Konfigurieren von AAA und Zertifizierungsauthentifizierung für sicheren Client auf FTD über FDM

Inhalt

Einleitung

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

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

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

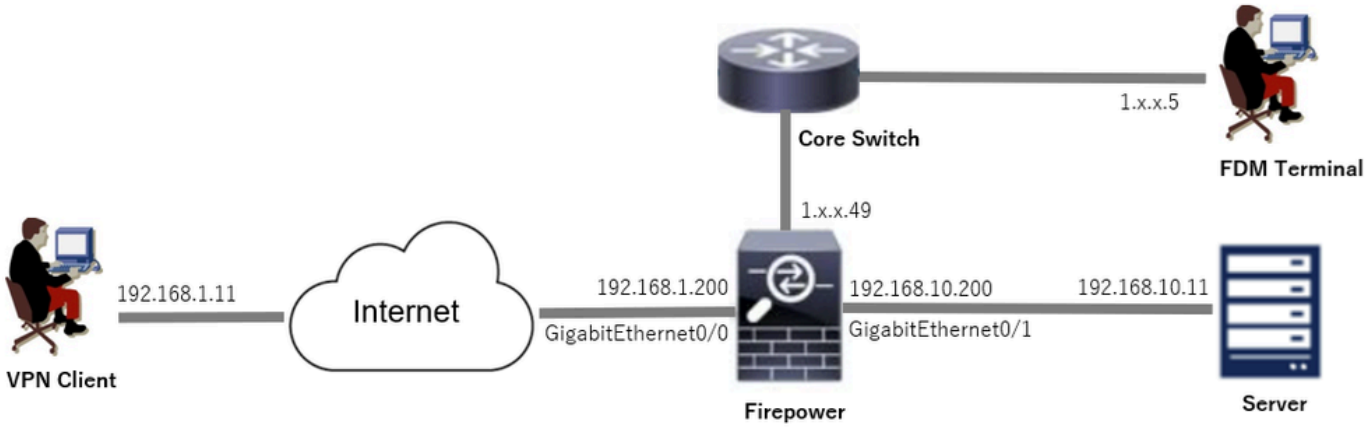
Der FirePOWER Device Manager (FDM) ist eine vereinfachte, webbasierte Management-Schnittstelle zur Verwaltung von Cisco FirePOWER Threat Defense (FTD)-Geräten. Mit dem Firepower Gerätemanager können Netzwerkadministratoren ihre FTD-Geräte konfigurieren und verwalten, ohne das komplexere Firepower Management Center (FMC) verwenden zu müssen. FDM bietet eine intuitive Benutzeroberfläche für grundlegende Aufgaben wie die Einrichtung von Netzwerkschnittstellen, Sicherheitszonen, Zugriffskontrollrichtlinien und VPNs sowie für die Überwachung der Geräteleistung und von Sicherheitsereignissen. Sie eignet sich für kleine bis mittelgroße Bereitstellungen, bei denen eine vereinfachte Verwaltung gewünscht wird.
In diesem Dokument wird beschrieben, wie Sie vordefinierte Benutzernamen in den Cisco Secure Client auf der von FDM verwalteten FTD integrieren.
Wenn Sie FTD mit FMC verwalten, lesen Sie den Leitfaden Konfigurieren von AAA und Zertifizierungsauthentifizierung für sicheren Client auf FTD über FMC.

Dies ist die Zertifikatskette mit dem allgemeinen Namen jedes im Dokument verwendeten Zertifikats.

- 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 FDM

Schritt 1: FTD-Schnittstelle konfigurieren

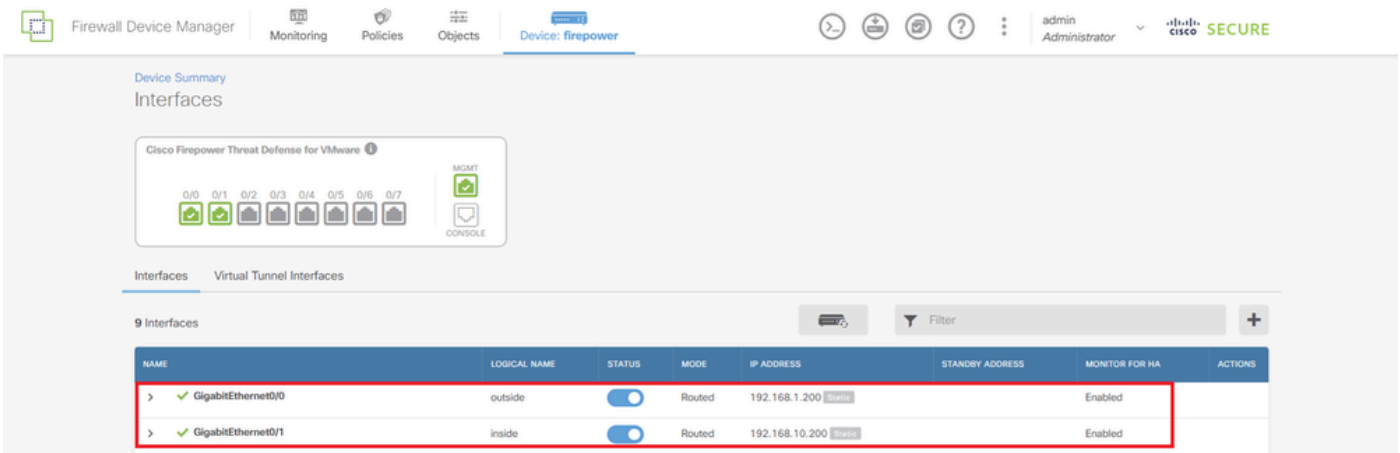
Navigieren Sie zu Device > Interfaces > View All Interfaces (Gerät > Schnittstellen), konfigurieren Sie die interne und externe Schnittstelle für FTD auf der Registerkarte Interfaces (Schnittstellen).

