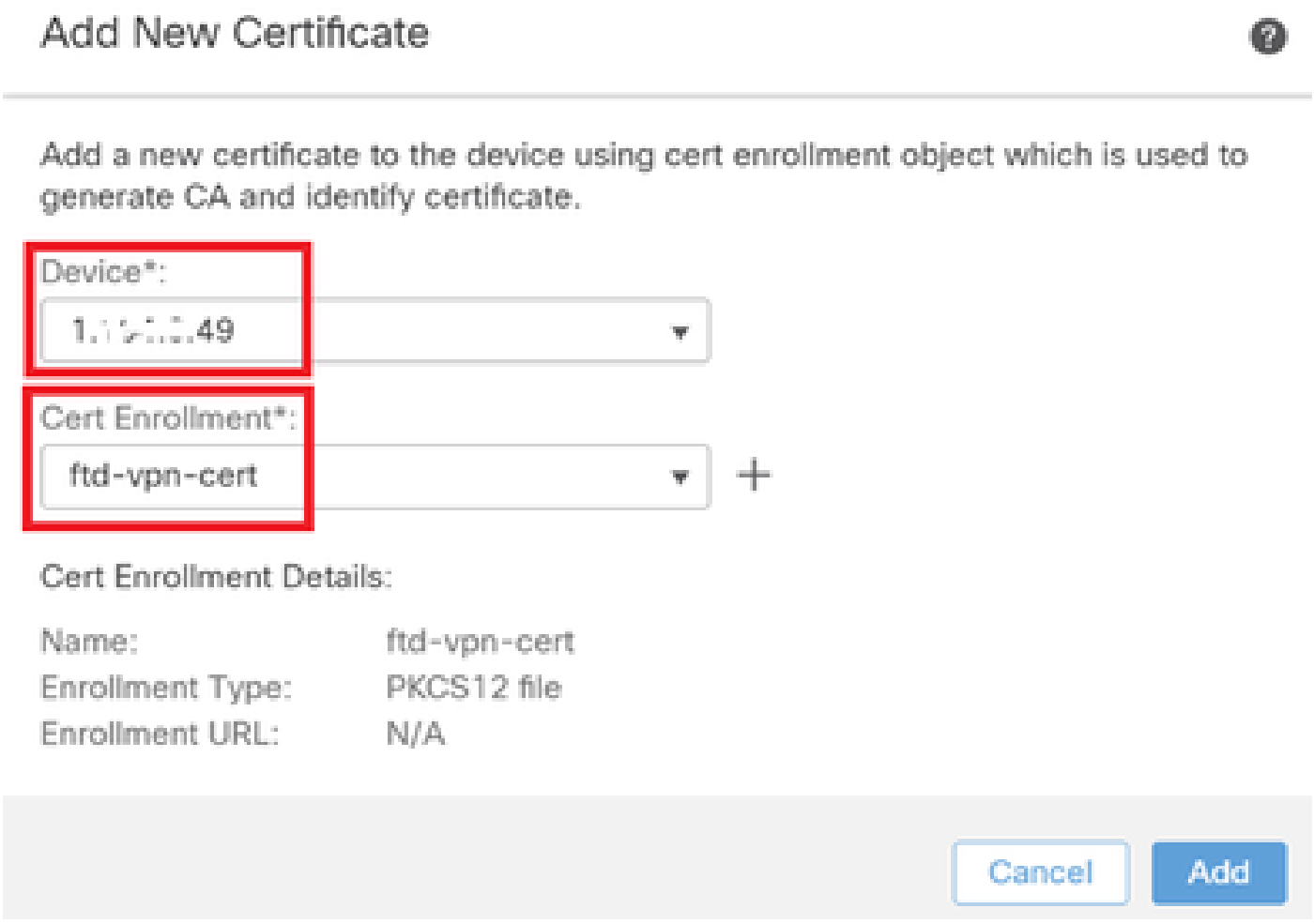
Navigieren Sie zuGeräte > Zertifikate, und klicken Sie auf die Schaltfläche Hinzufügen.



FTD-Zertifikat hinzufügen

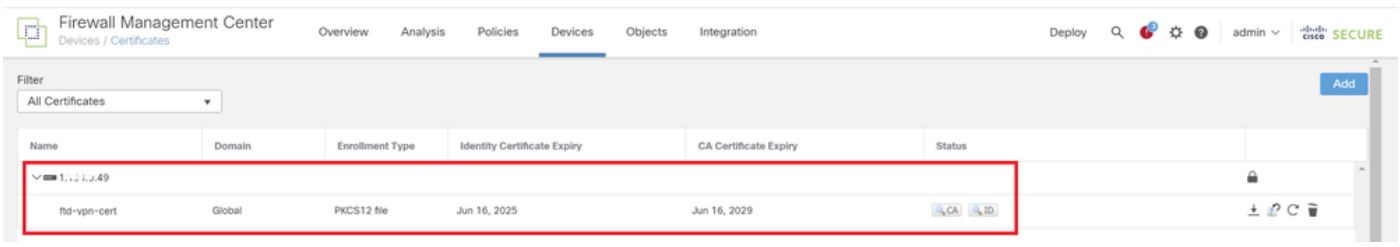
Geben Sie die erforderlichen Informationen ein, um die neue Zertifikatsregistrierung an FTD zu binden.

- Gerät: 1.x.x.49
- Zertifikatregistrierung: ftd-vpn-cert



Zertifikat an FTD binden

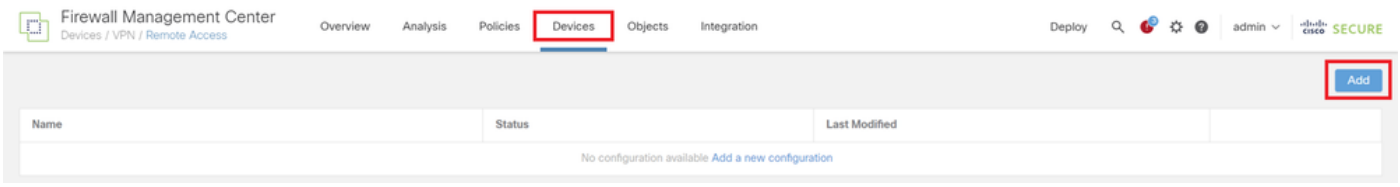
Bestätigen Sie den Status der Zertifikatbindung.



Status der Zertifikatbindung

Schritt 6: Richtlinienzuweisung für Techniker-Verbindungsprofil hinzufügen

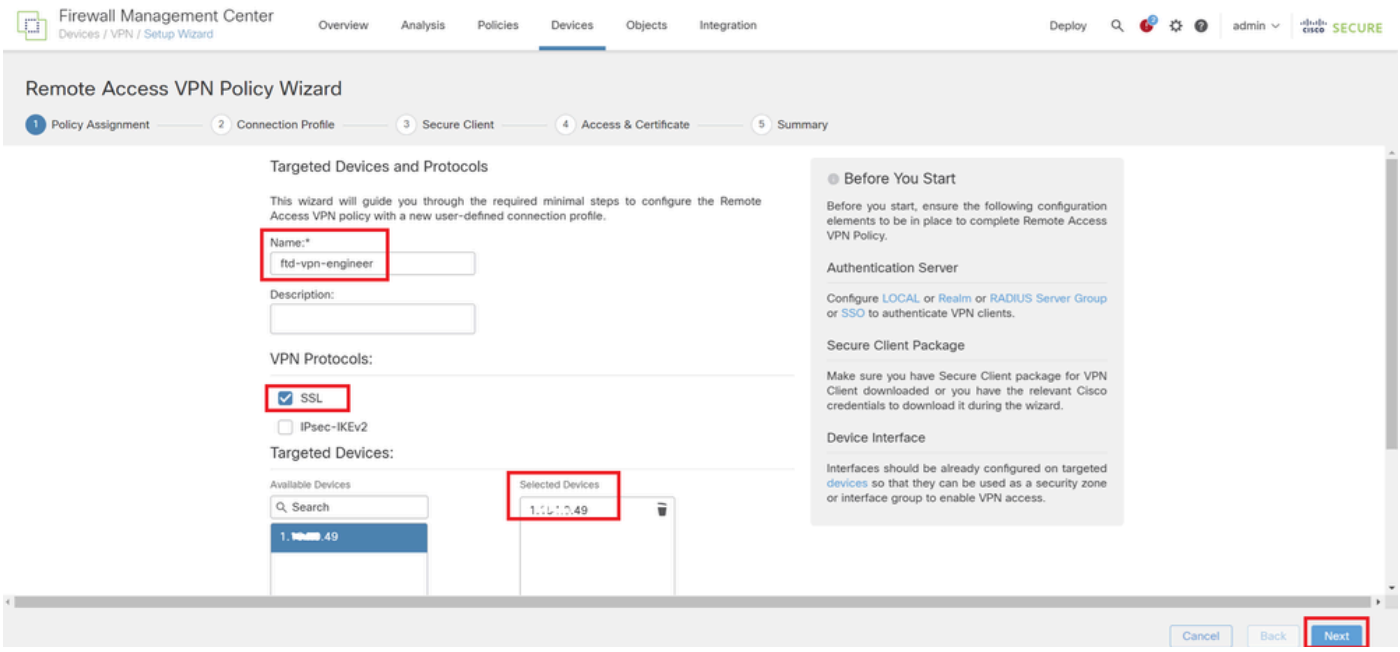
Navigieren Sie zuGeräte > VPN > Remotezugriff, und klicken Sie auf Hinzufügen.



Remote Access-VPN hinzufügen

Geben Sie die erforderlichen Informationen ein, und klicken Sie aufWeiter.

