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.

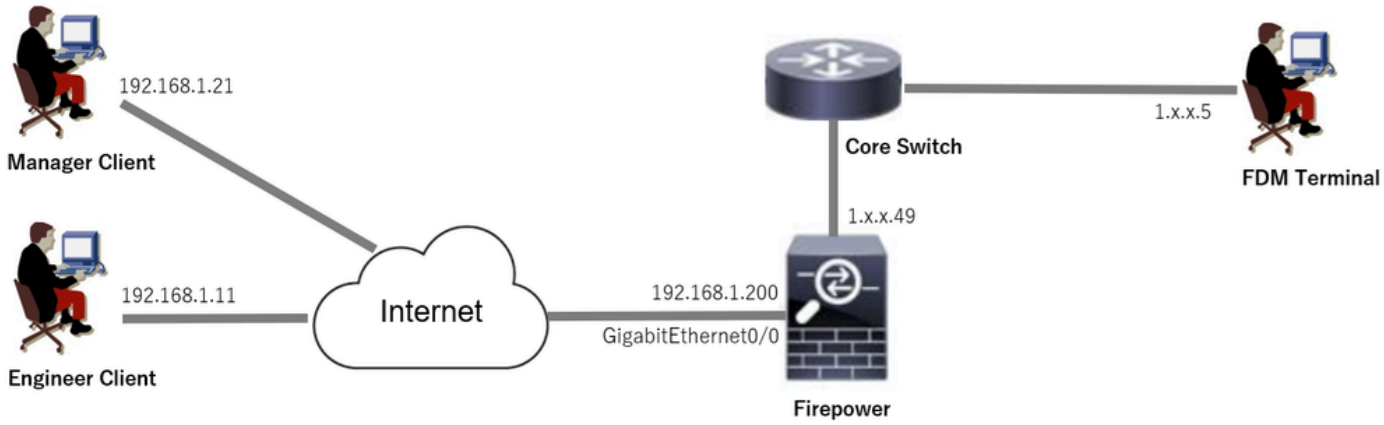
In diesem Dokument wird beschrieben, wie der Cisco Secure Client mithilfe des allgemeinen Namens eines SSL-Zertifikats authentifiziert wird.

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

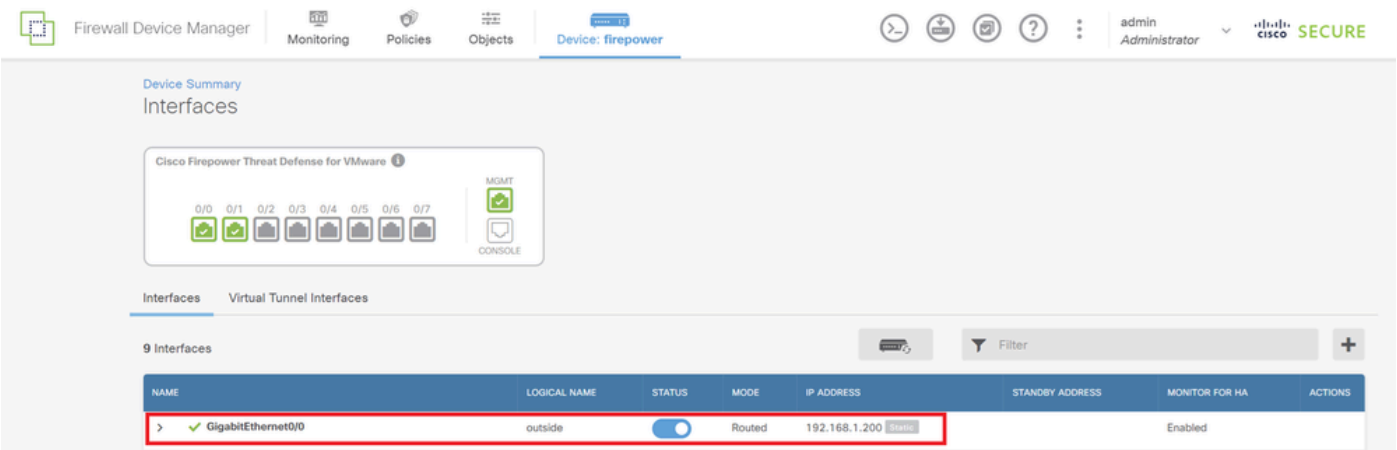
Konfiguration in FDM

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

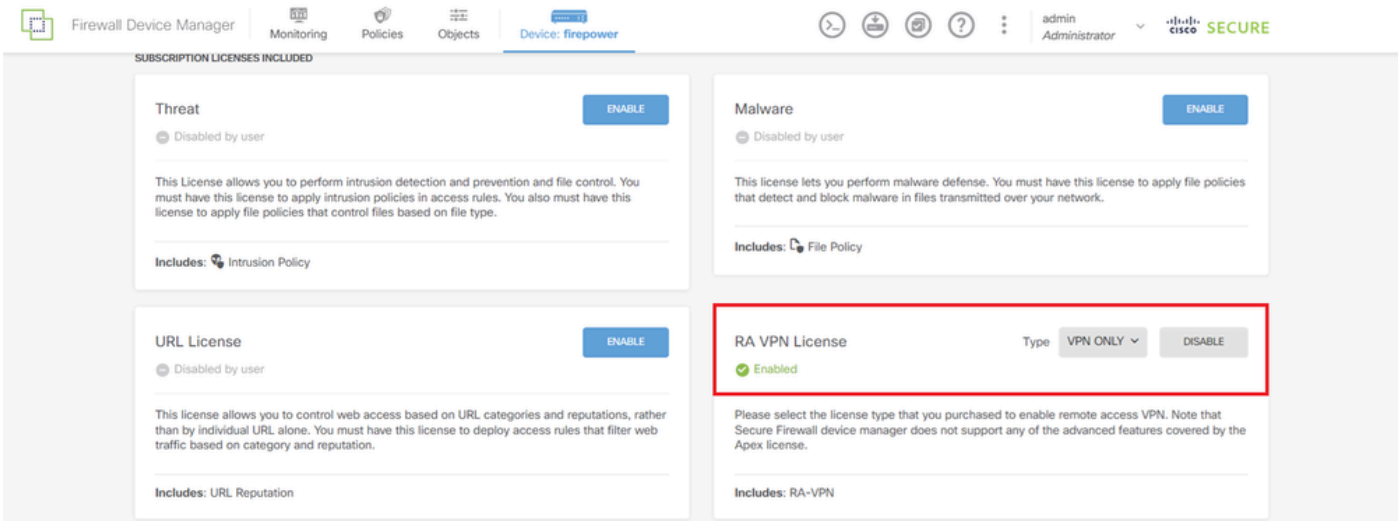
- Name: außen
- IP-Adresse: 192.168.1.200/24



FTD-Schnittstelle

Schritt 2: Cisco Secure Client-Lizenz bestätigen

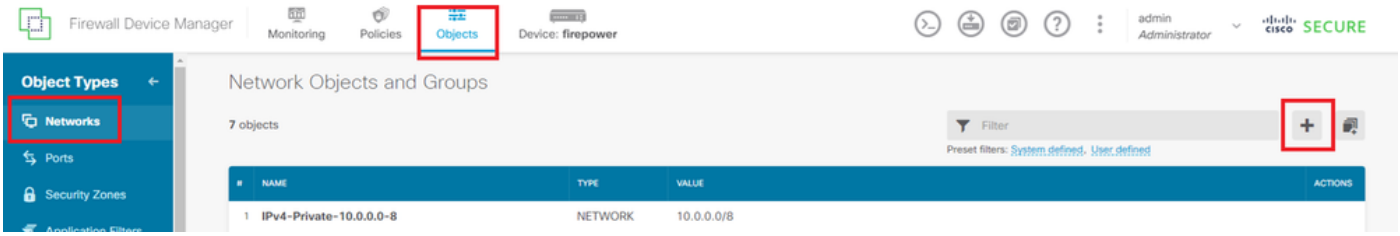
Navigieren Sie zu Device > Smart License > View Configuration, und bestätigen Sie den Artikel Cisco Secure Client License in RA VPN License.



Secure Client-Lizenz

Schritt 3: Adresspool hinzufügen

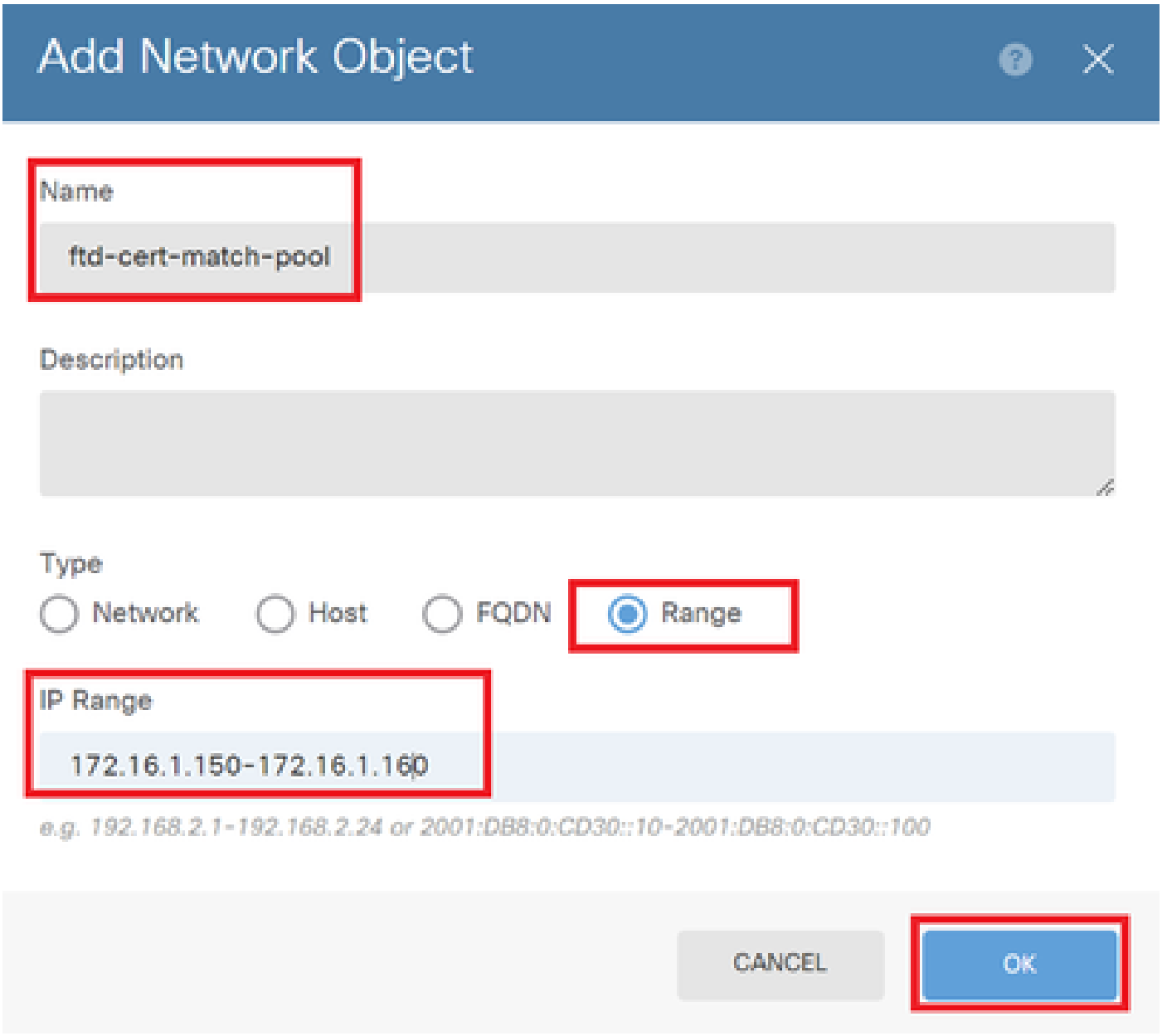
Navigieren Sie zu Objekte > Netzwerke, und klicken Sie auf + Schaltfläche.