Bei GigabitEthernet0/0

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

Bei GigabitEthernet0/1

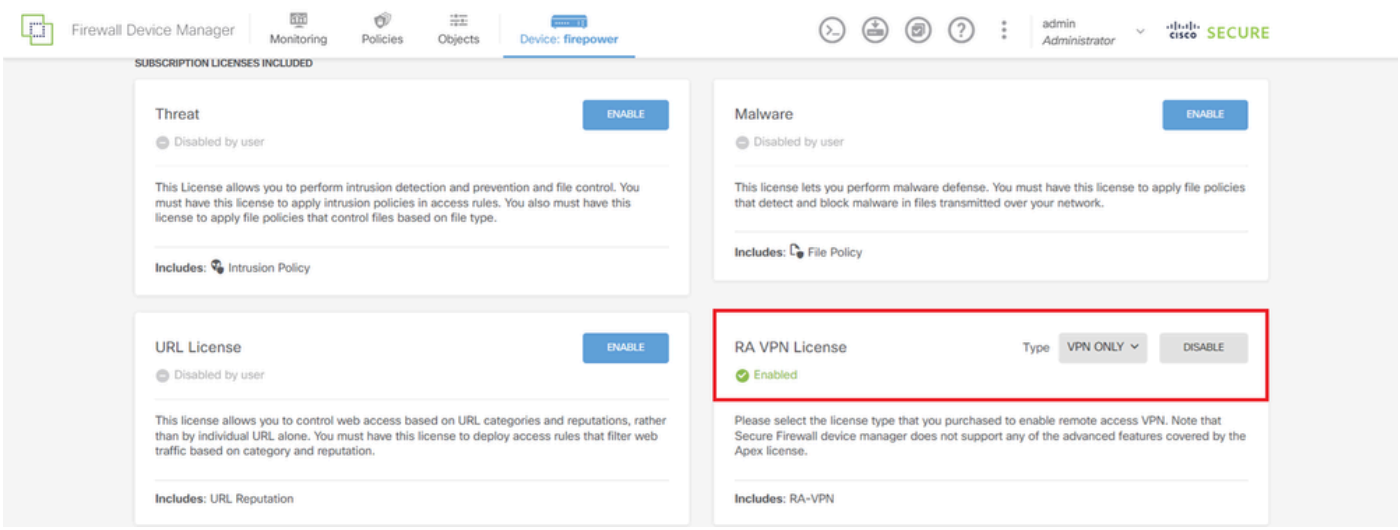
- Name: innen
- IP-Adresse: 192.168.10.200/24



FTD-Schnittstelle

Schritt 2: Cisco Secure Client-Lizenz bestätigen

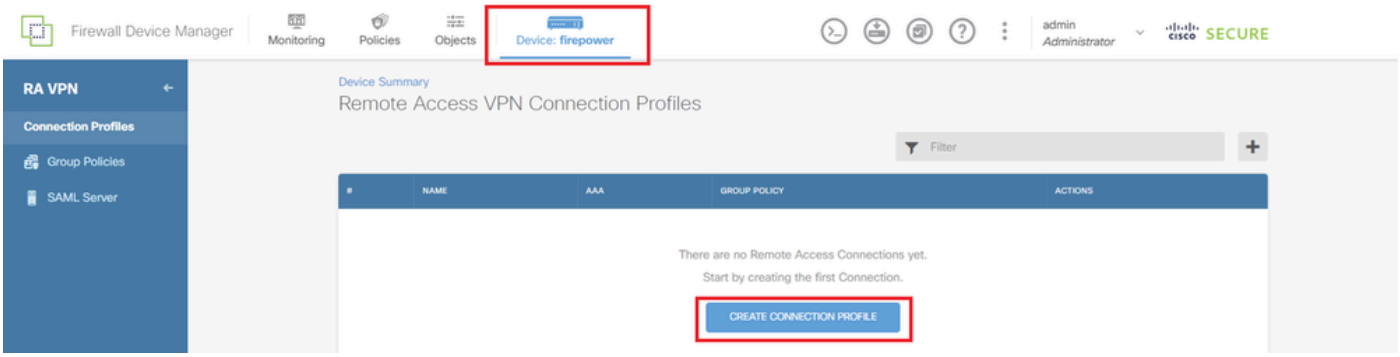
Navigieren Sie zu Device > Smart License > View Configuration, und bestätigen Sie die Cisco Secure Client-Lizenz in RA VPN Licensing.