- Name: ftd-vpn-engineer
- VPN-Protokolle: SSL
- Zielgeräte: 1.x.x.49



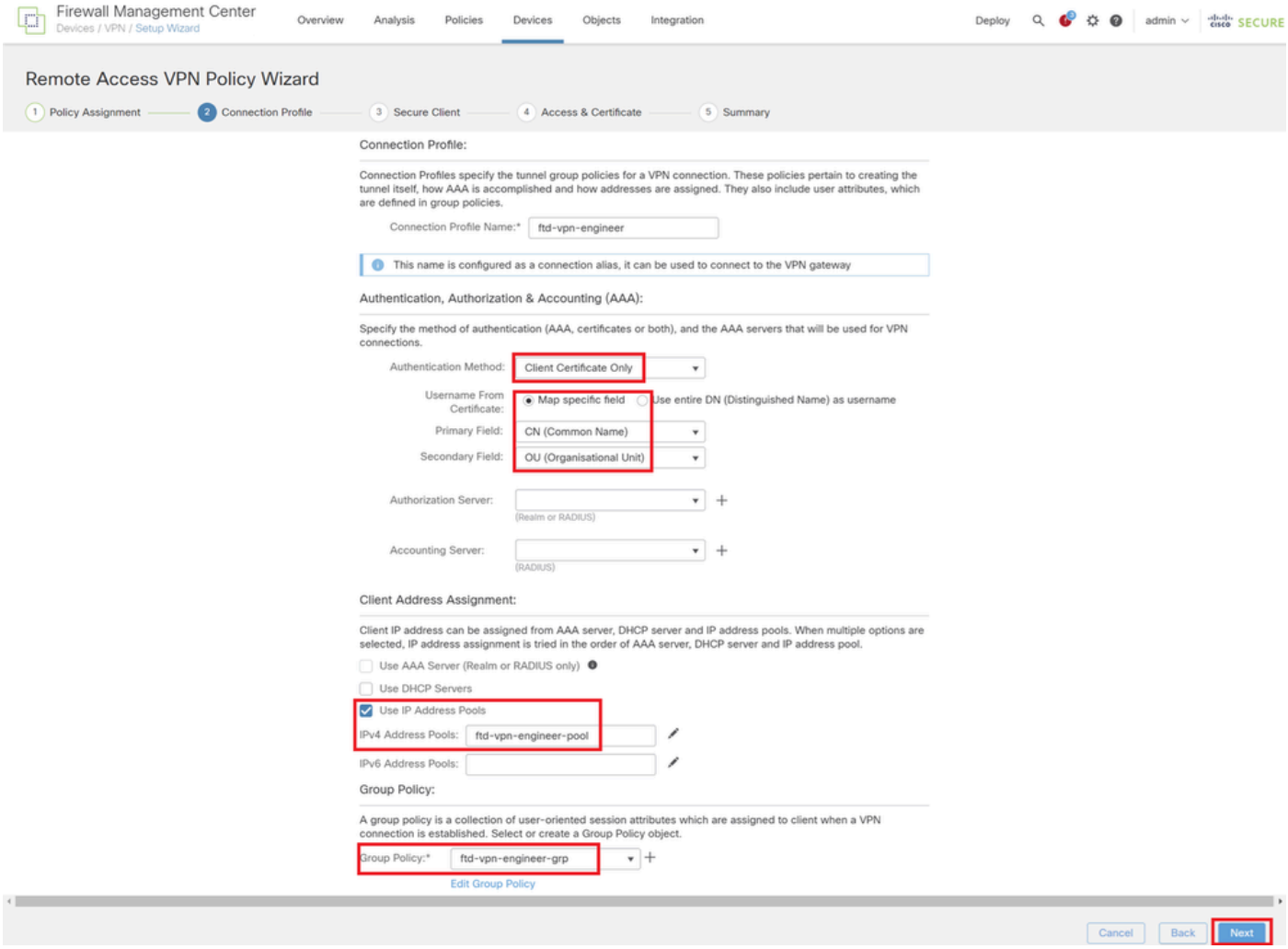
Richtlinienzuweisung

Schritt 7. Konfigurieren von Details für das Verbindungsprofil eines Technikers

Geben Sie die erforderlichen Informationen ein, und klicken Sie aufWeiter.

- Authentifizierungsmethode: Nur Client-Zertifikat
- Benutzername vom Zertifikat: Zuordnungsspezifisches Feld
- Primärfeld: CN (Common Name)
- Sekundäres Feld: OU (Organisationseinheit)

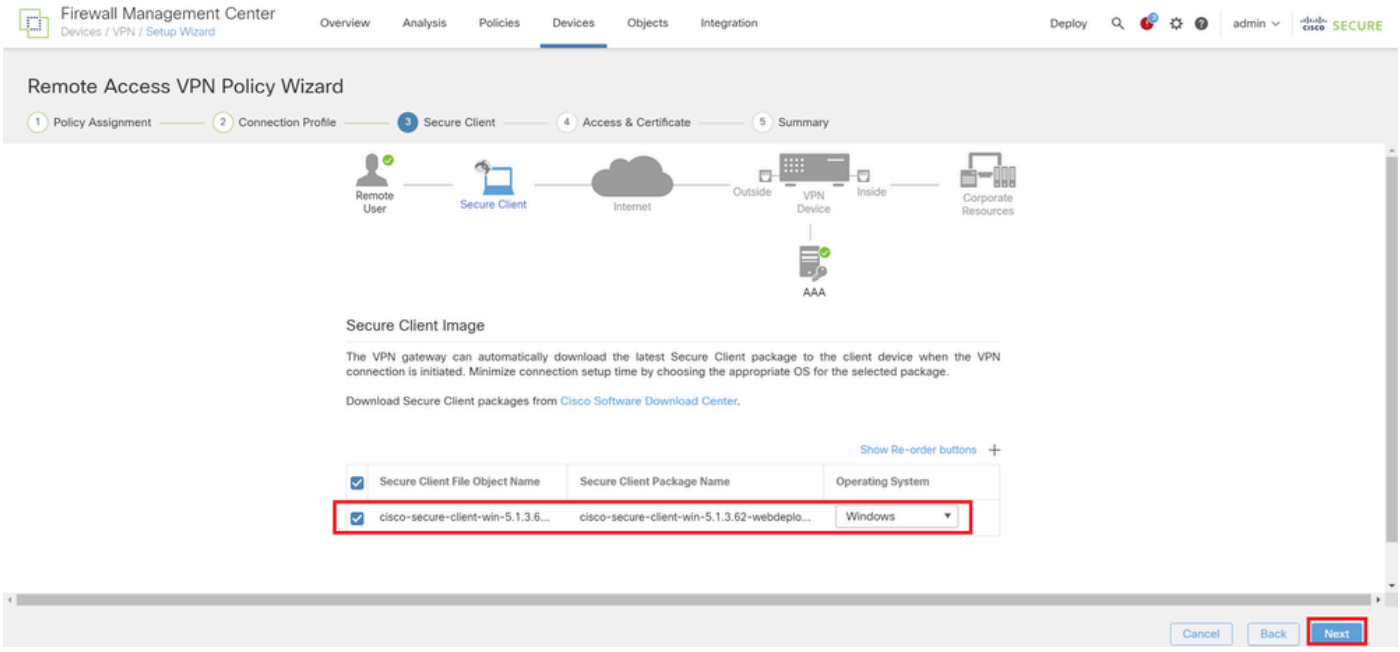
- IPv4-Adresspools: ftd-vpn-engineer-pool
- Gruppenrichtlinie: ftd-vpn-engineer-grp



Details zum Verbindungsprofil

Schritt 8: Konfigurieren von sicherem Client-Image für Techniker-Verbindungsprofil

Wählen Sie sichere Client-Abbilddatei aus, und klicken Sie auf Weiter.

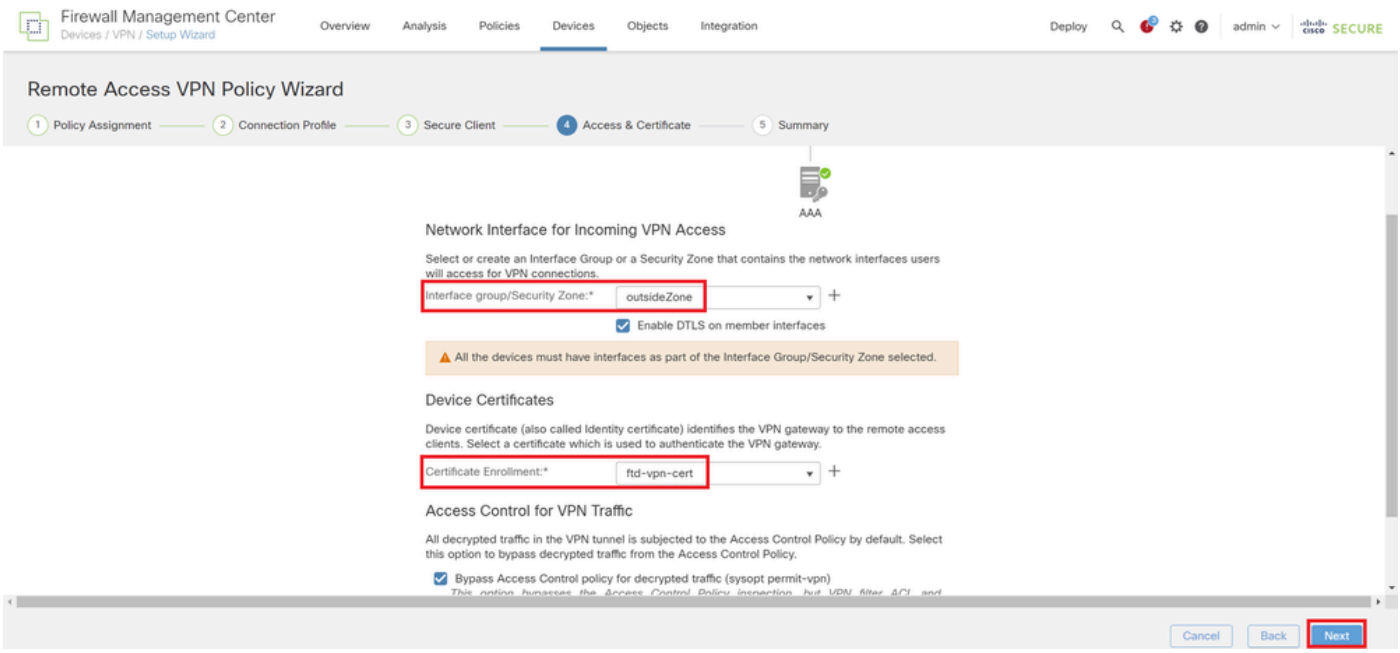


Sicheren Client auswählen

Schritt 9. Konfigurieren des Zugriffs und des Zertifikats für das Techniker-Verbindungsprofil

Wählen Sie einen Wert für Schnittstellengruppe/Sicherheitszone und Zertifikatregistrierungselemente aus, und klicken Sie auf die Schaltfläche Weiter.