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

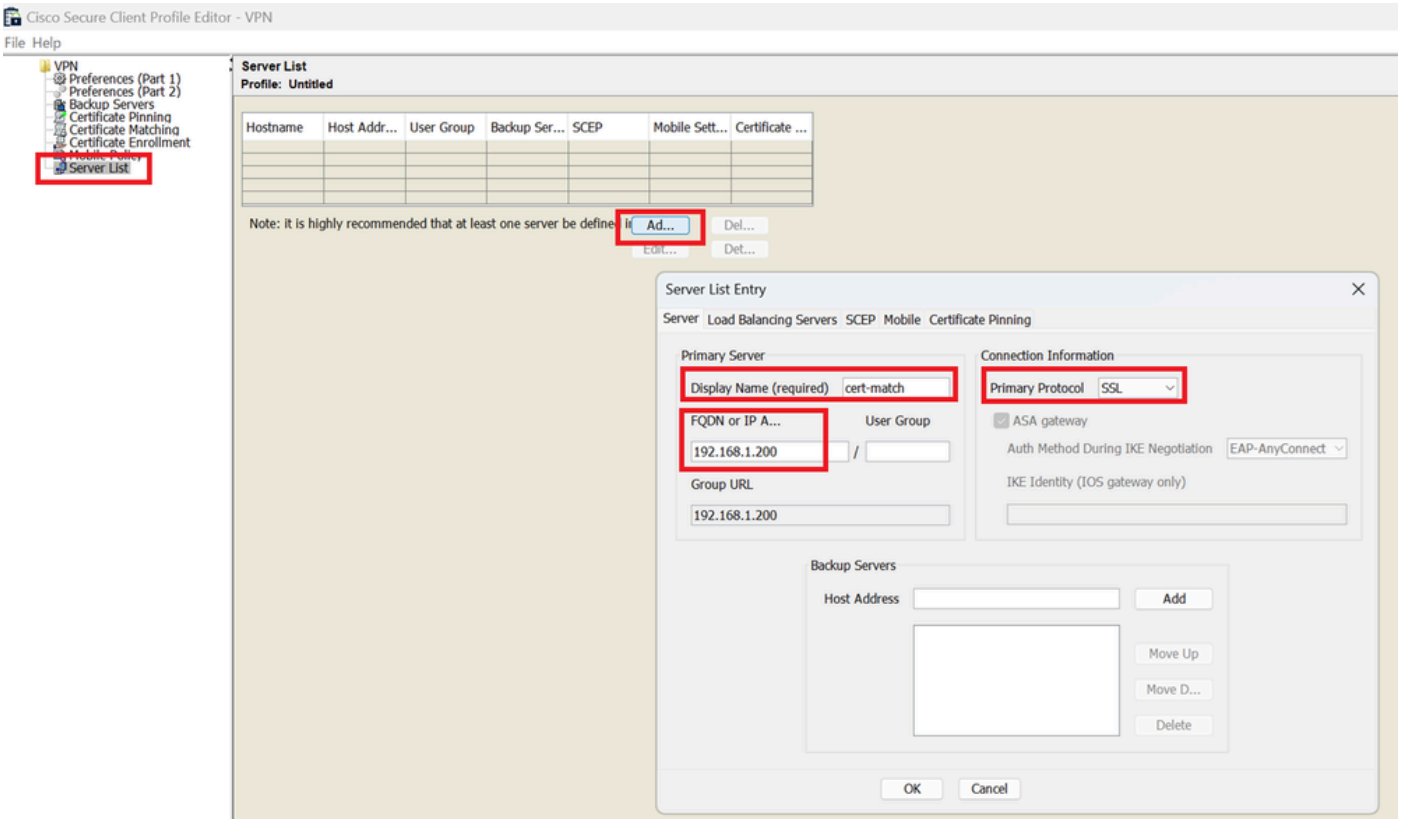


Details zum IPv4-Adresspool

Schritt 4: Sicheres Clientprofil erstellen

Laden Sie den Secure Client Profile Editor von der Cisco Software-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.

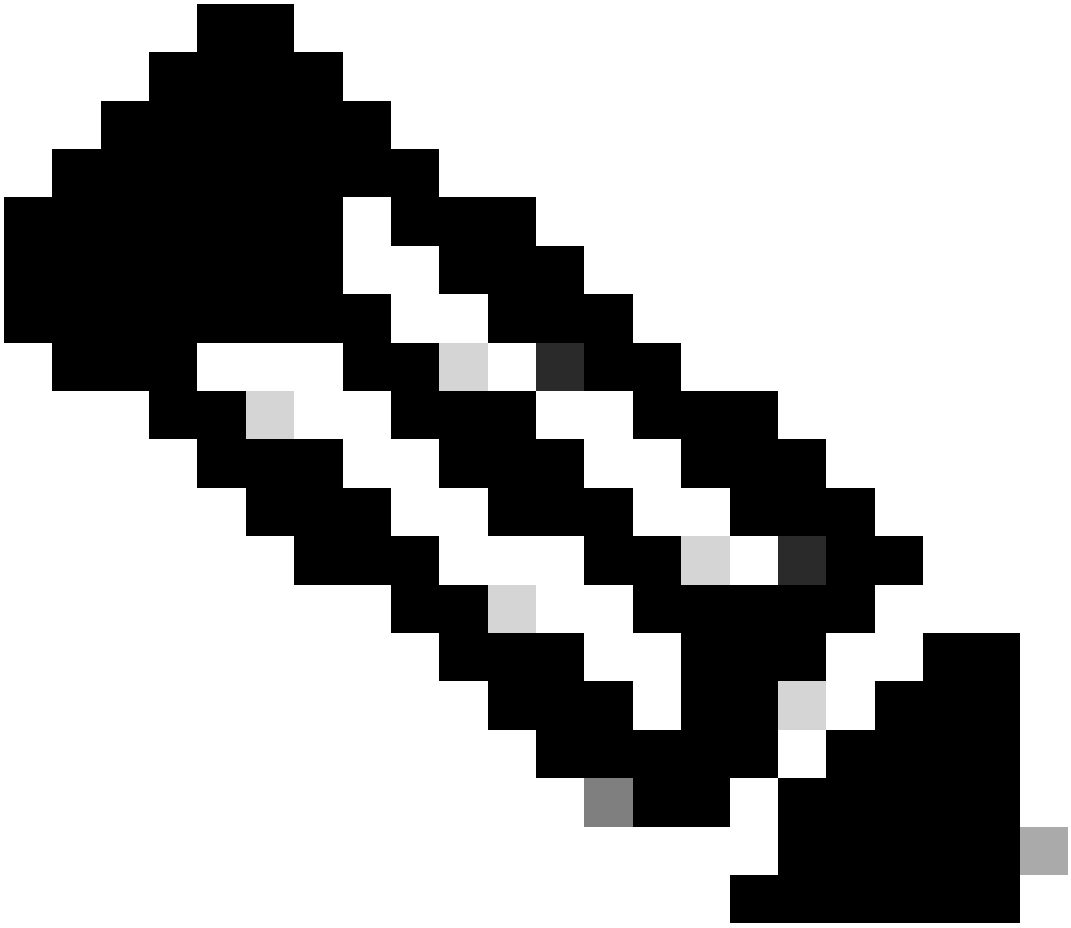
- Anzeigename: Zertifikatübereinstimmung
- FQDN oder IP-Adresse: 192.168.1.200
- Primäres Protokoll: SSL



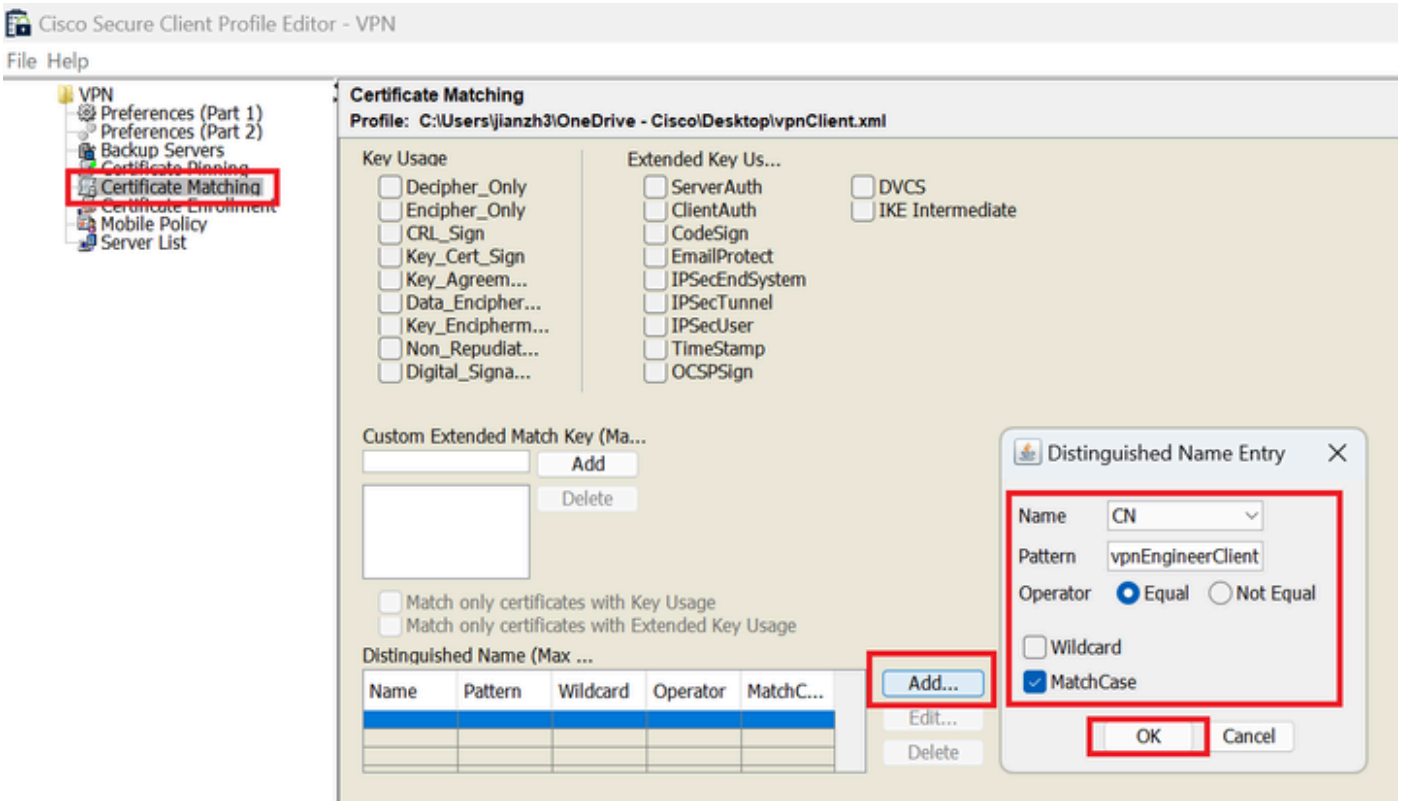
Server-Listeneintrag

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.