Secure Client-Lizenz

Schritt 3: VPN-Verbindungsprofil für Remote-Zugriff hinzufügen

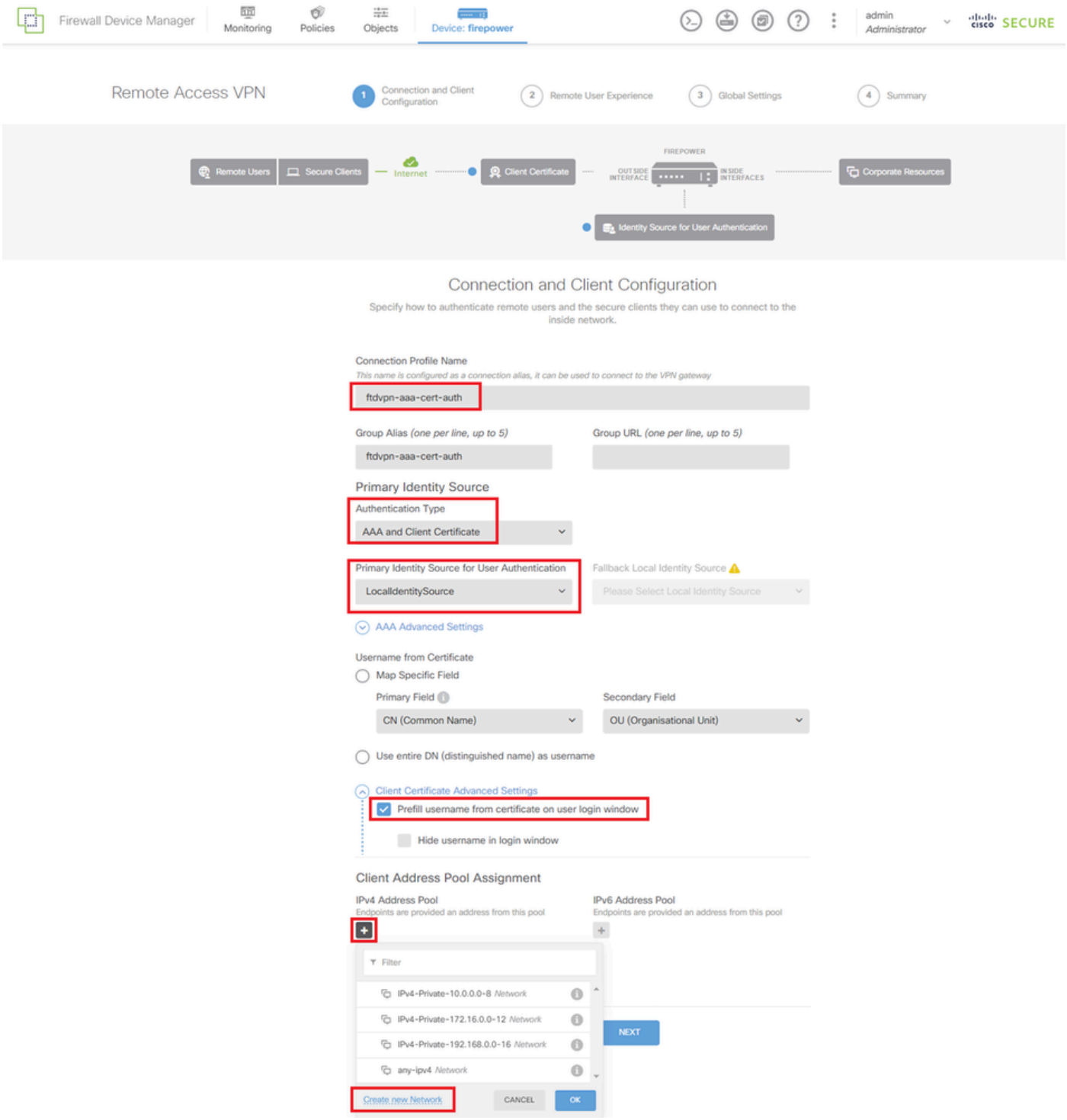
Navigieren Sie zu Gerät > Remotezugriff-VPN > Konfiguration anzeigen, und klicken Sie auf die Schaltfläche VERBINDUNGSPROFIL ERSTELLEN.



VPN-Verbindungsprofil für Remote-Zugriff hinzufügen

Geben Sie die erforderlichen Informationen für das Verbindungsprofil ein, und klicken Sie im IPv4-Adresspool-Element auf die Schaltfläche Create new Network (Neues Netzwerk erstellen).

- Name des Verbindungsprofils: ftdvpn-aaa-cert-auth
- Authentifizierungstyp: AAA- und Client-Zertifikat
- Primäre Identitätsquelle für die Benutzerauthentifizierung: LocalIdentitySource
- Erweiterte Einstellungen für Clientzertifikat: Benutzernamen vom Zertifikat bei Benutzeranmeldung vorab ausfüllen