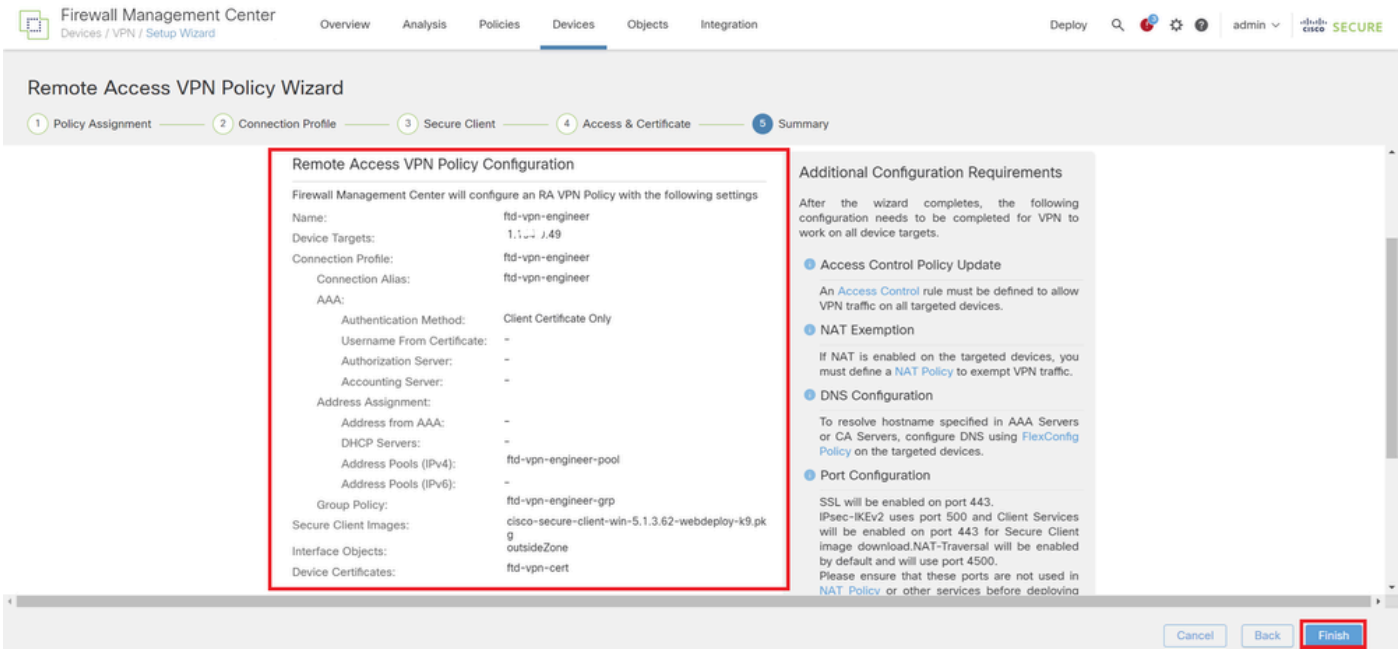
- Schnittstellengruppe/Sicherheitszone: outsideZone
- Zertifikatregistrierung: ftd-vpn-cert



Details zum Zugriff und Zertifikat

Schritt 10. Zusammenfassung für Techniker-Verbindungsprofil bestätigen

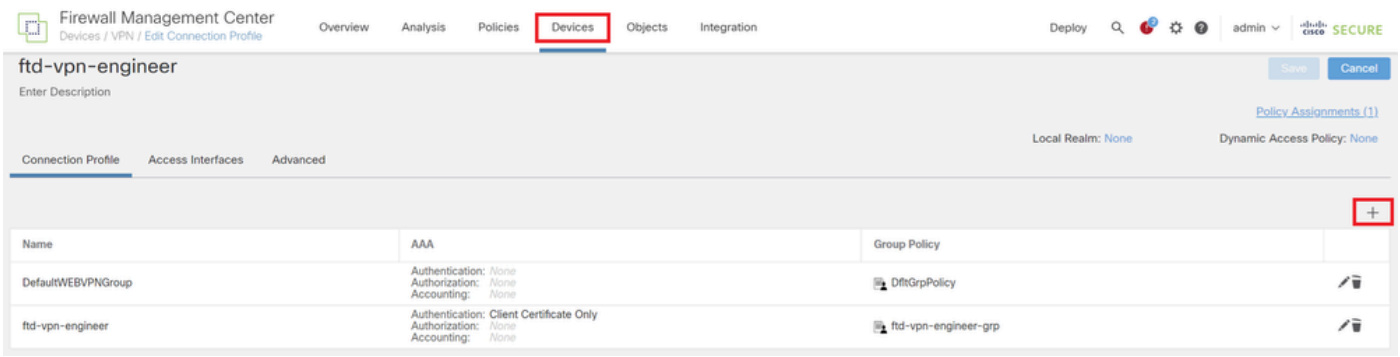
Bestätigen Sie die für die VPN-Richtlinie für den Remotezugriff eingegebenen Informationen, und klicken Sie auf die Schaltfläche Fertig stellen.



Details zur VPN-Richtlinie für den Remote-Zugriff

Schritt 11. Hinzufügen eines Verbindungsprofils für den Manager-VPN-Client

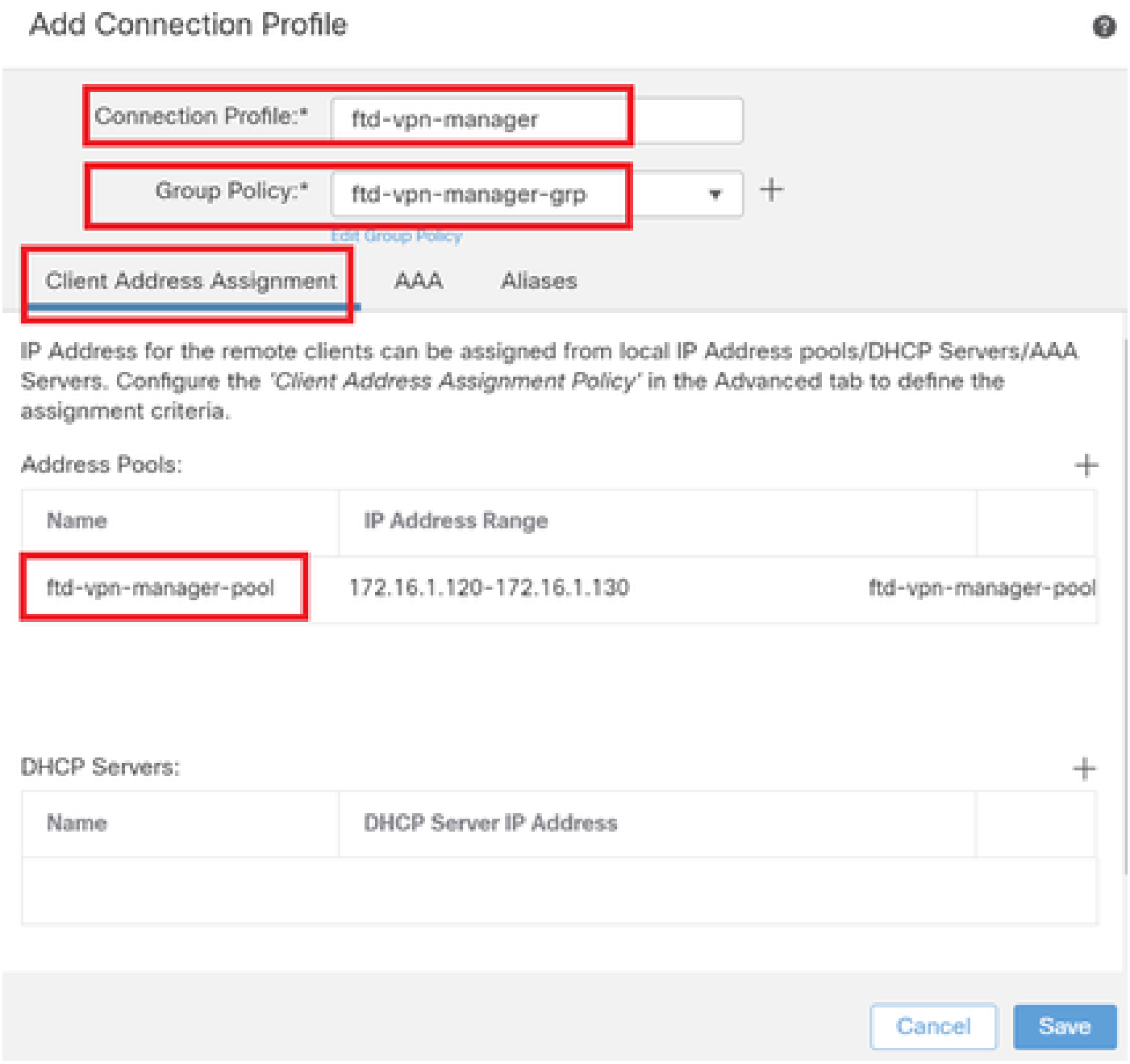
Navigieren Sie zu Geräte > VPN > Remotezugriff > Verbindungsprofil, und klicken Sie auf +.