Distinguished Name-Eintrag

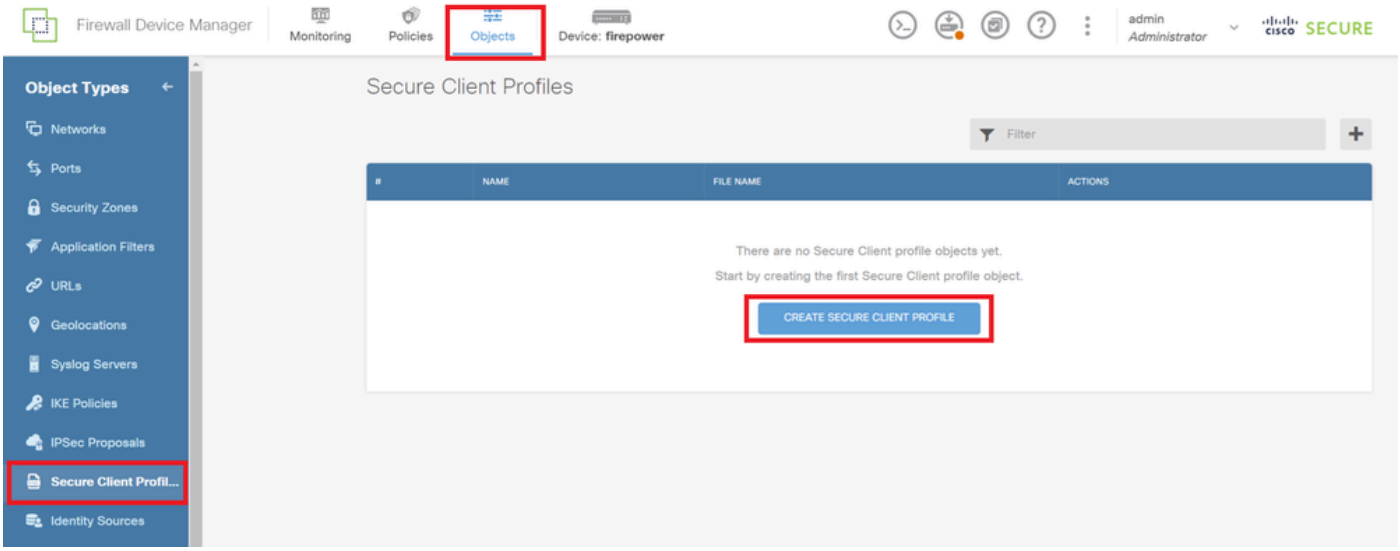
Speichern Sie das sichere Clientprofil auf dem lokalen Computer, und bestätigen Sie die Profildetails.

```
<CertificateMatch>
  <MatchOnlyCertsWithKU>false</MatchOnlyCertsWithKU>
  <DistinguishedName>
    <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
      <Name>CN</Name>
      <Pattern>vpnEngineerClientCN</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
<EnableAutomaticServerSelection UserControllable="false">
  false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>cert-match</HostName>
    <HostAddress>192.168.1.200</HostAddress>
  </HostEntry>
</ServerList>
</AnyConnectProfile>
```

Sicheres Client-Profil

Schritt 5: Hochladen eines sicheren Client-Profils an FDM

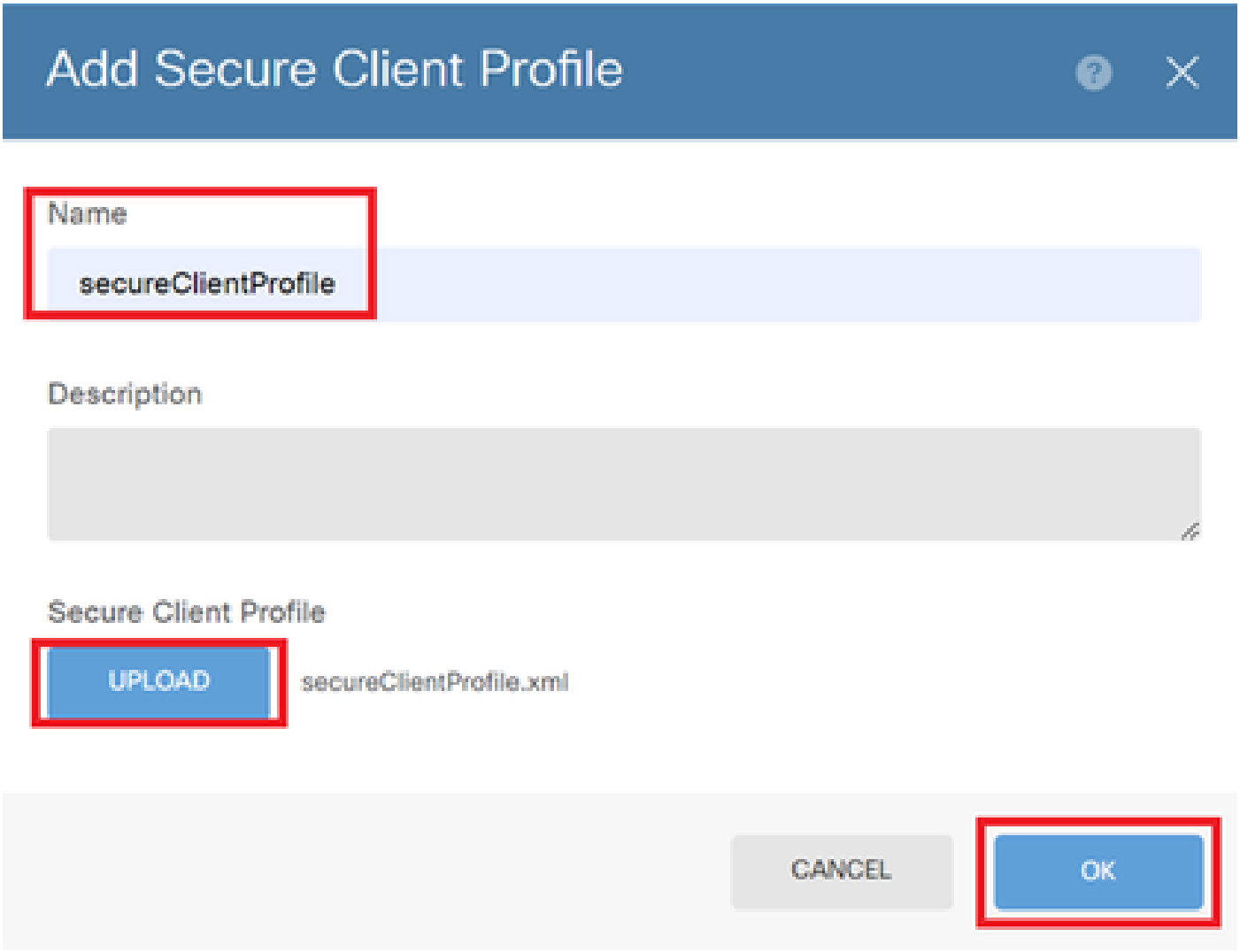
Navigieren Sie zu Objekte > Secure Client Profile, und klicken Sie auf CREATE SECURE CLIENT PROFILE (SICHERES CLIENT-PROFIL ERSTELLEN).



Sicheres Clientprofil erstellen

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

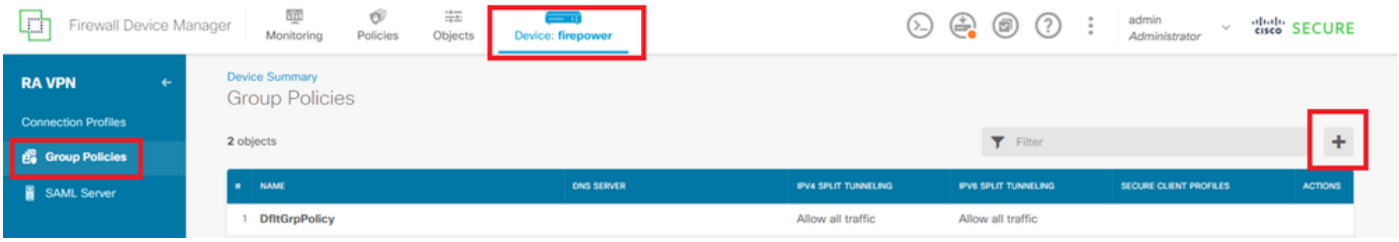
- Name: secureClientProfile
- Sicheres Clientprofil: secureClientProfile.xml (Hochladen vom lokalen Computer)



Sicheres Clientprofil hinzufügen

Schritt 6: Gruppenrichtlinie hinzufügen

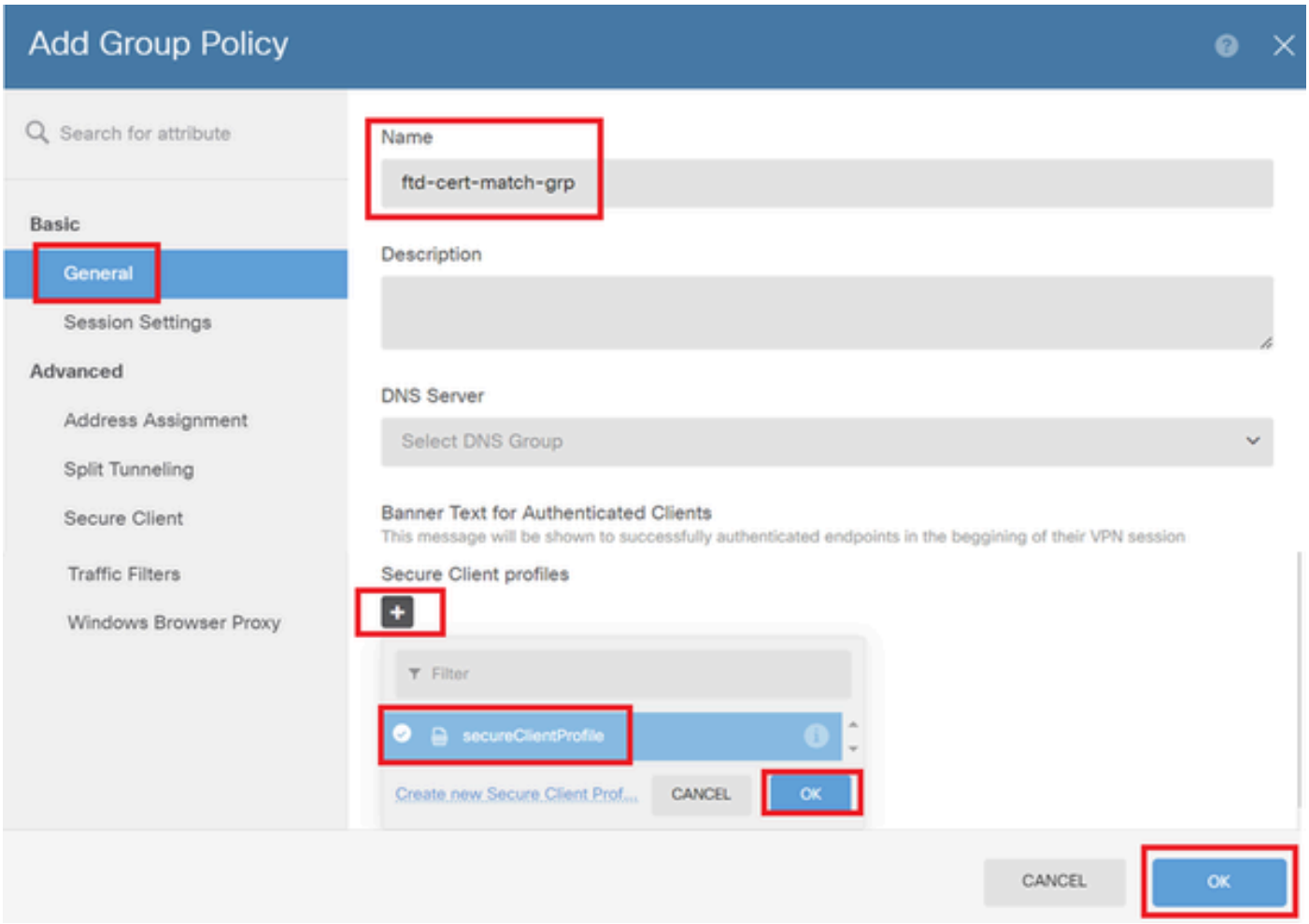
Navigieren Sie zu Gerät > Remotezugriff-VPN > Konfiguration anzeigen > Gruppenrichtlinien, und klicken Sie auf +.