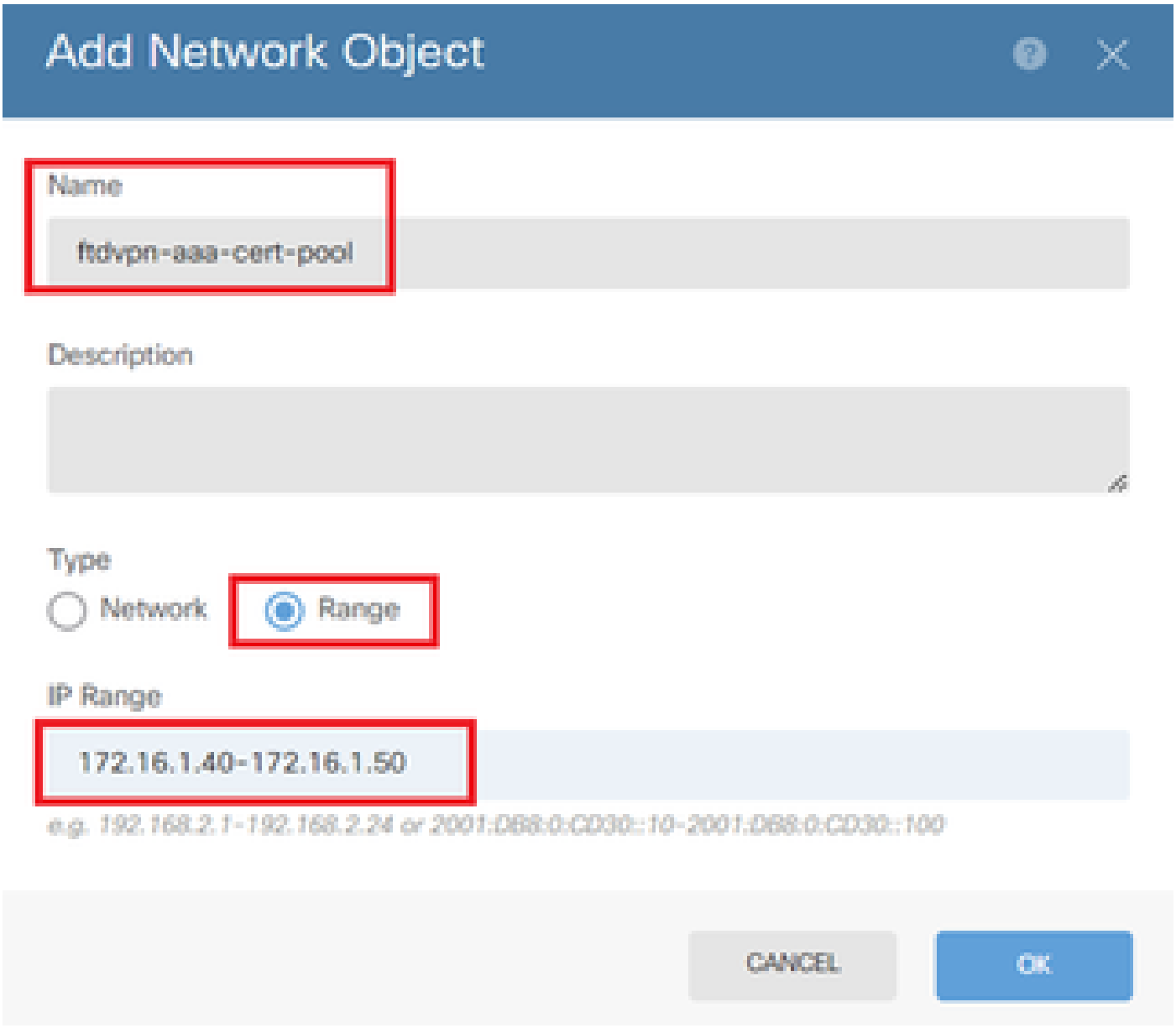


Details zum VPN-Verbindungsprofil

Schritt 4: Adresspool für Verbindungsprofil hinzufügen

Geben Sie die erforderlichen Informationen ein, um einen neuen IPv4-Adresspool hinzuzufügen. Wählen Sie einen neu hinzugefügten IPv4-Adresspool für das Verbindungsprofil aus, und klicken Sie auf die Schaltfläche Weiter.

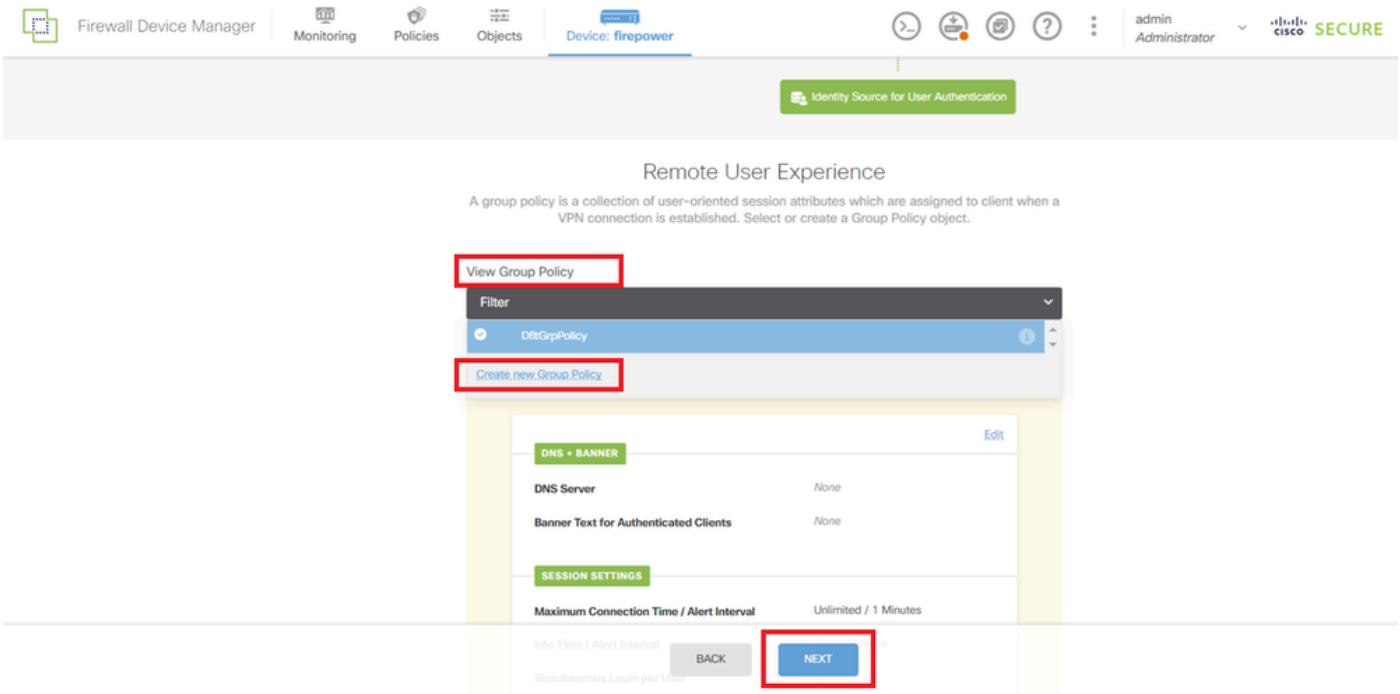
- Name: ftdvpn-aaa-cert-pool
- Typ: Bereich
- IP-Bereich: 172.16.1.40-172.16.1.50