Hinzufügen eines Verbindungsprofils für den Manager-VPN-Client

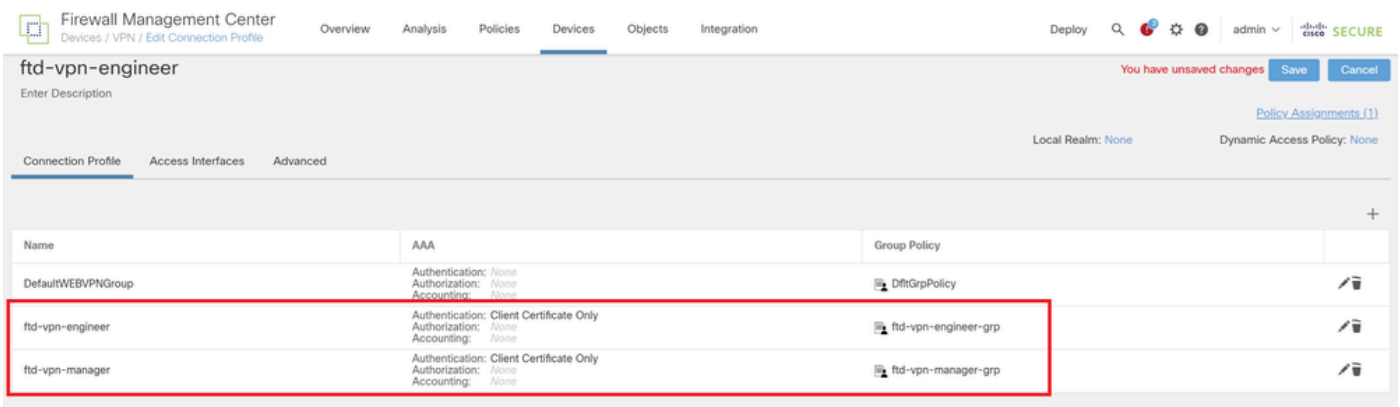
Geben Sie die erforderlichen Informationen für das Verbindungsprofil ein, und klicken Sie auf die Schaltfläche Speichern.

- Name: ftd-vpn-manager
- Gruppenrichtlinie: ftd-vpn-manager-grp
- IPv4-Adresspools: ftd-vpn-manager-pool



Details zum Verbindungsprofil für den Manager-VPN-Client

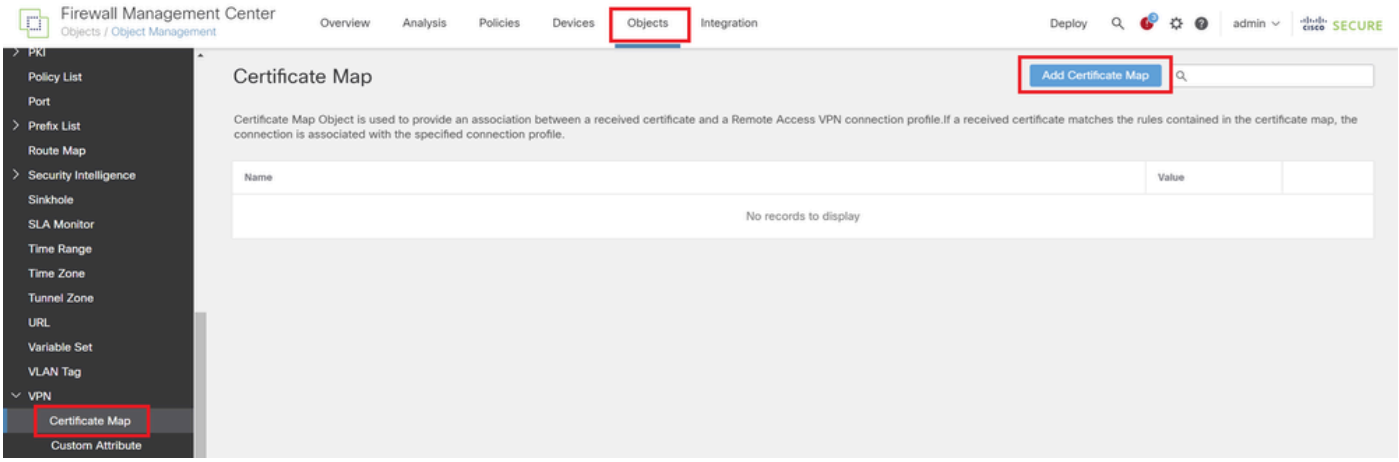
Neue hinzugefügte Verbindungsprofile bestätigen



Hinzufügen von Verbindungsprofilen bestätigen

Schritt 12: Zertifikatzuordnung hinzufügen

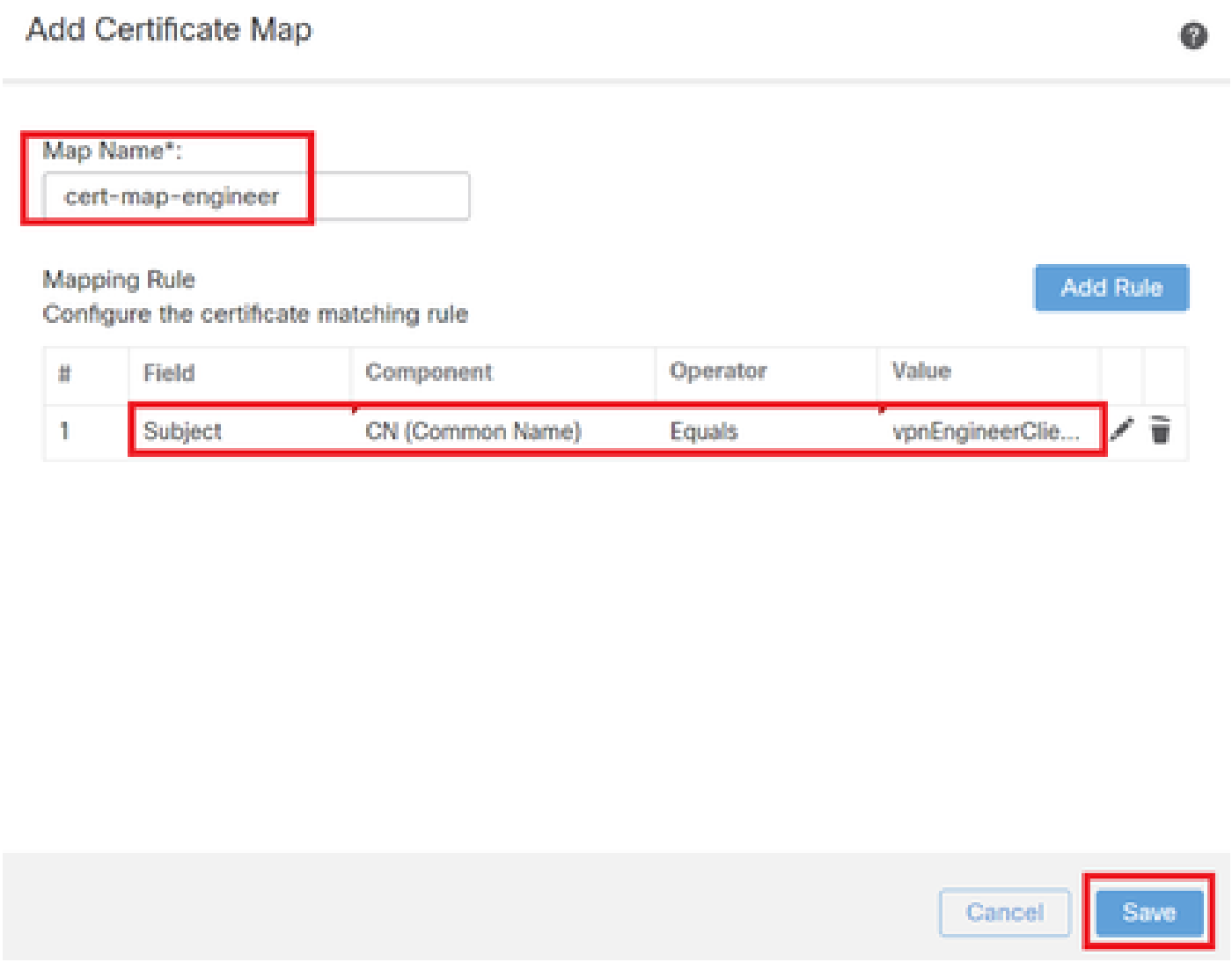
Navigieren Sie zu Objekte > Objektverwaltung > VPN > Zertifikatzuordnung, und klicken Sie auf die Schaltfläche Zertifikatzuordnung hinzufügen.



Zertifikatzuordnung hinzufügen

Geben Sie die erforderlichen Informationen für die Zertifikatszuordnung des VPN-Clients des Technikers ein, und klicken Sie auf die Schaltfläche Speichern.

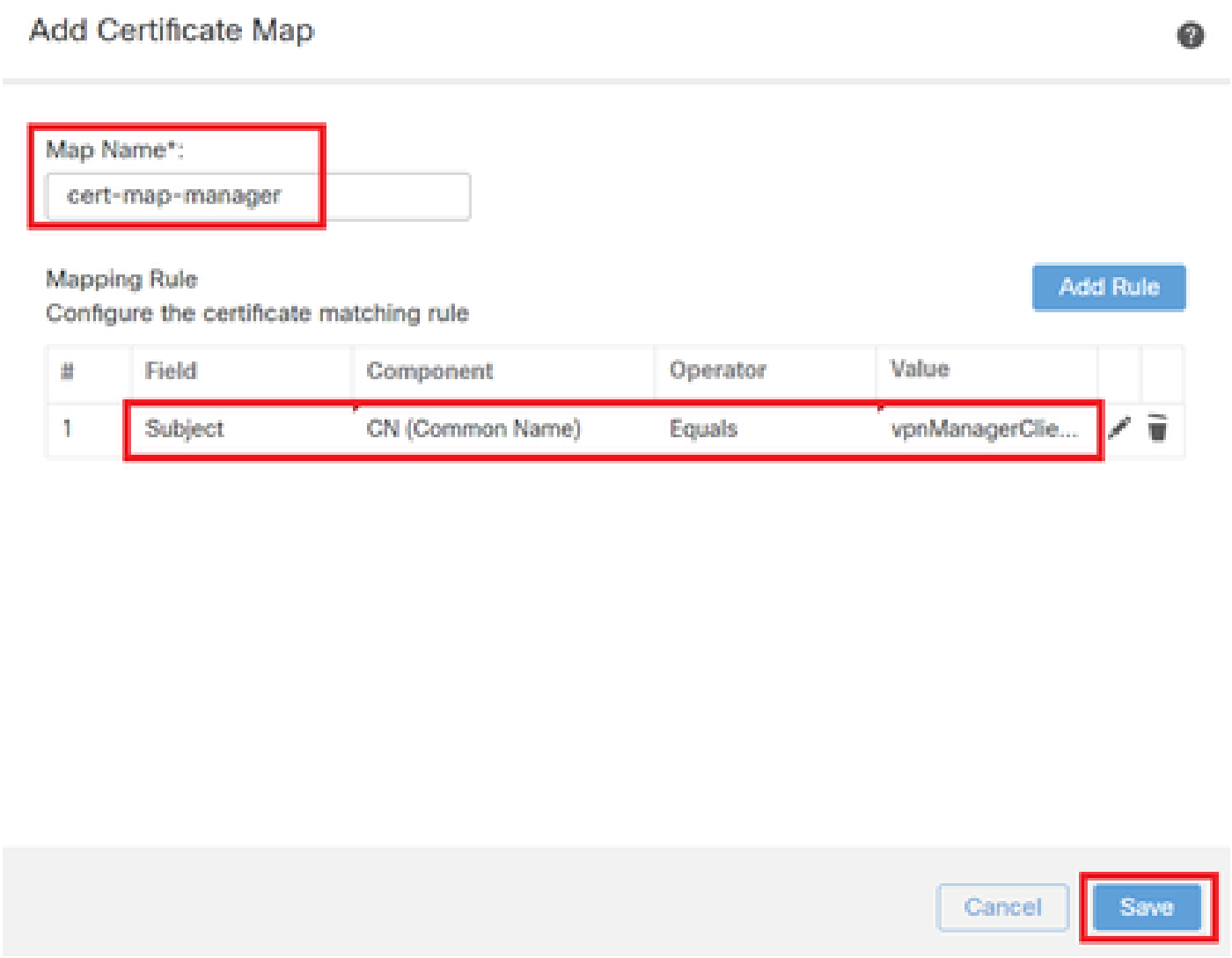
- Name der Karte: cert-map-engineer
- Zuordnungsregel: CN (Common Name) Equals vpnEngineerClientCN