Gruppenrichtlinie hinzufügen

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

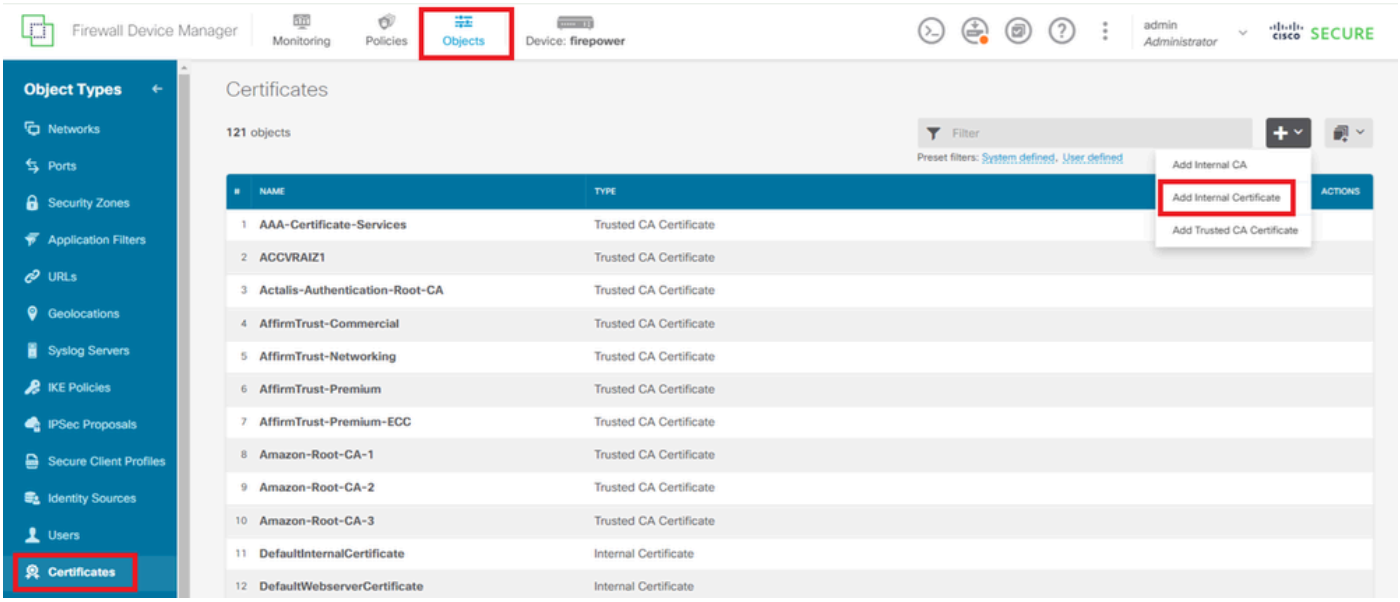
- Name: ftd-cert-match-grp
- Profile für sichere Clients: secureClientProfile



Details zur Gruppenrichtlinie

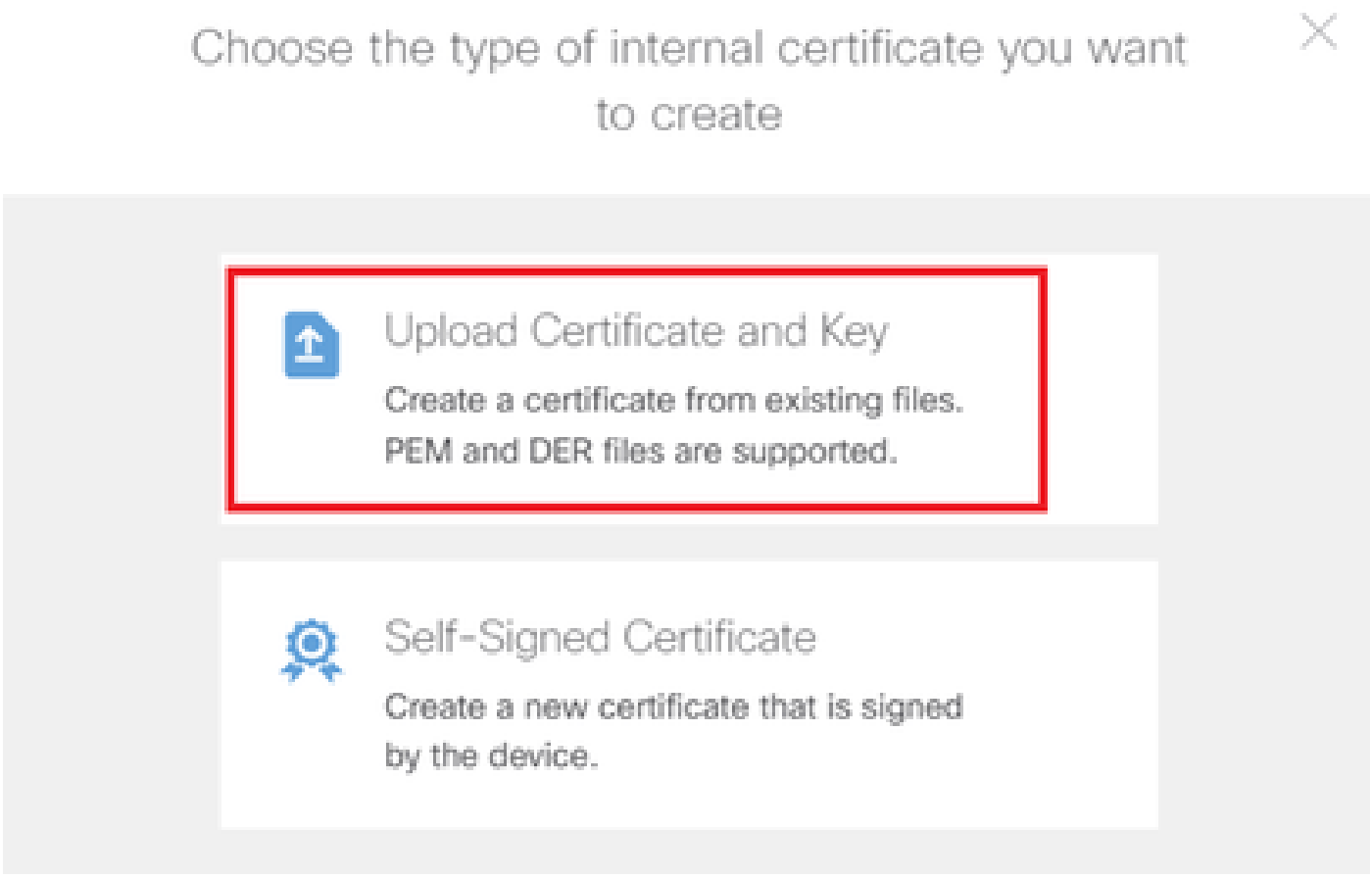
Schritt 7. FTD-Zertifikat hinzufügen

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



Internes Zertifikat hinzufügen

Klicken Sie auf Zertifikat und Schlüssel hochladen.

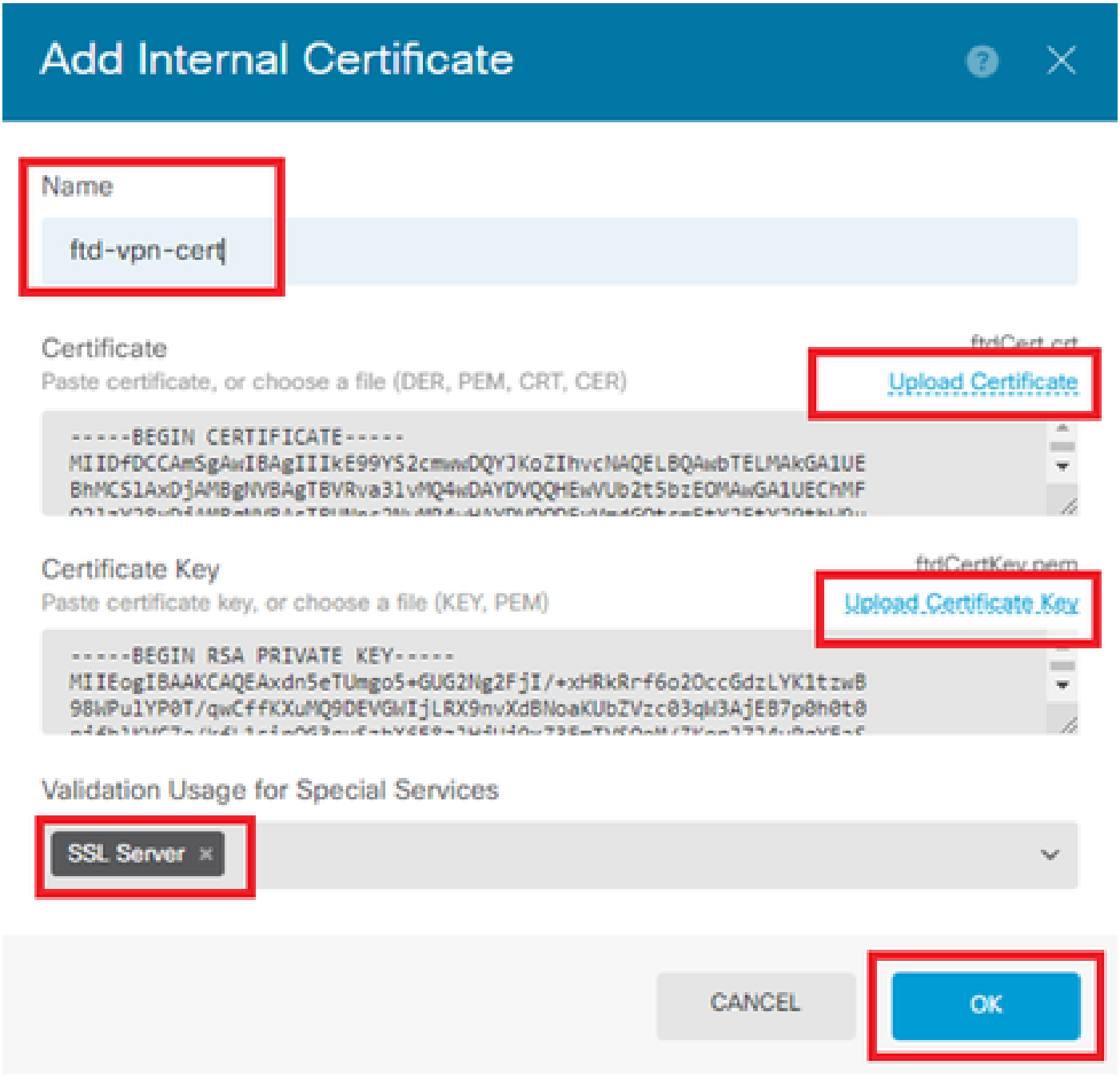


Zertifikat und Schlüssel hochladen

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.