Details zum IPv4-Adresspool

Schritt 5: Gruppenrichtlinie für Verbindungsprofil hinzufügen

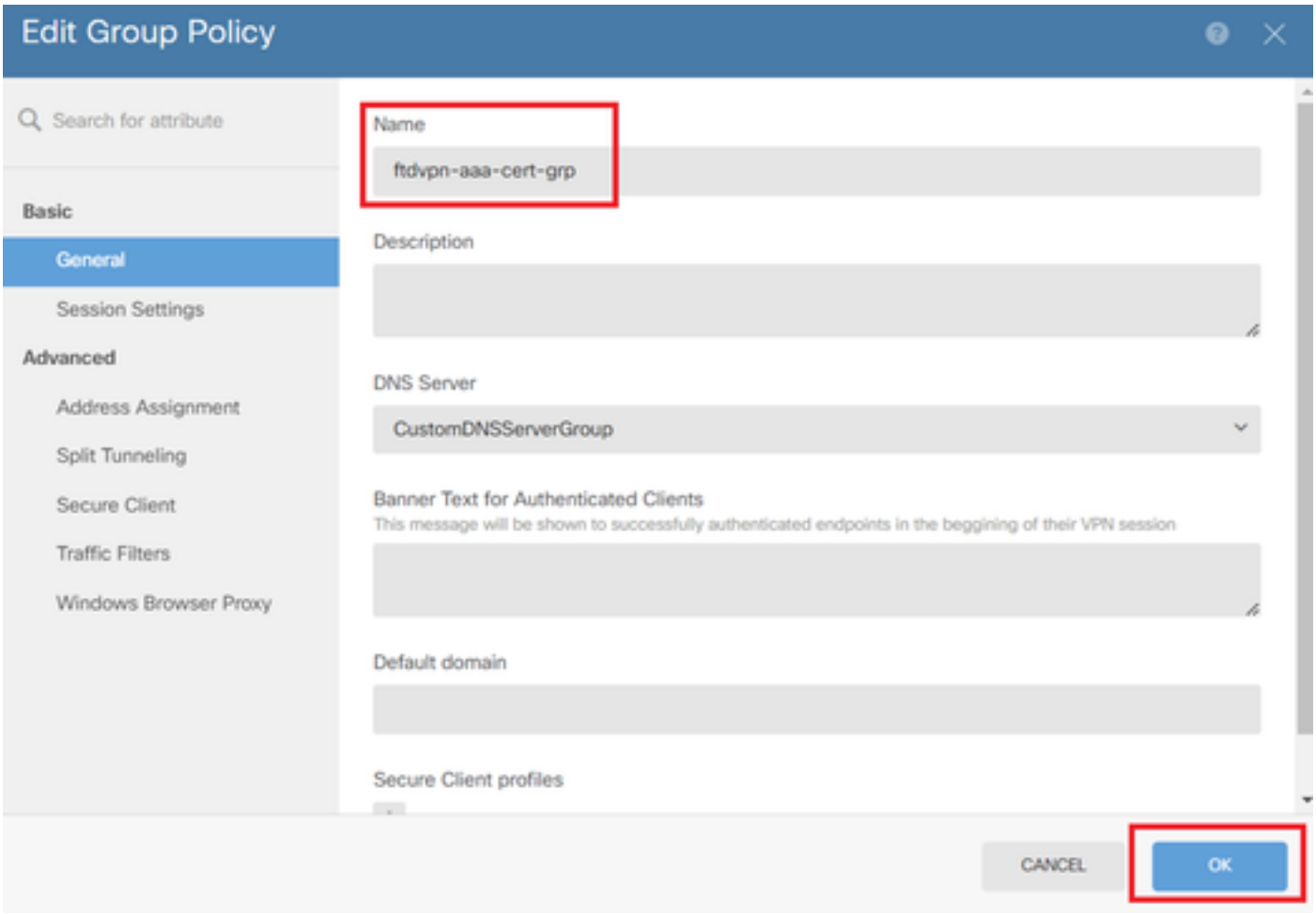
Klicken Sie im Element Gruppenrichtlinie anzeigen auf Neue Gruppenrichtlinie erstellen.



Gruppenrichtlinie hinzufügen

Geben Sie die erforderlichen Informationen ein, um eine neue Gruppenrichtlinie hinzuzufügen, und klicken Sie auf die Schaltfläche OK. Wählen Sie eine neue hinzugefügte Gruppenrichtlinie für das Verbindungsprofil aus.