Zertifikatszuordnung für Techniker-Client

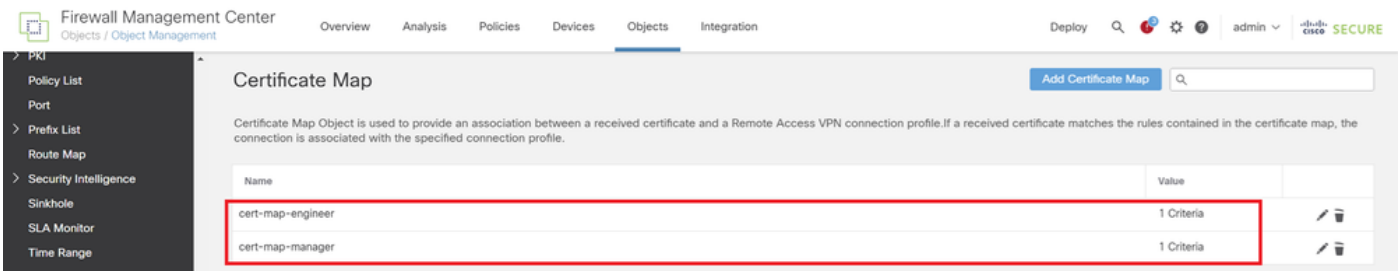
Geben Sie die erforderlichen Informationen für die Zertifikatszuordnung des VPN-Clients des Managers ein, und klicken Sie auf die Schaltfläche Speichern.

- Kartenname: cert-map-manager
- Zuordnungsregel: CN (Common Name) Equals vpnManagerClientCN



Zertifikatszuordnung für Manager-Client

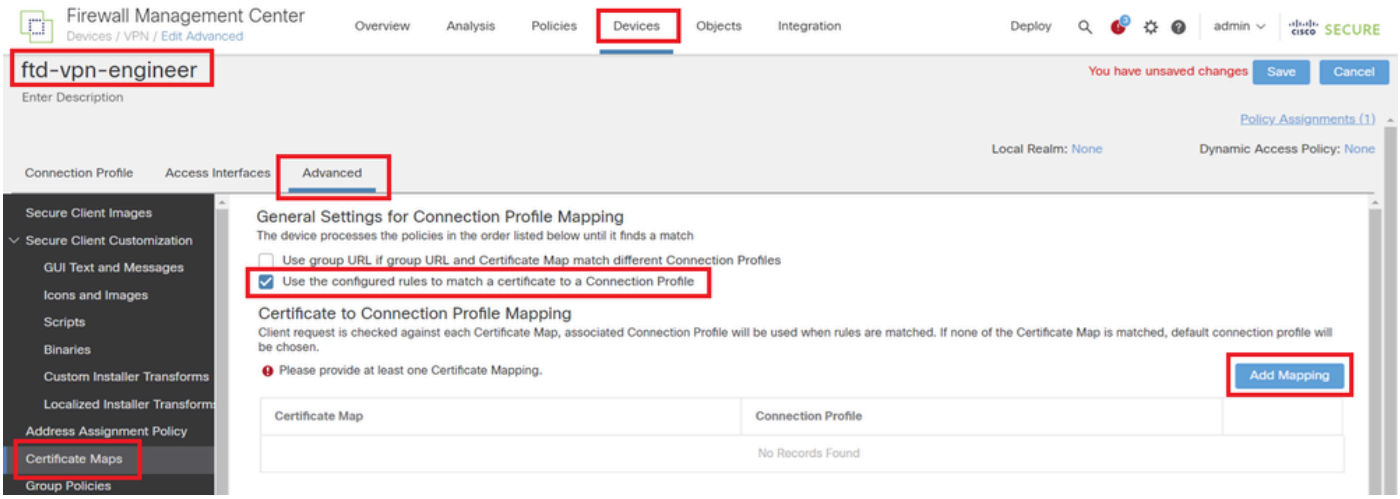
Neue hinzugefügte Zertifikatszuordnungen bestätigen.



Neue Zertifikatzuordnungen

Schritt 13: Binden der Zertifikatzuordnung an das Verbindungsprofil

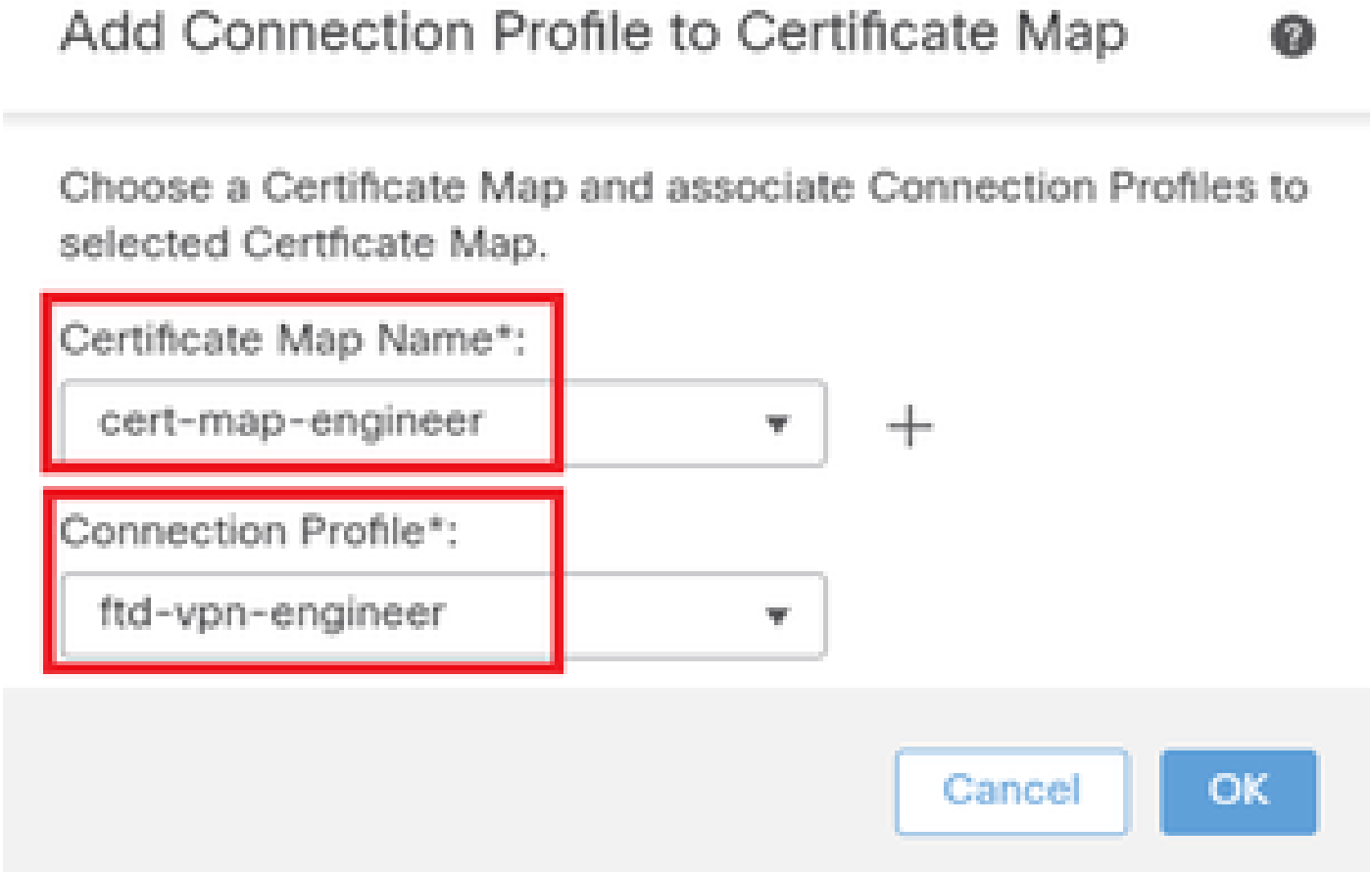
Navigieren Sie zu Devices > VPN > Remote Access, und bearbeiten Sie ftd-vpn-engineer. Navigieren Sie anschließend zu Erweitert > Zertifikatzuordnungen, und klicken Sie auf die Schaltfläche Zuordnung hinzufügen.



Zertifikatzuordnung binden

Bindende Zertifikatzuordnung zum Verbindungsprofil für VPN-Client des Technikers.