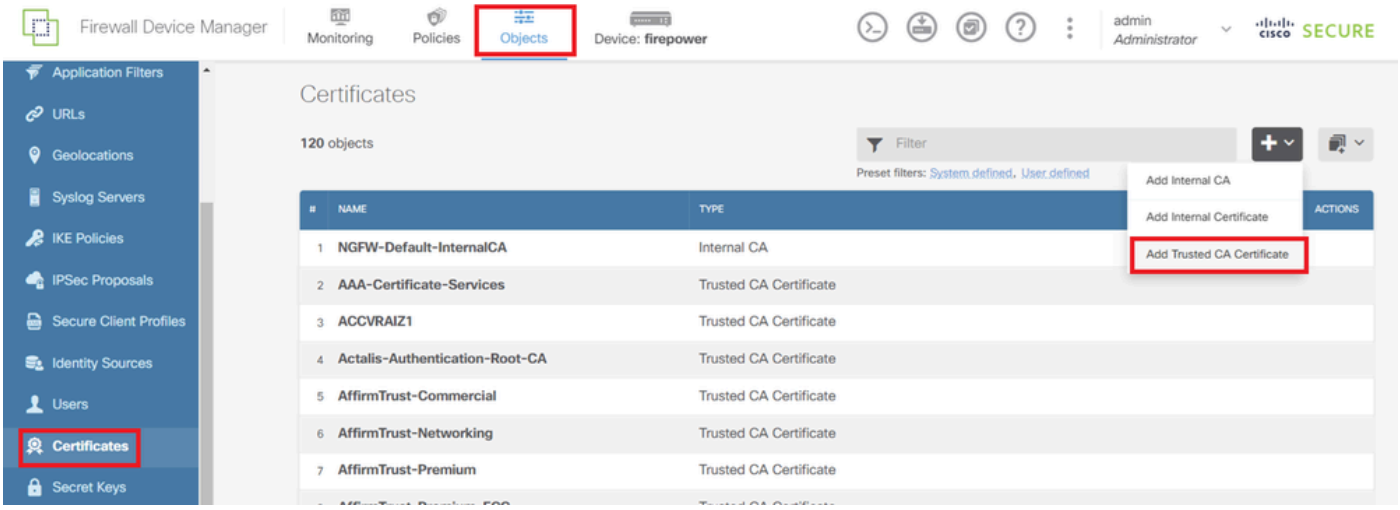
- Name: ftd-vpn-Zertifikat
- Validierungsverwendung für spezielle Services: SSL-Server



Details des internen Zertifikats

Schritt 8: CA zu FTD hinzufügen

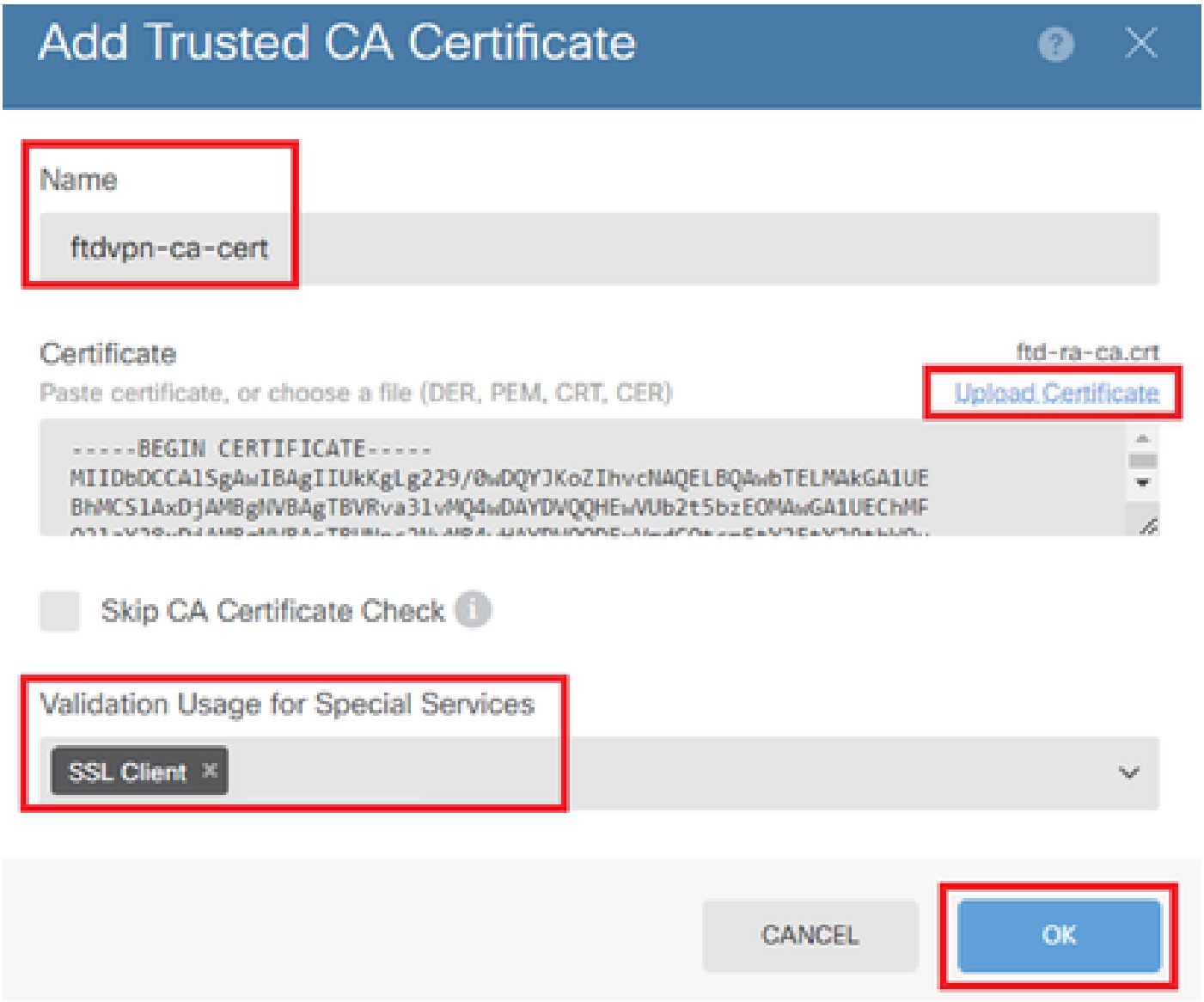
Navigieren Sie zu Objekte > Zertifikate, und klicken Sie auf Vertrauenswürdiges Zertifizierungsstellenzertifikat hinzufügen aus + Element.



Vertrauenswürdiges Zertifizierungsstellenzertifikat hinzufügen

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

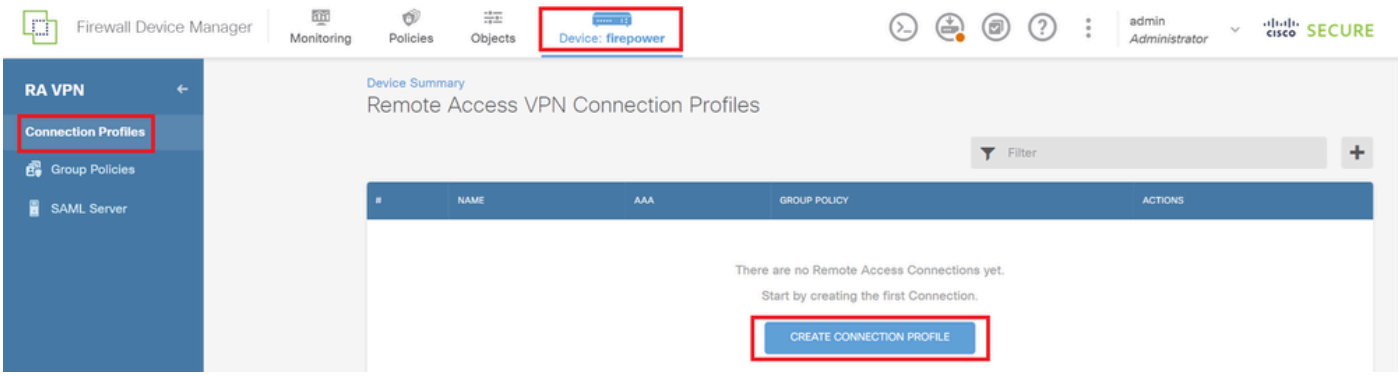
- Name: ftdvpn-ca-cert
- Validierung und Verwendung für spezielle Services: SSL-Client



Details zum vertrauenswürdigen Zertifizierungsstellenzertifikat

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.

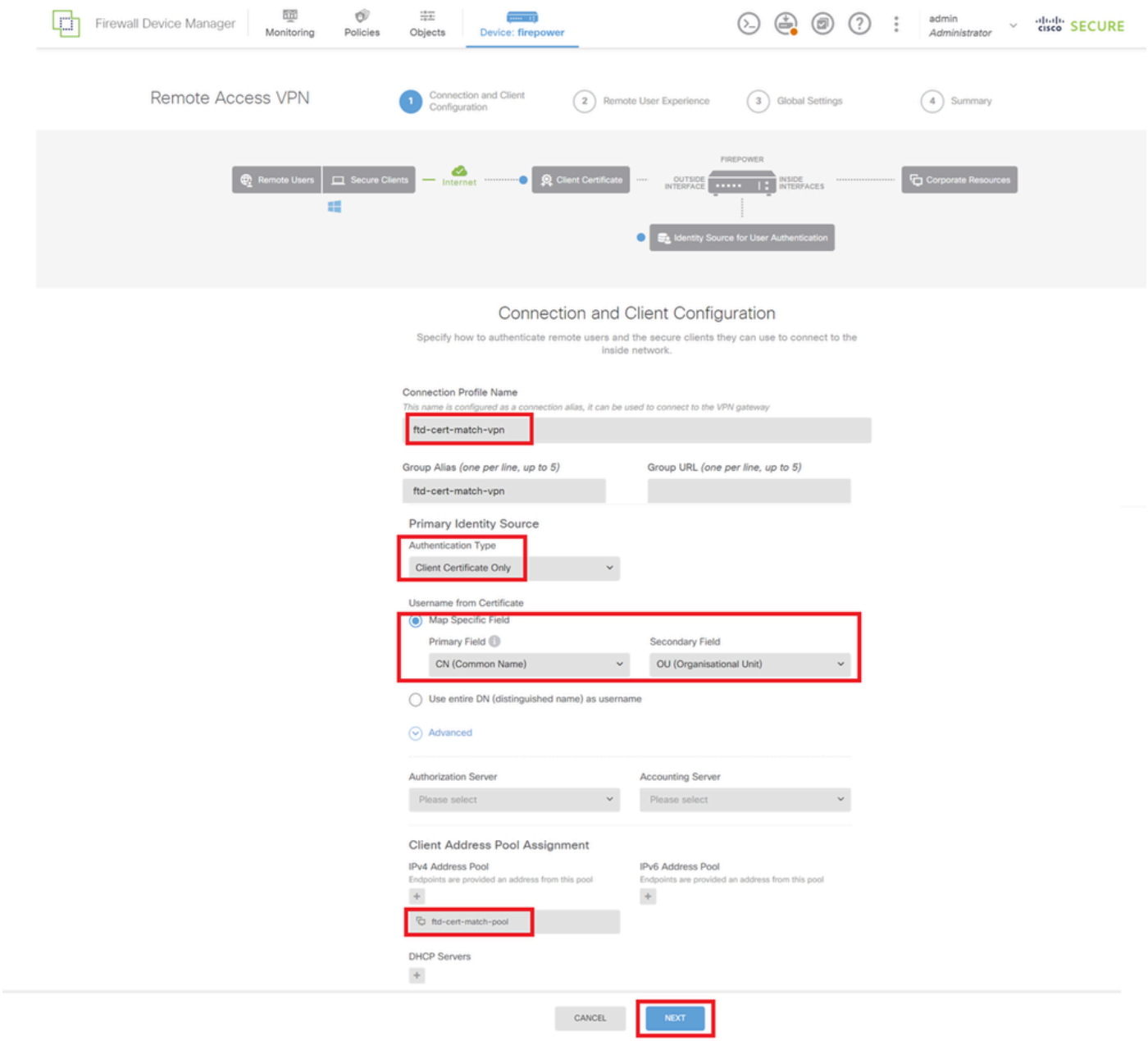


VPN-Verbindungsprofil für Remote-Zugriff hinzufügen

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

Schaltfläche Weiter.