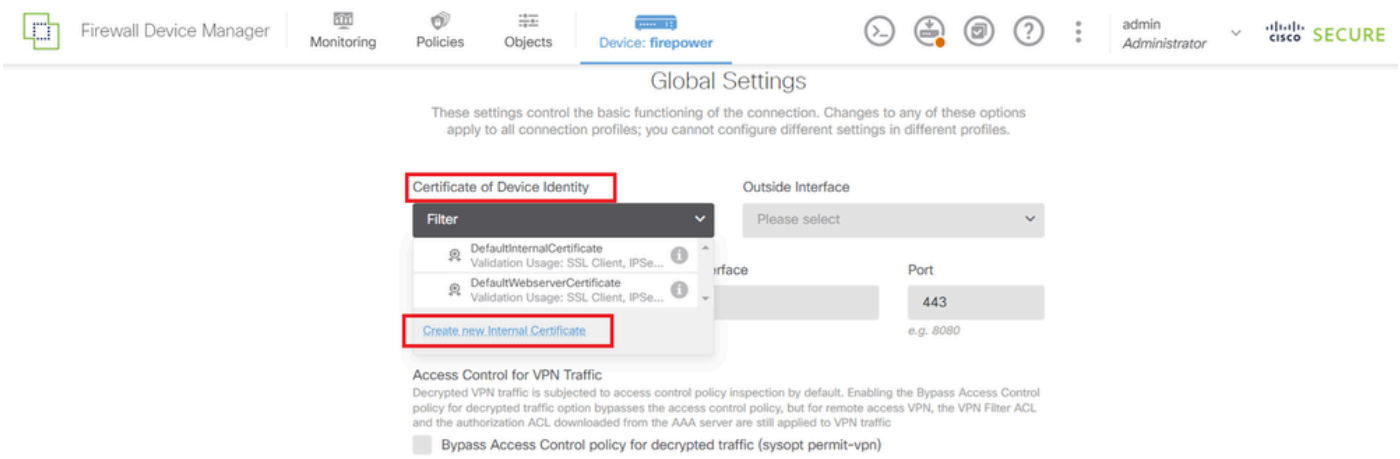
- Name: ftdvpn-aaa-cert-grp



Details zur Gruppenrichtlinie

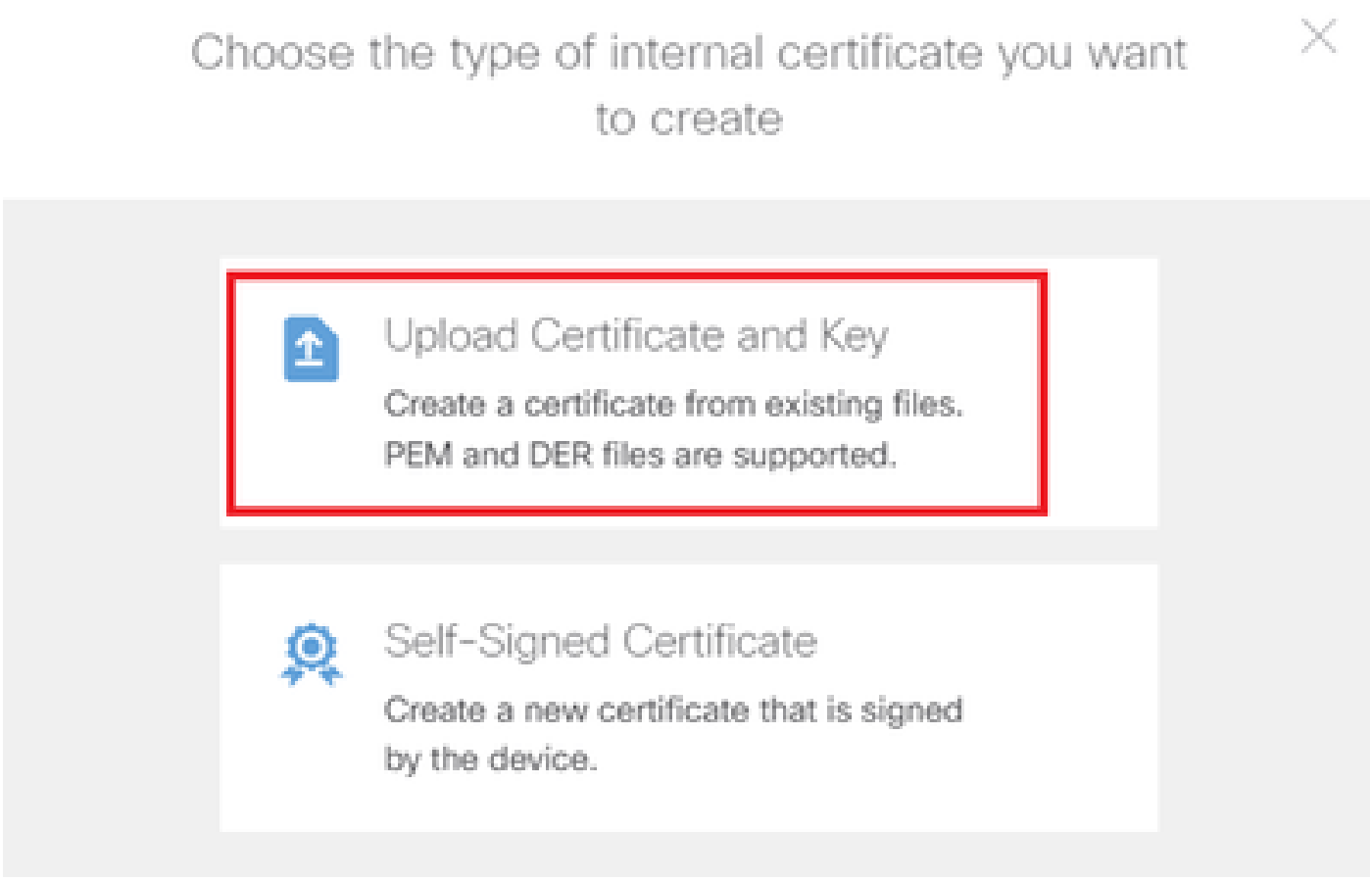
Schritt 6: Konfigurieren der Geräteidentität und der externen Schnittstelle für das Verbindungsprofil

Klicken Sie im Element Certificate of Device Identity (Geräteidentitätszertifikat) auf Neues internes Zertifikat erstellen.