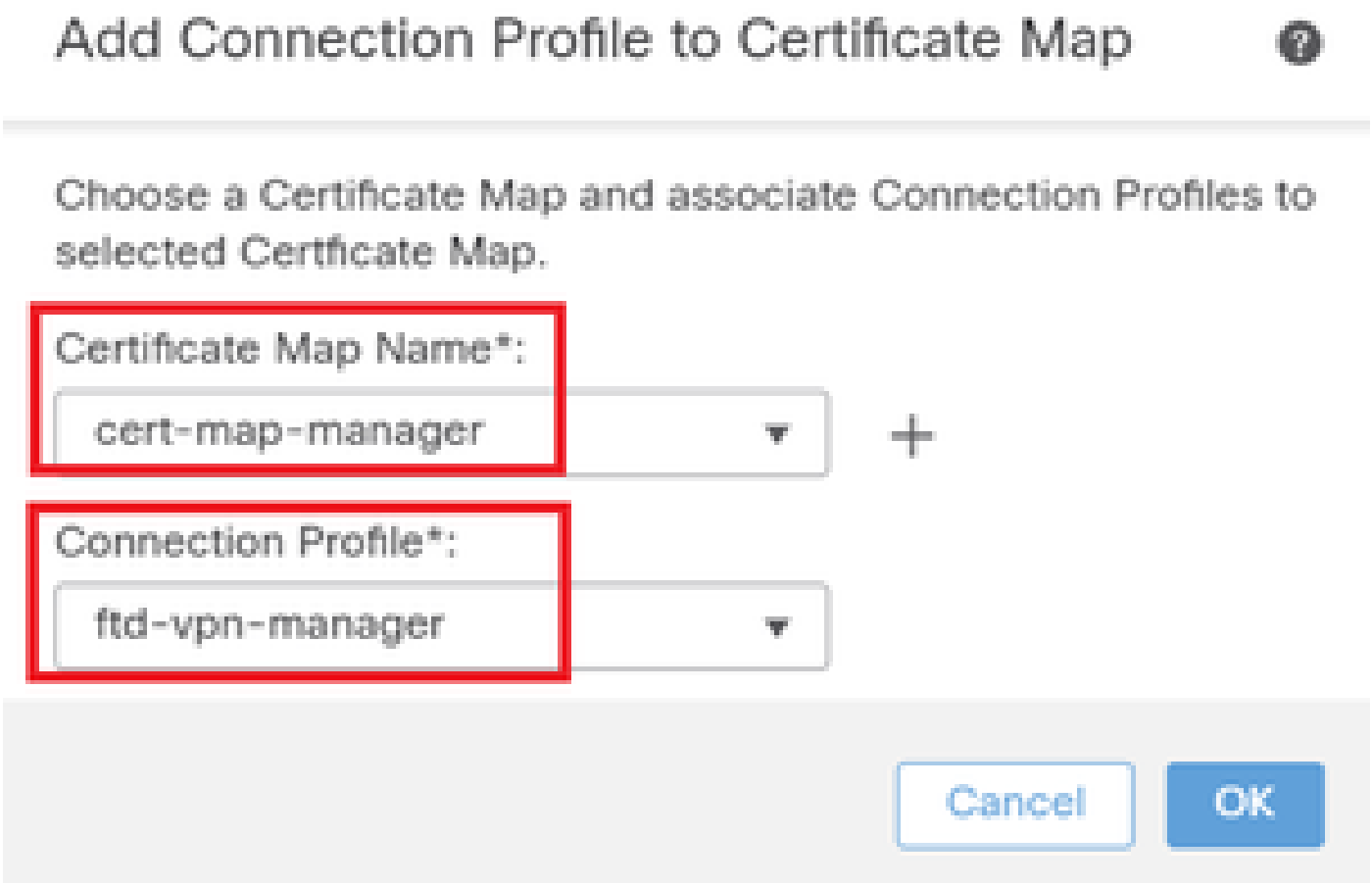
- Name der Zertifikatszuordnung: cert-map-engineer
- Connection Profile: ftd-vpn-engineer



Bindende Zertifikatzuordnung für Techniker-VPN-Client

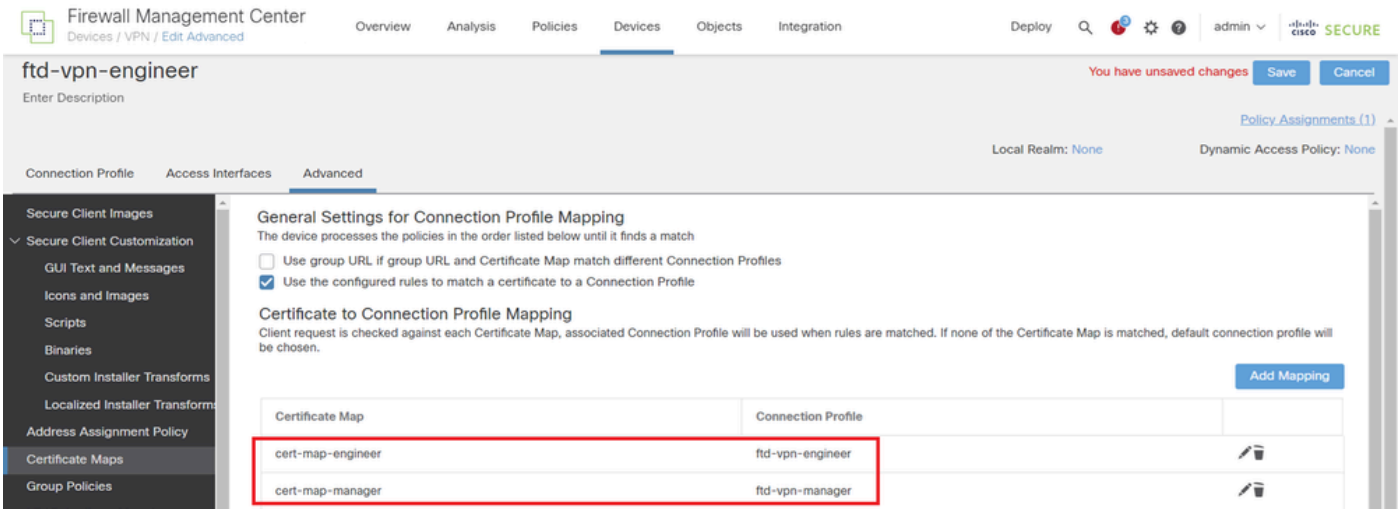
Bindende Zertifikatzuordnung zum Verbindungsprofil für Manager-VPN-Client.

- Name der Zertifikatszuordnung: cert-map-manager
- Verbindungsprofil: ftd-vpn-manager



Bindende Zertifikatzuordnung für Manager VPN Client

Bestätigen Sie die Einstellung der Zertifikatbindung.



Zertifikatbindung bestätigen

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

// Defines a pool of addresses
ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0
ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0

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

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

certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Defines Certificate Map for Engineer VPN Clients
crypto ca certificate map cert-map-engineer 10
subject-name attr cn eq vpnEngineerClientCN

// Defines Certificate Map for Manager VPN Clients
crypto ca certificate map cert-map-manager 10
subject-name attr cn eq vpnManagerClientCN

// 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
certificate-group-map cert-map-engineer 10 ftd-vpn-engineer
certificate-group-map cert-map-manager 10 ftd-vpn-manager
error-recovery disable

// Configures the group-policy to allow SSL connections from manager VPN clients
group-policy ftd-vpn-manager-grp internal
group-policy ftd-vpn-manager-grp attributes
banner none
wins-server none
```

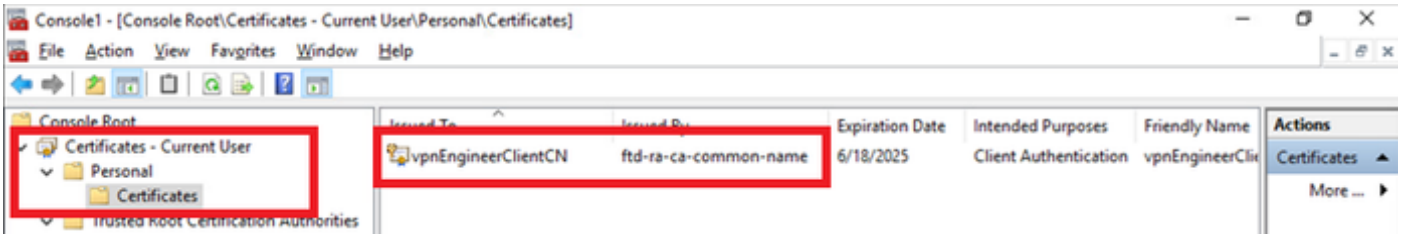
```
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
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 group-policy to allow SSL connections from engineer VPN clients
group-policy ftd-vpn-engineer-grp internal
group-policy ftd-vpn-engineer-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 certificate authentication for engineer VPN clients
tunnel-group ftd-vpn-engineer type remote-access
tunnel-group ftd-vpn-engineer general-attributes
address-pool ftd-vpn-engineer-pool
default-group-policy ftd-vpn-engineer-grp
tunnel-group ftd-vpn-engineer webvpn-attributes
authentication certificate
group-alias ftd-vpn-engineer enable

// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate
```

Bestätigung in VPN-Client

Schritt 1: Clientzertifikat bestätigen

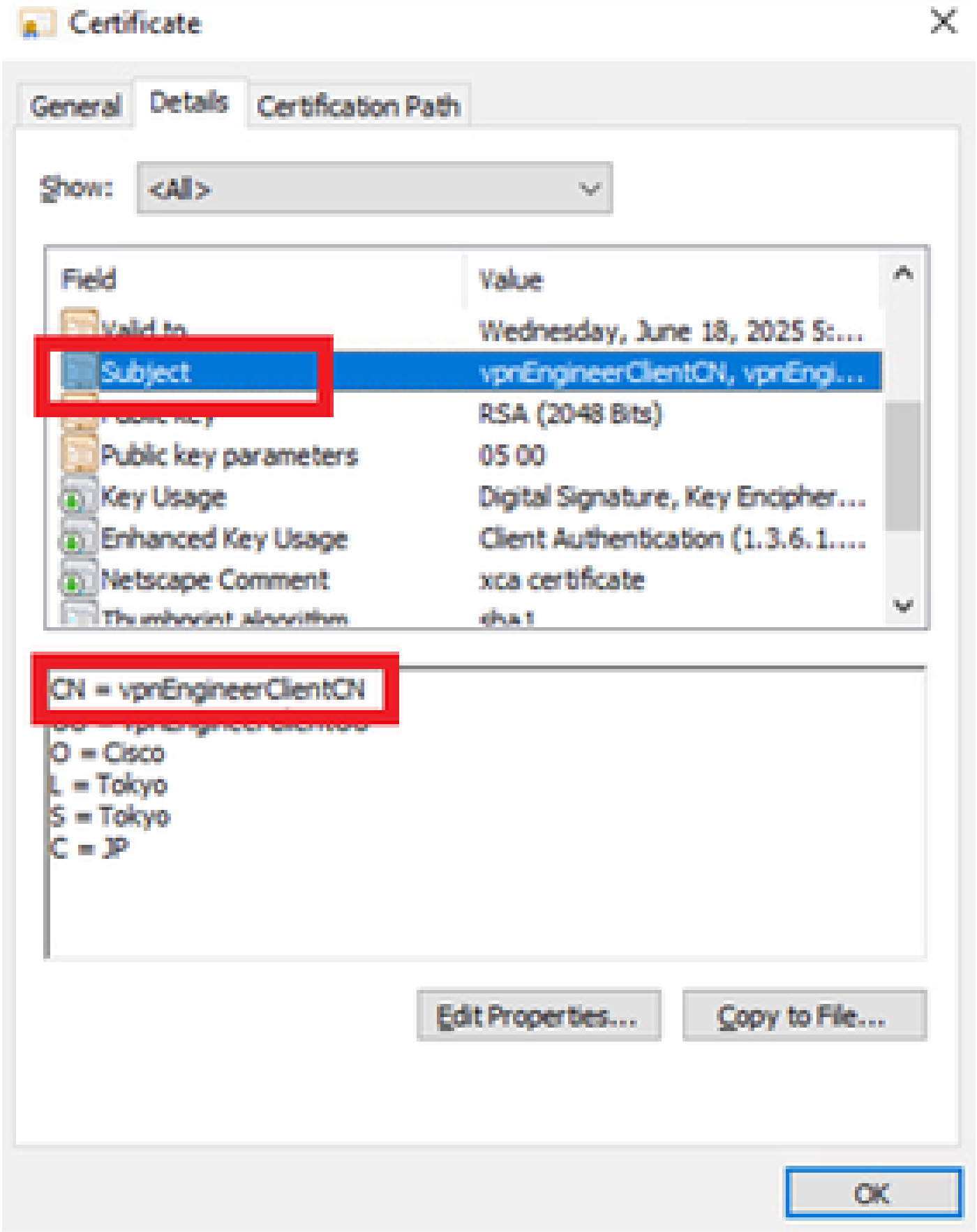
Navigieren Sie im VPN-Client des Technikers zu Certificates - Current User > Personal > Certificates, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.



Zertifikat für Techniker-VPN-Client bestätigen

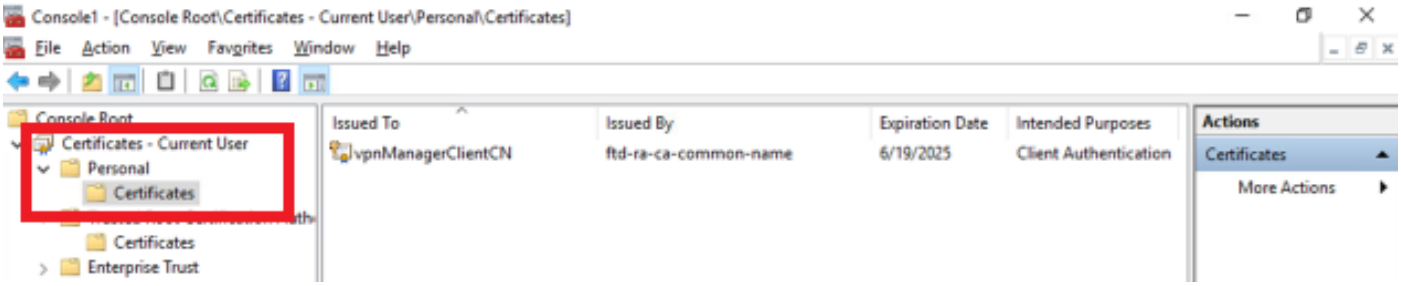
Doppelklicken Sie auf das Clientzertifikat, navigieren Sie zuDetails, und überprüfen Sie die Details vonSubject.

- Betreff: CN = vpnEngineerClientCN



Details zum Techniker-Client-Zertifikat

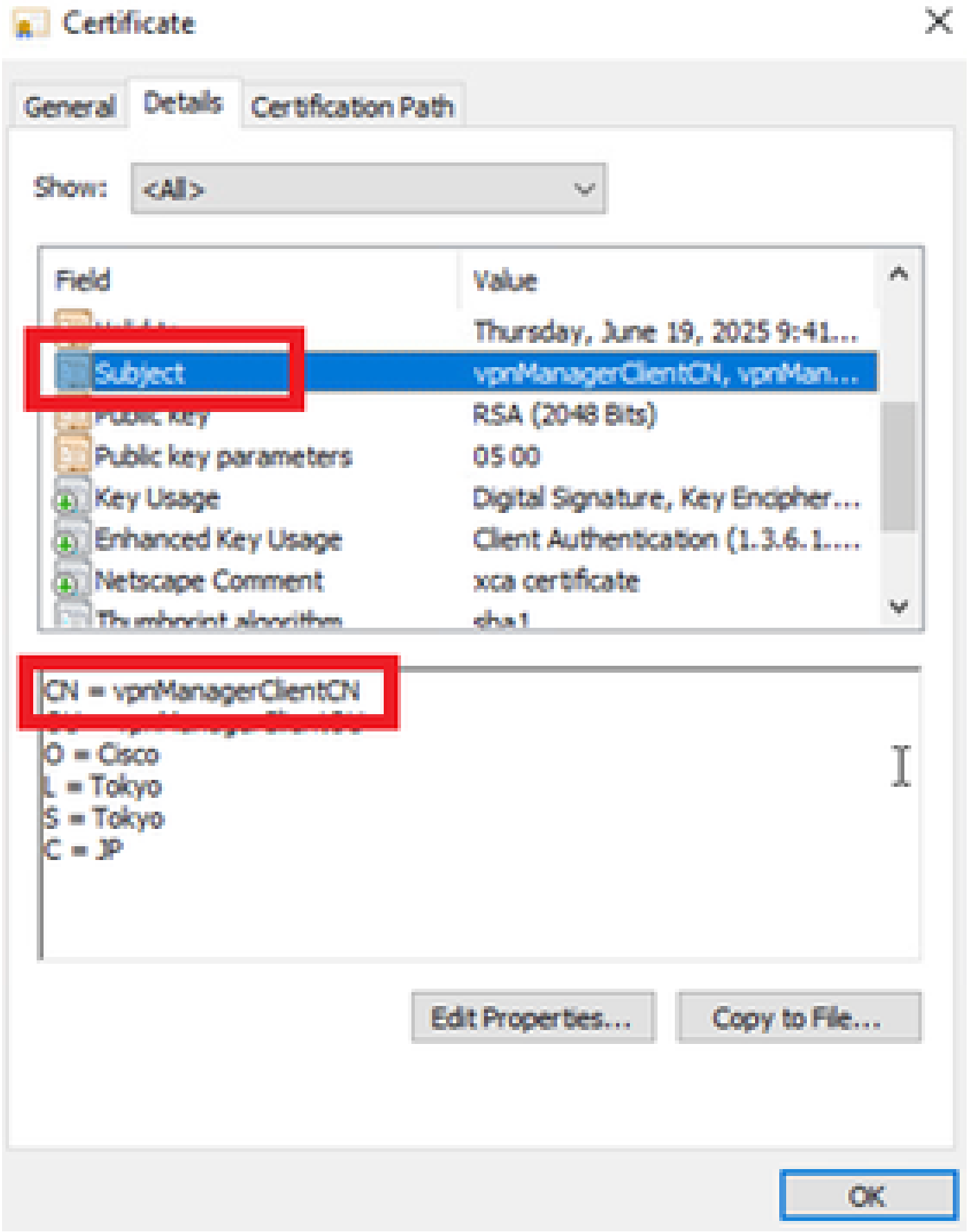
Navigieren Sie im VPN-Client des Managers zu Certificates - Current User > Personal > Certificates, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.



Zertifikat für Manager VPN Client bestätigen

Doppelklicken Sie auf das Clientzertifikat, navigieren Sie zuDetails, und überprüfen Sie die Details vonSubject.

- Betreff: CN = vpnManagerClientCN

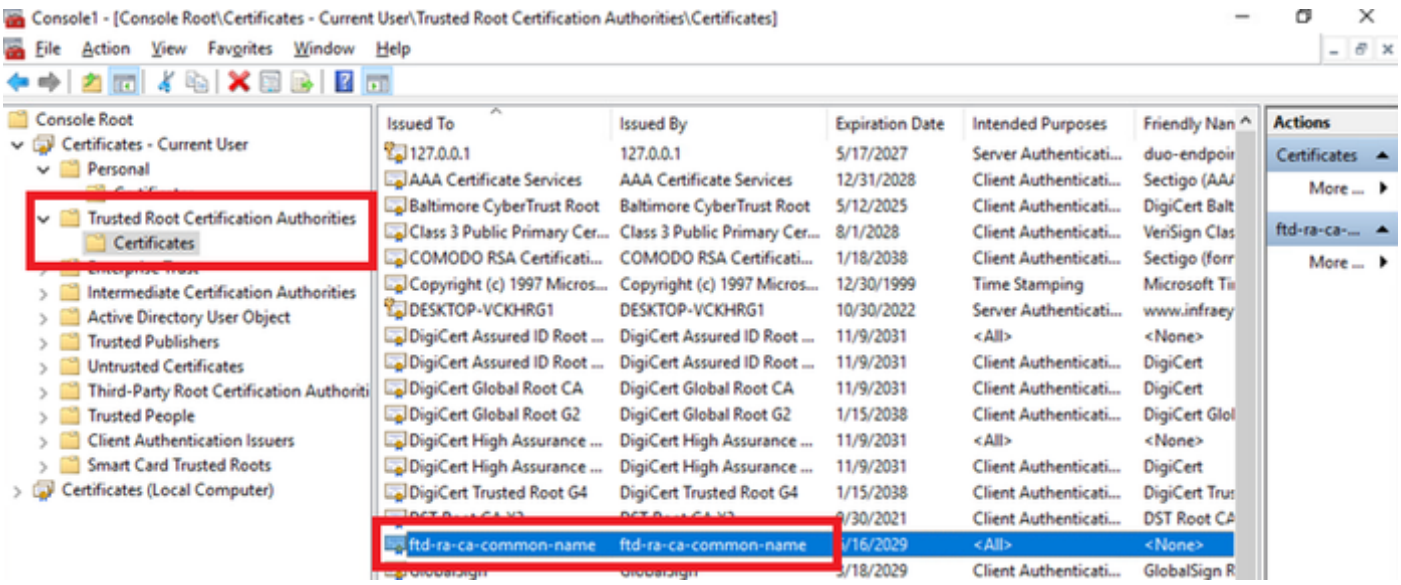


Details zum Manager-Clientzertifikat

Schritt 2: 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

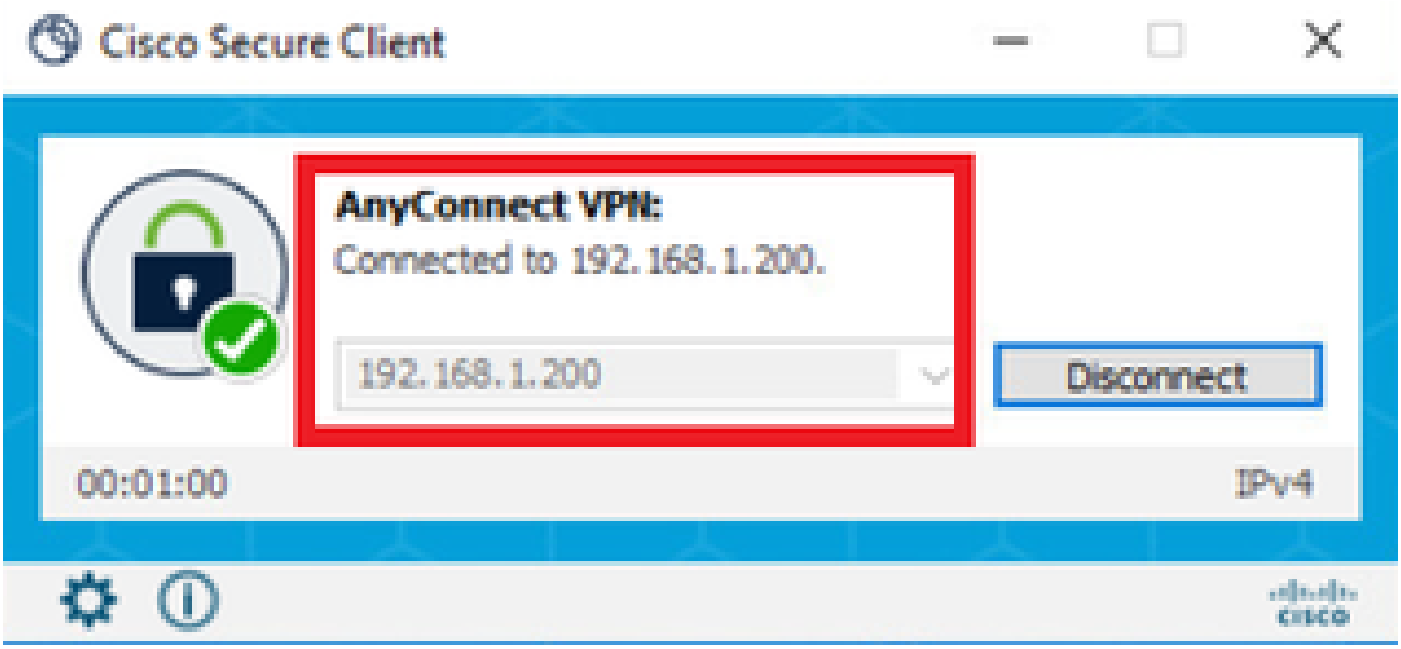


Zertifizierungsstelle bestätigen

Überprüfung

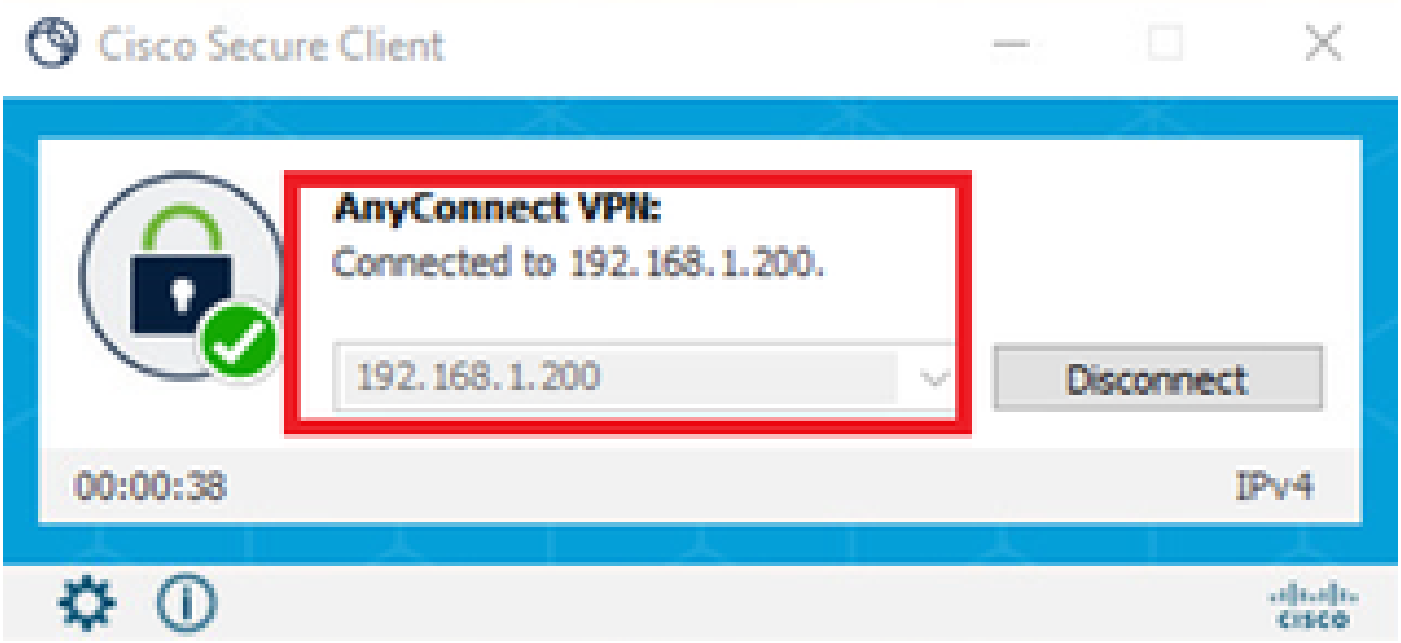
Schritt 1: VPN-Verbindung initiieren

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.



VPN-Verbindung vom Techniker-Client initiieren

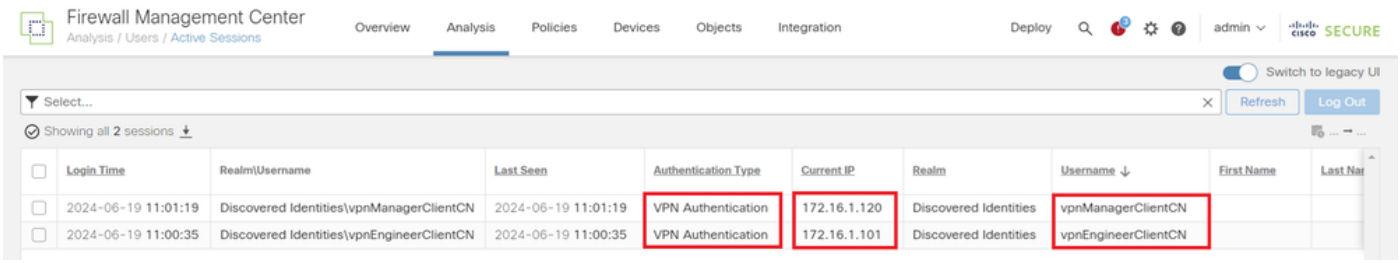
Initiieren Sie im Manager VPN Client die Verbindung zum Cisco Secure Client. Der Benutzername und das Kennwort müssen nicht eingegeben werden, da die VPN-Verbindung erfolgreich hergestellt wurde.



VPN-Verbindung vom Manager-Client 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-Sitzungen in FTD CLI bestätigen

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