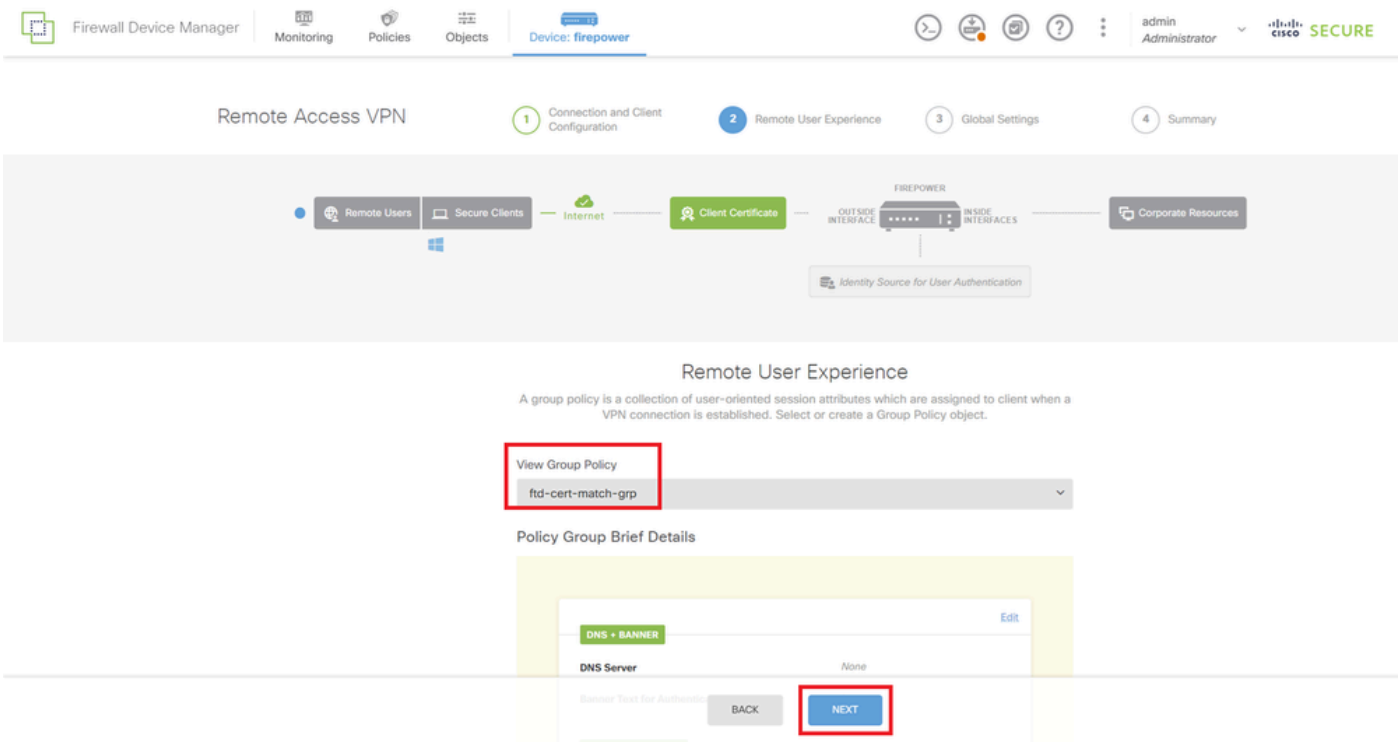
- Name des Verbindungsprofils: ftd-cert-match-vpn
- Authentifizierungstyp: Nur Client-Zertifikat
- Benutzername vom Zertifikat: Zuordnungsspezifisches Feld
- Primärfeld: CN (Common Name)
- Sekundäres Feld: OU (Organisationseinheit)
- IPv4-Adresspools: ftd-cert-match-pool



Details zum VPN-Verbindungsprofil

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

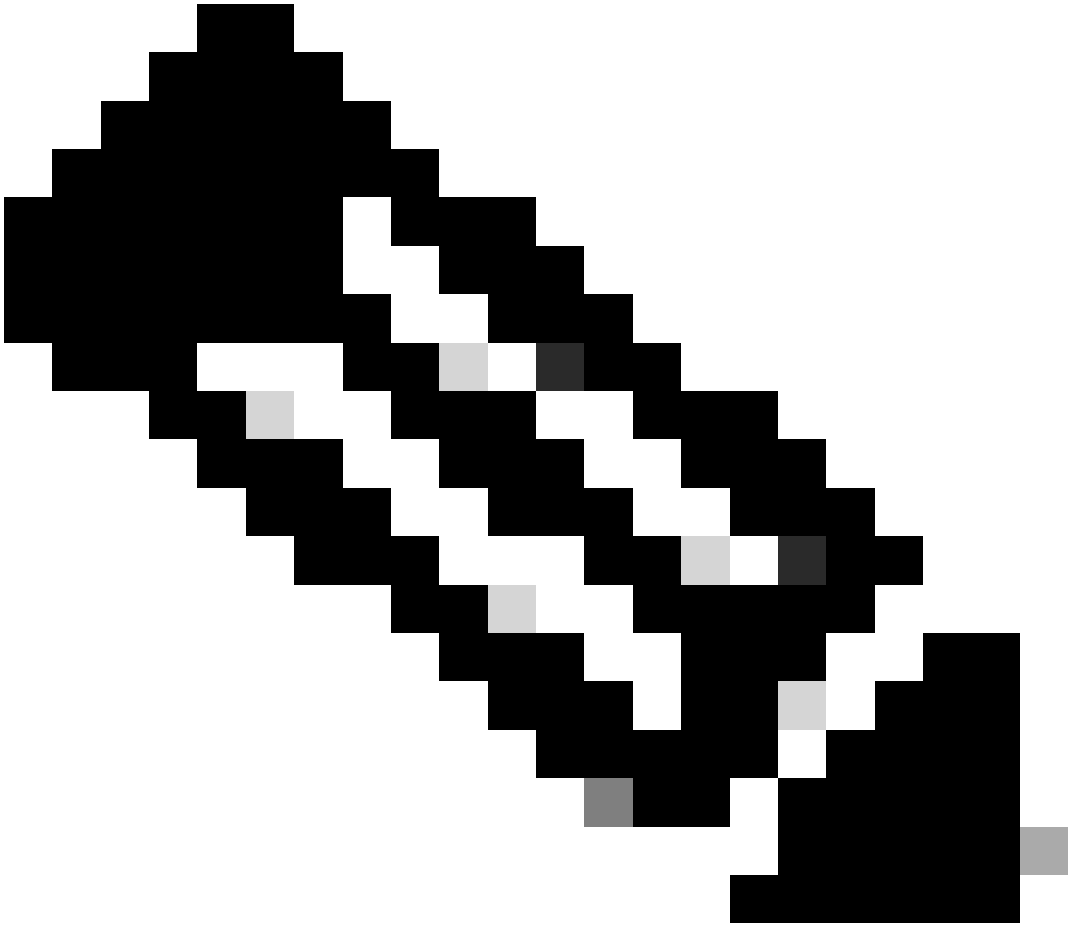
- Gruppenrichtlinie anzeigen: ftd-cert-match-grp