Internes Zertifikat hinzufügen

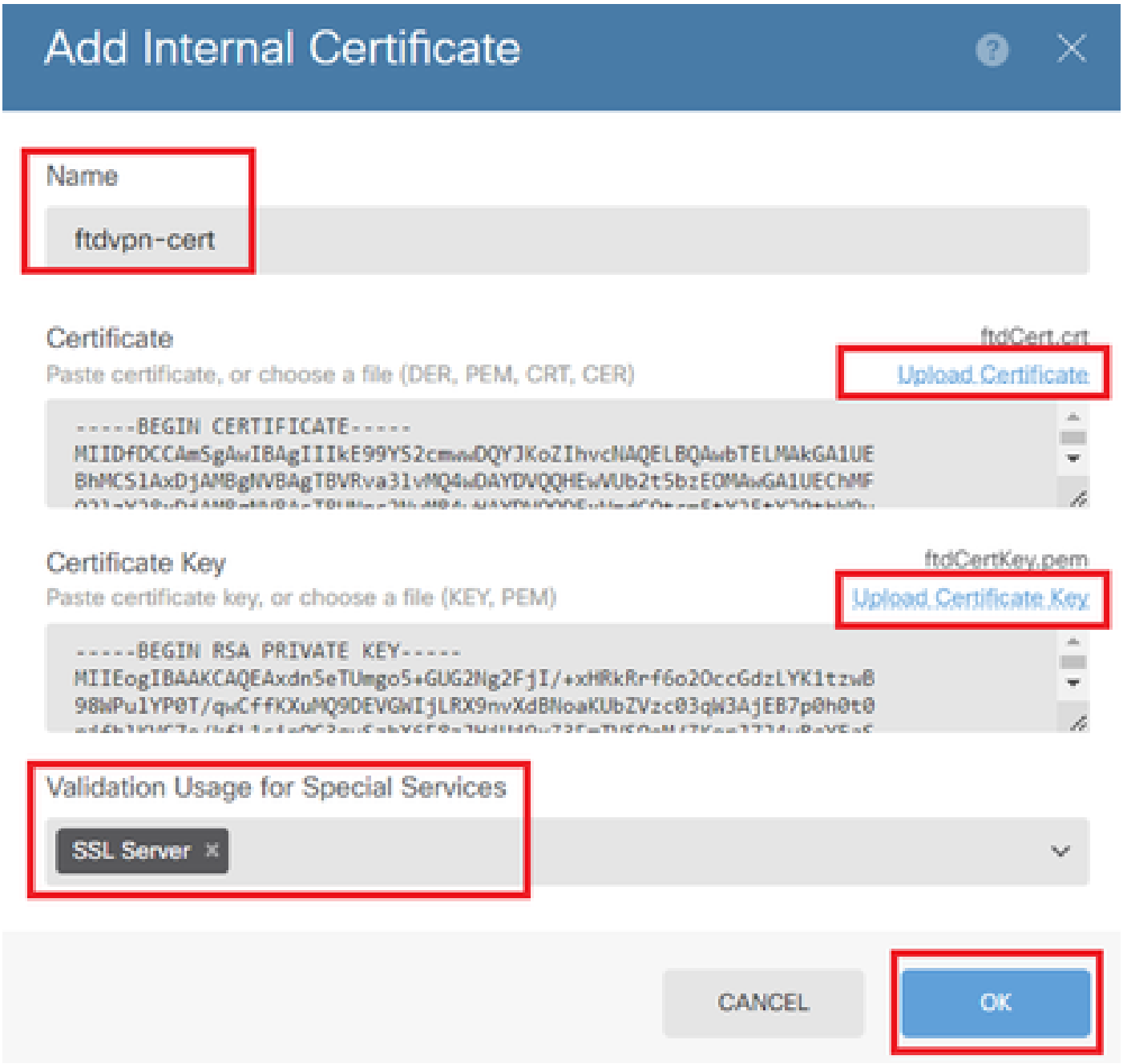
Klicken Sie auf Zertifikat und Schlüssel hochladen.



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.

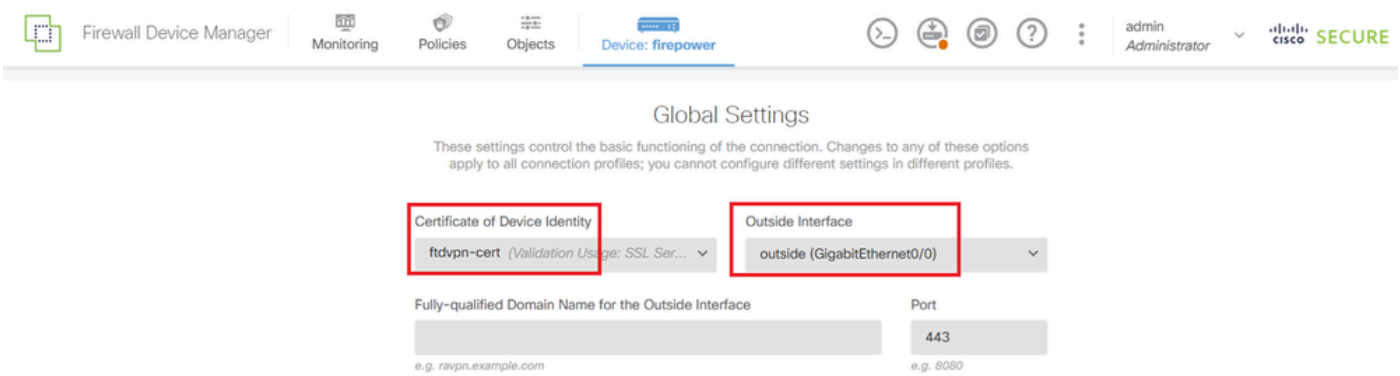
- Name: ftdvpn-cert
- Validierungsverwendung für spezielle Services: SSL-Server



Details des internen Zertifikats

Wählen Sie Certificate of Device Identity und Outside Interface für die VPN-Verbindung aus.

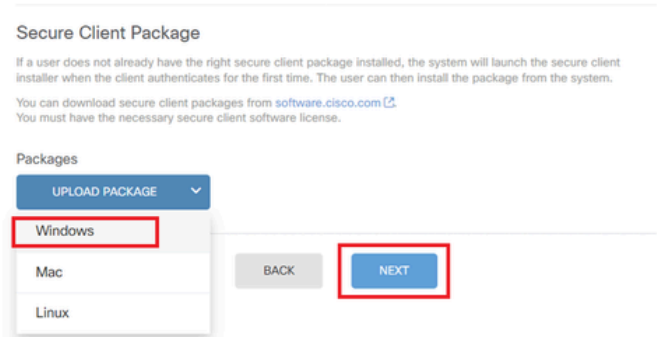
- Zertifikat für die Geräteidentität: ftdvpn-cert
- Externe Schnittstelle: außen (GigabitEthernet0/0)