```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 13
Assigned IP : 172.16.1.101 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 : 14782 Bytes Rx : 12714
Pkts Tx : 2 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer
Login Time : 02:00:35 UTC Wed Jun 19 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000d00066723bc3
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 13.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50225 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 13.2
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50232
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 1775
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 13.3
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 50825
UDP Dst Port : 443 Auth Mode : Certificate
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 : 10939
Pkts Tx : 0 Pkts Rx : 30
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Username : vpnManagerClientCN Index : 14
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
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 : 14782 Bytes Rx : 13521
Pkts Tx : 2 Pkts Rx : 57
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager
Login Time : 02:01:19 UTC Wed Jun 19 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000e00066723bef
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 14.1
Public IP : 192.168.1.21
Encryption : none Hashing : none
TCP Src Port : 49809 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 14.2
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 49816
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 3848
Pkts Tx : 1 Pkts Rx : 25
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 14.3
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 65501
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 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 : 9673
Pkts Tx : 0 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0

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 in der Lina-Engine während der VPN-Verbindung vom Engineering-Client.

```
<#root>

Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn
Jun 19 2024 02:00:35: %FTD-6-717022:

Certificate was successfully validated

. serial number: 7AF1C78ADCC8F941, subject name:

CN=vpnEngineerClientCN

,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-engineer

, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEnginee
Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user
Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50
```

Dies ist ein Beispiel für Debug-Protokolle im Lina-Modul während der VPN-Verbindung vom Manager-Client.

```
<#root>

Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vp
Jun 19 2024 02:01:19: %FTD-6-717022:

Certificate was successfully validated

. serial number: 1AD1B5EAE28C6D3C, subject name:

 CN=vpnManagerClientCN

,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
Jun 19 2024 02:01:19: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-manager
```

```
, Peer certificate: serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN,OU=vpnManagerC
Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user =
Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65
```

Zugehörige Informationen

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.