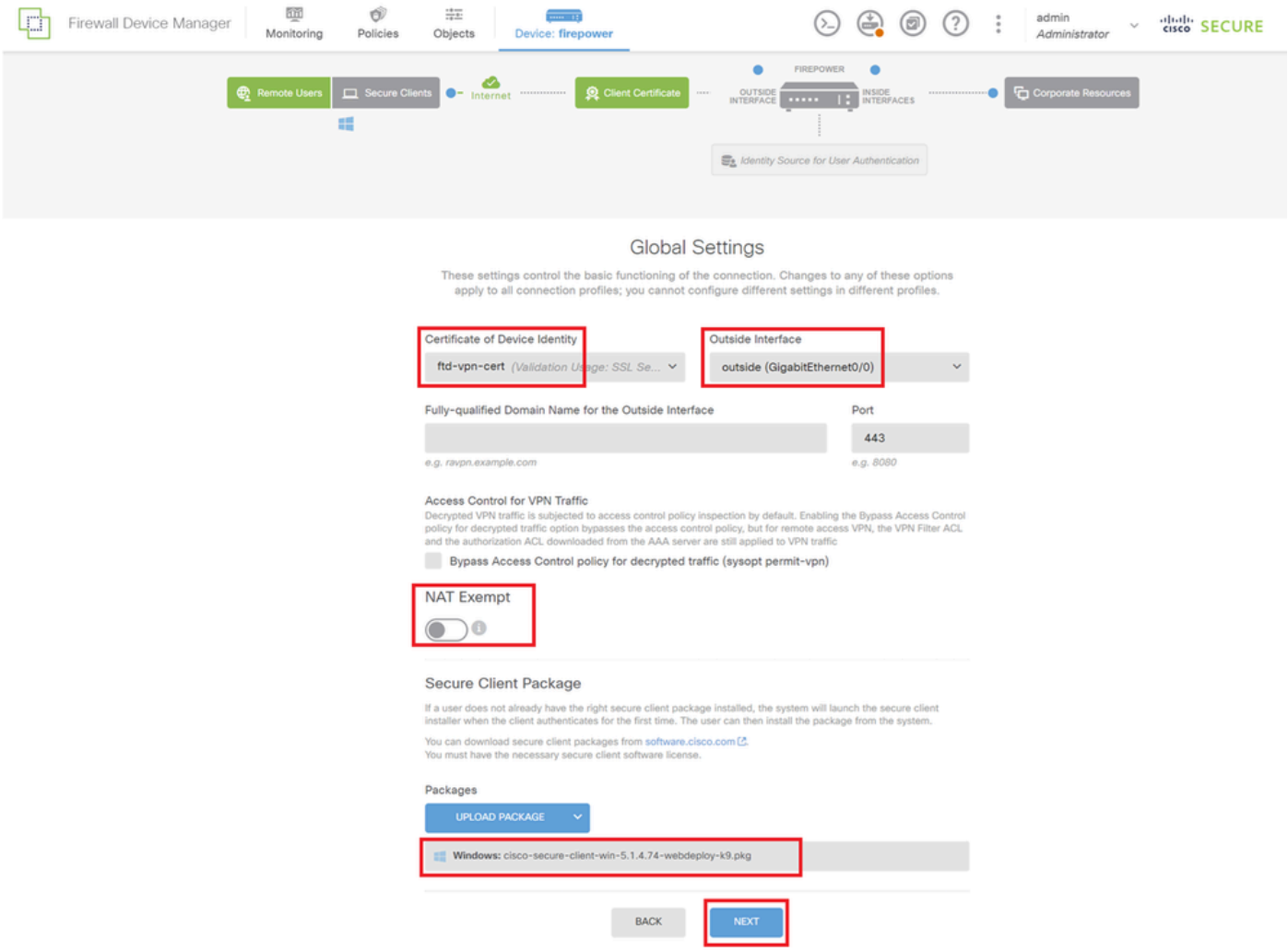
Gruppenrichtlinie auswählen

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



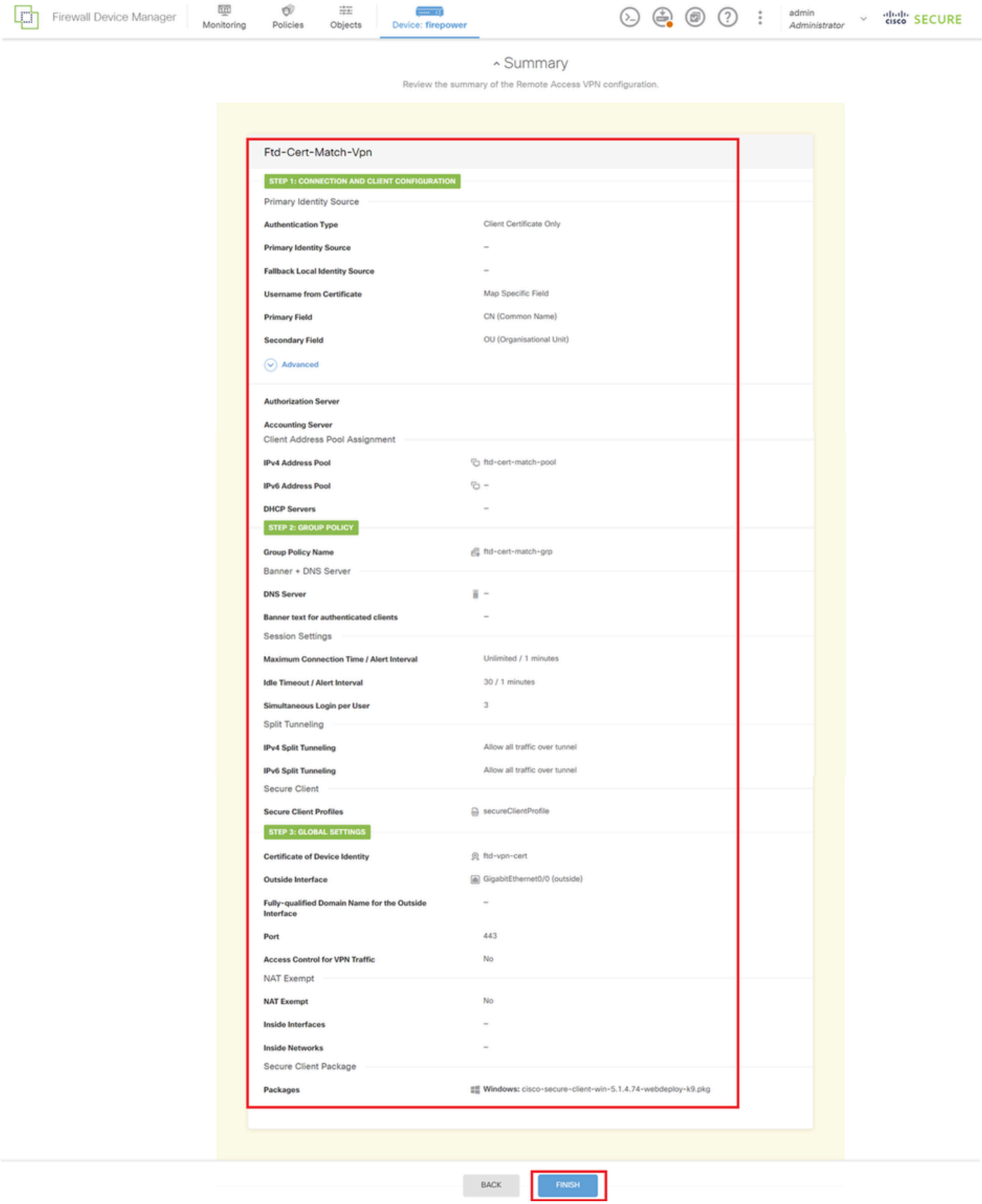
Hinweis: Deaktivieren der Funktion zum Ausschließen von NAT in diesem Dokument.



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.



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
```

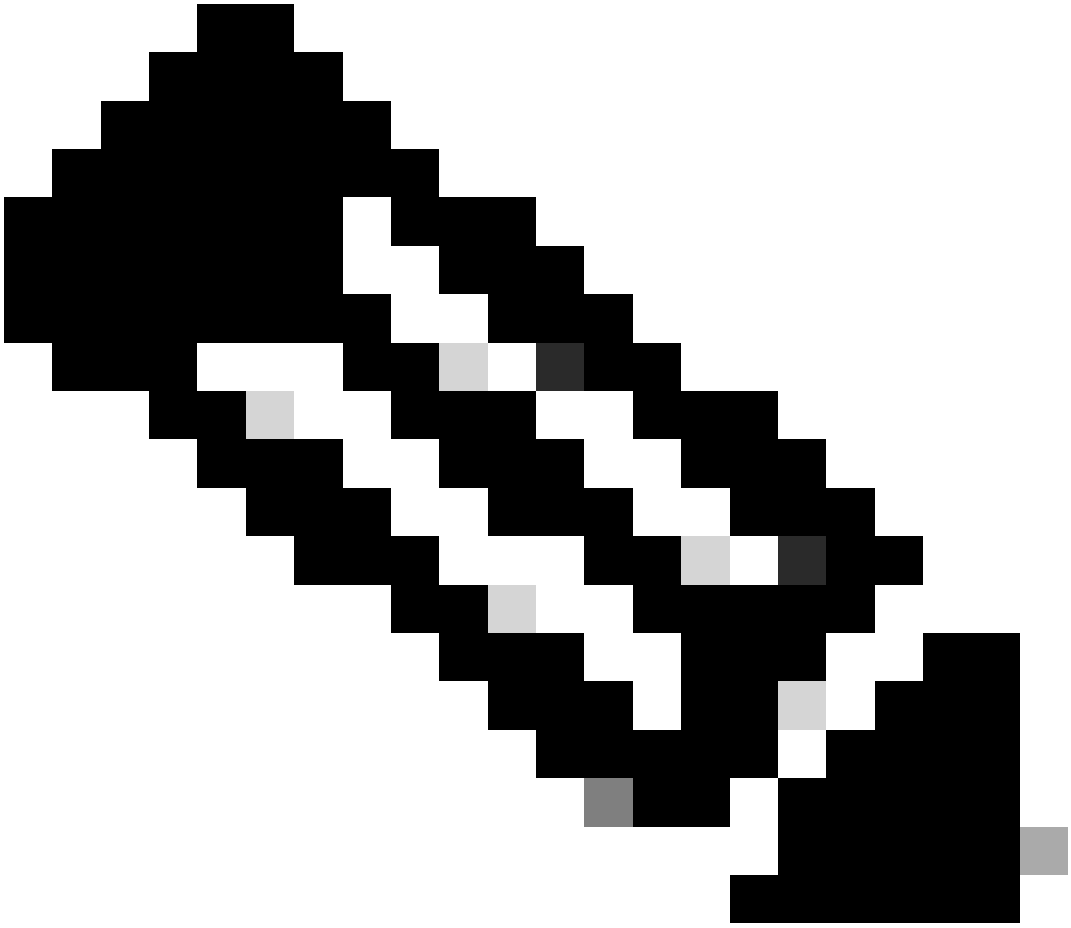
```
// Configures the group-policy to allow SSL connections
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 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
```

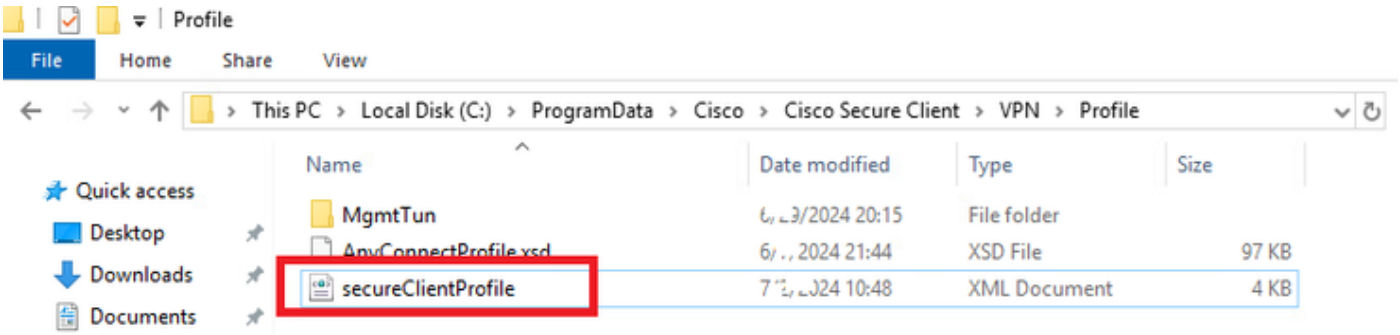
Bestätigung in VPN-Client

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

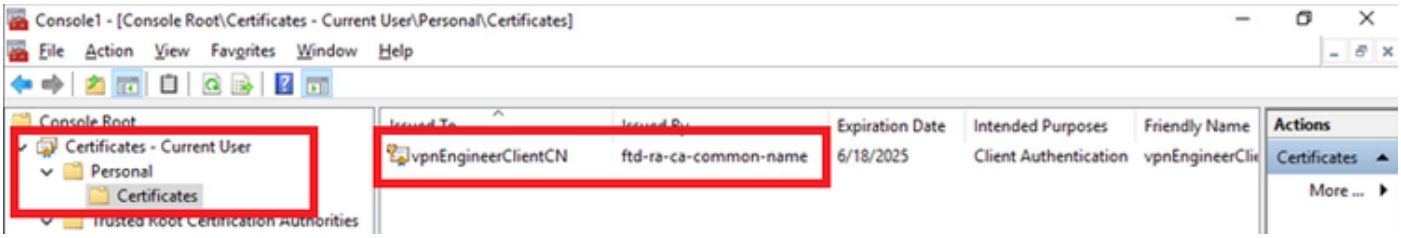


Kopieren des sicheren Clientprofils auf den VPN-Client

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,

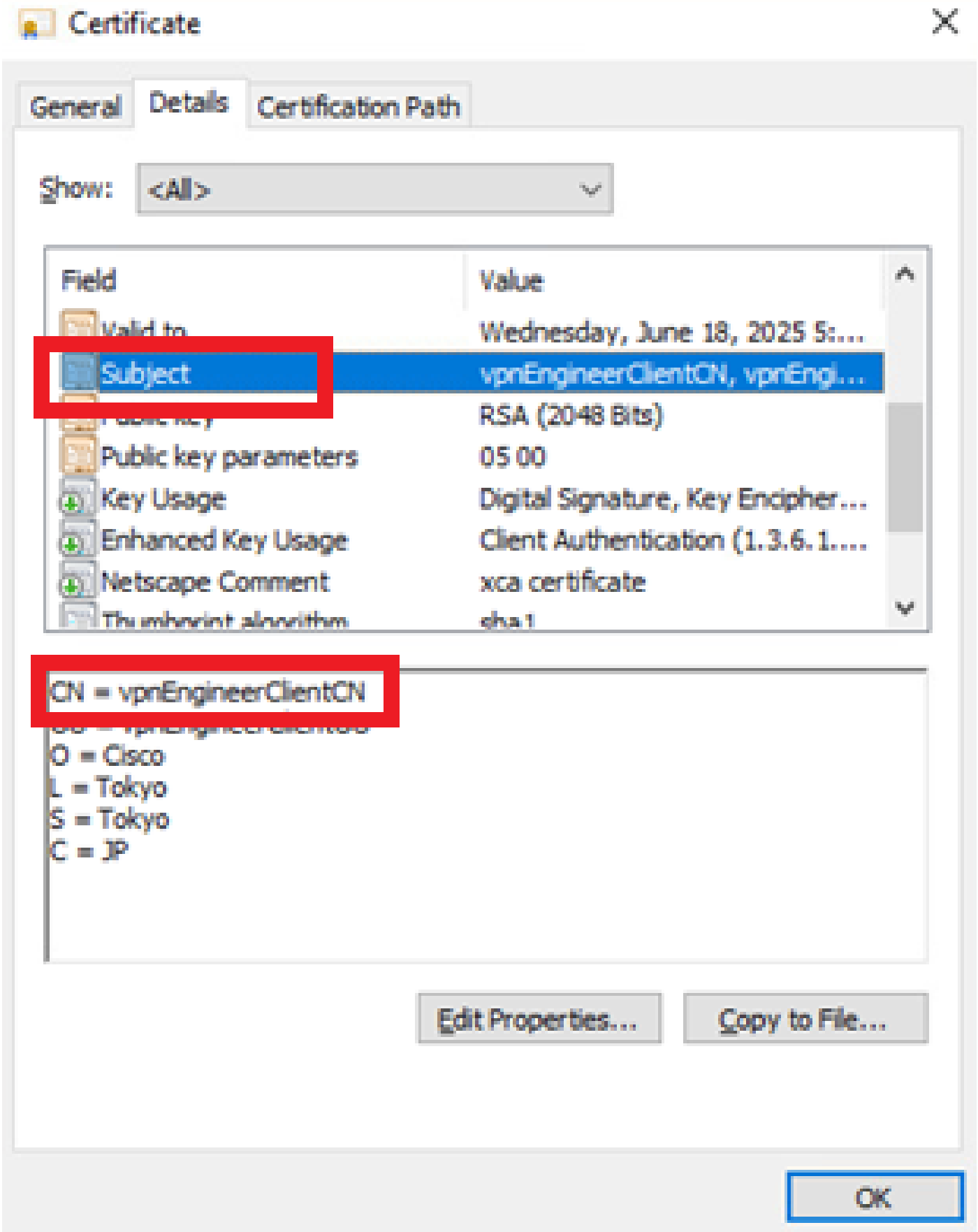
das für die Authentifizierung verwendet wird.



Zertifikat für Techniker-VPN-Client bestätigen

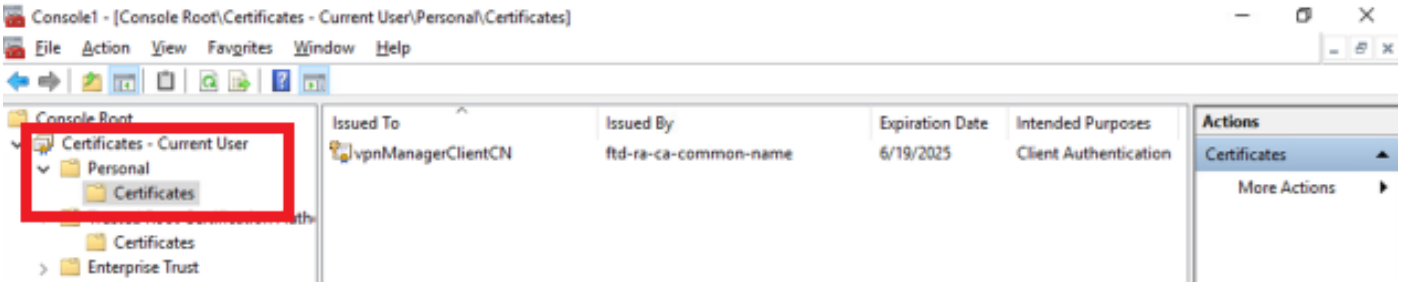
Doppelklicken Sie auf das Client-Zertifikat, navigieren Sie zu Details, überprüfen Sie die Details des Betreffs.

- Betreff: CN = vpnEngineerClientCN



Details zum Techniker-Client-Zertifikat

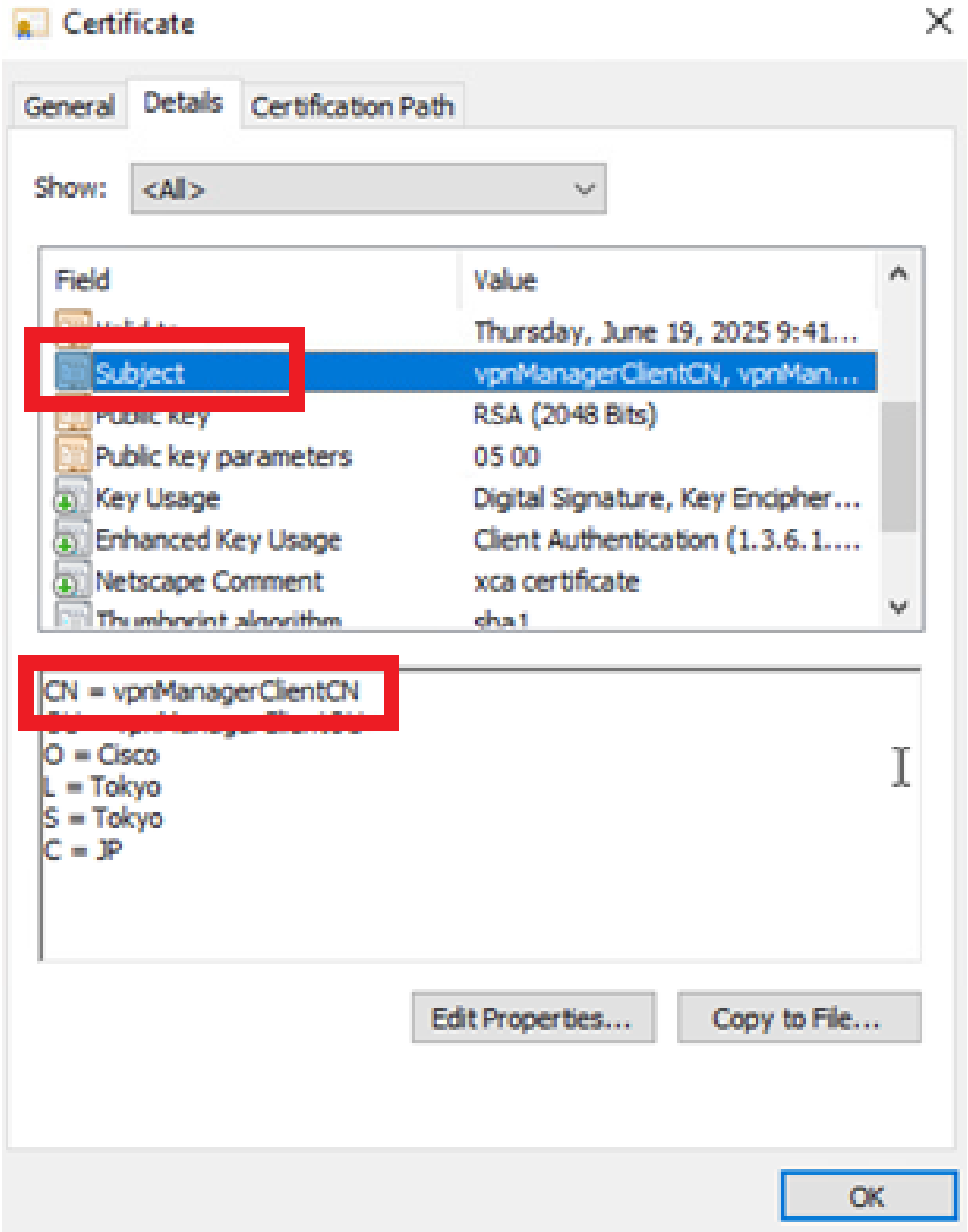
Navigieren Sie im VPN-Client des Managers zu Certificates - Current User > Personal > Certificates, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.



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

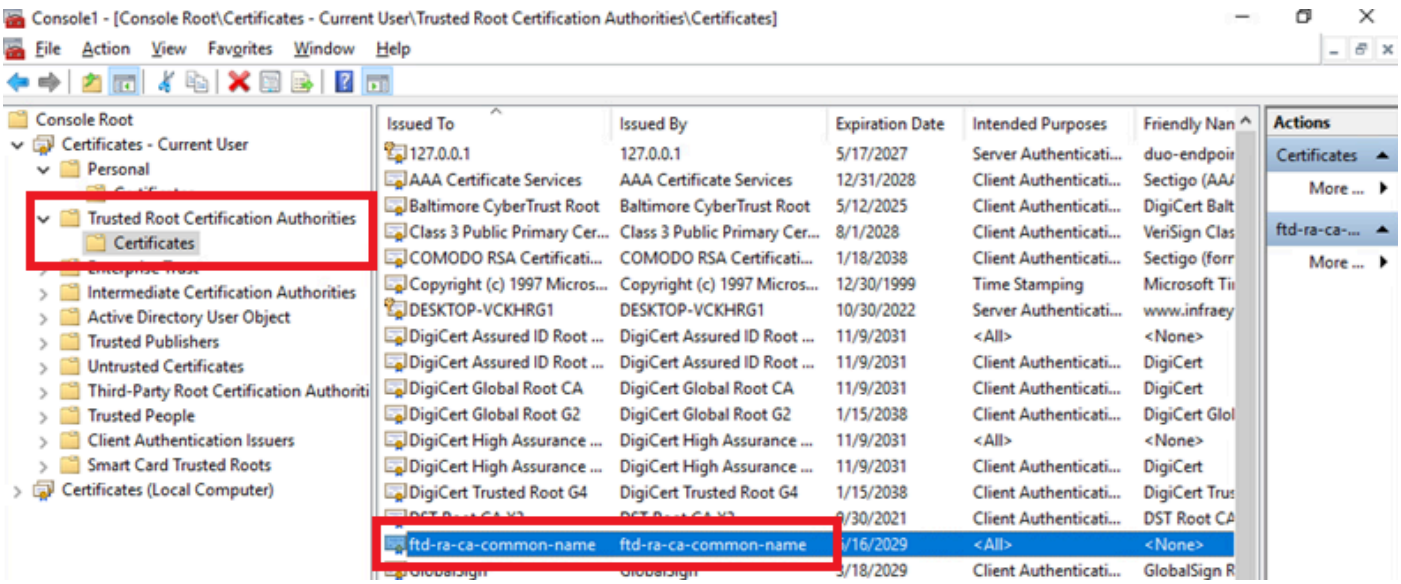


Details zum Manager-Clientzertifikat

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

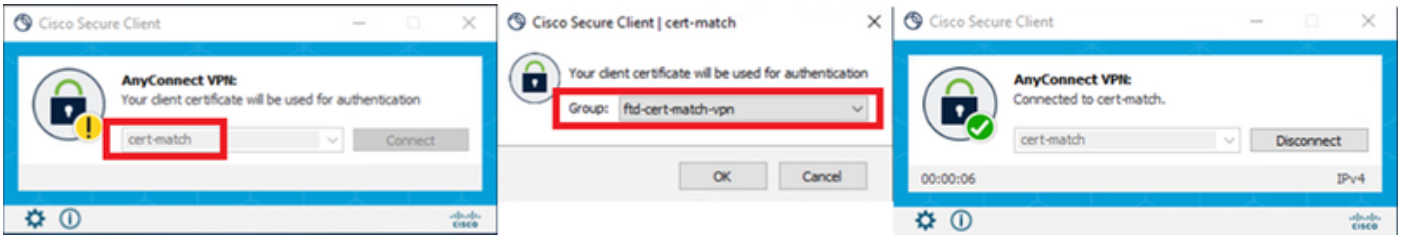


Zertifizierungsstelle bestätigen

Überprüfung

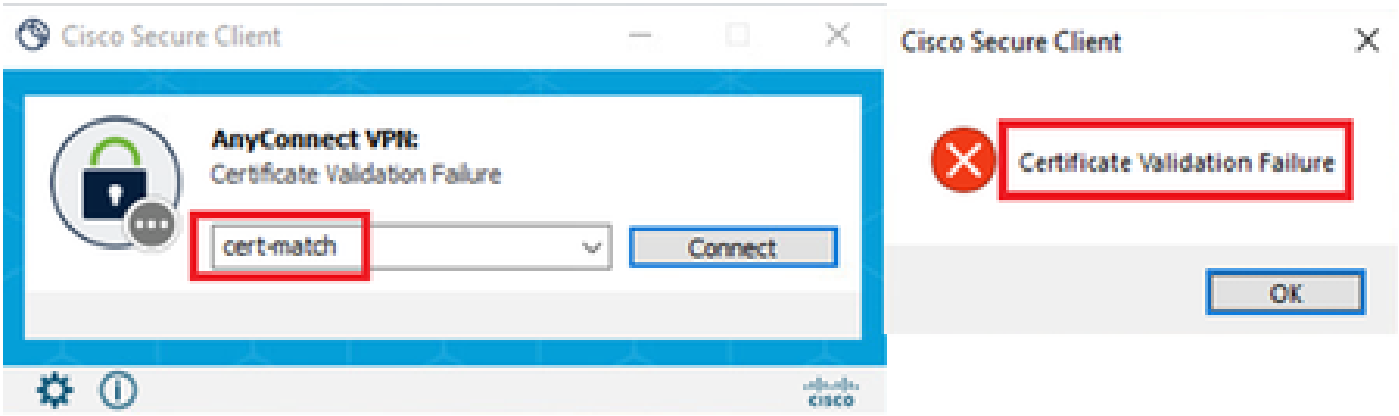
Schritt 1: VPN-Verbindung initiieren

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 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 aus`show 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 : 0000000000020000668393 2b
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=vpnEngineerClie
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.