Details der globalen Einstellungen

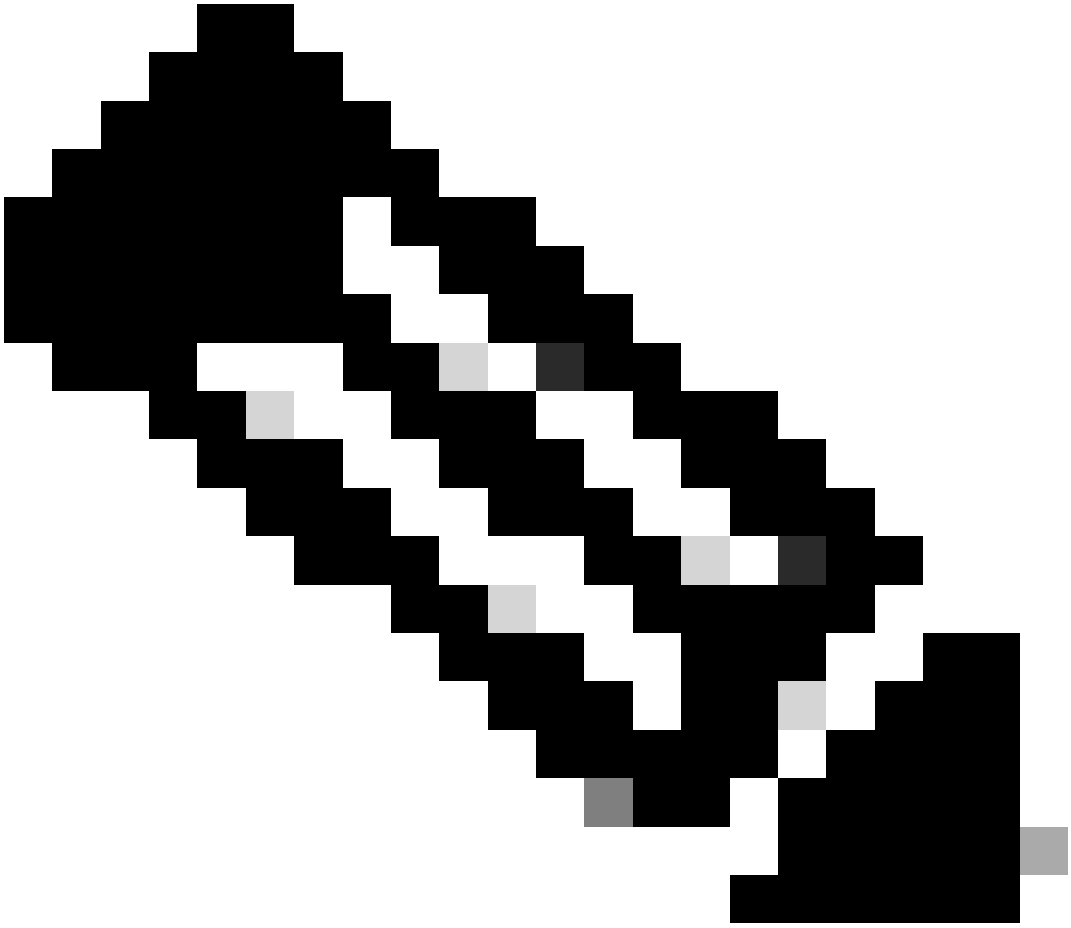
Schritt 7. Konfigurieren des sicheren Client-Abbilds für das Verbindungsprofil

Element Windows in Paketen auswählen

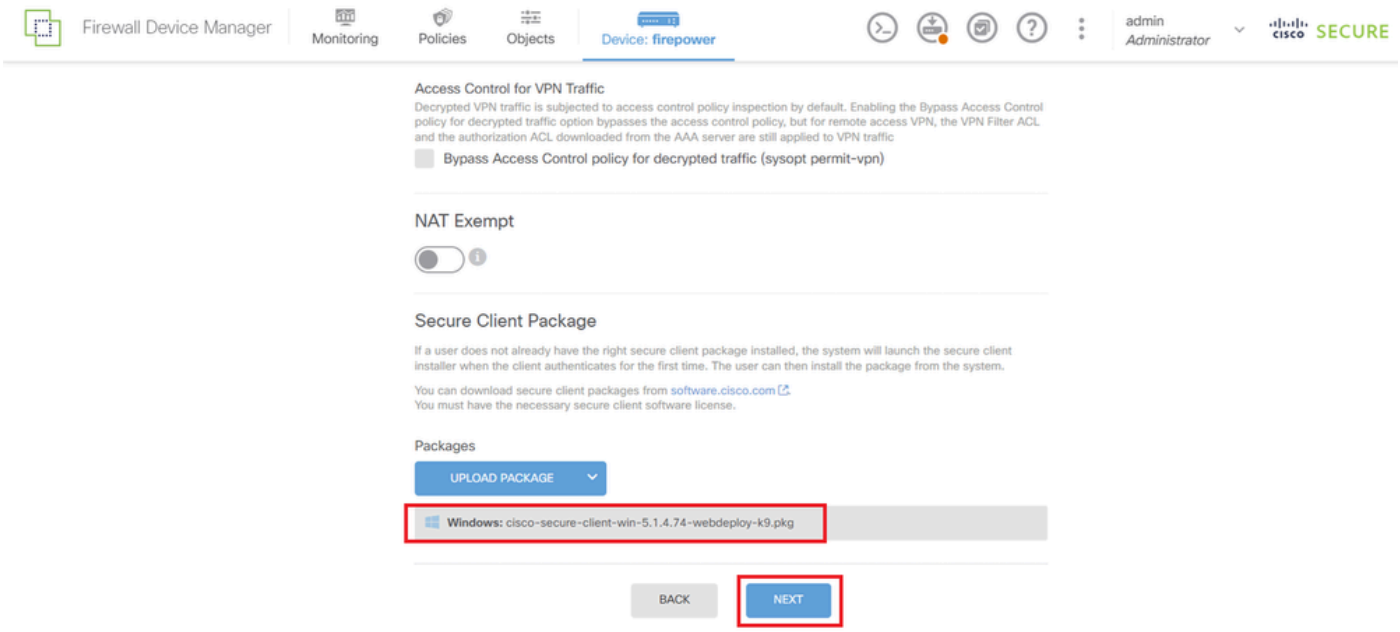


Paket mit sicherem Client-Image hochladen

Laden Sie die Datei für das sichere Client-Abbild vom lokalen Computer hoch, und klicken Sie auf Weiter.



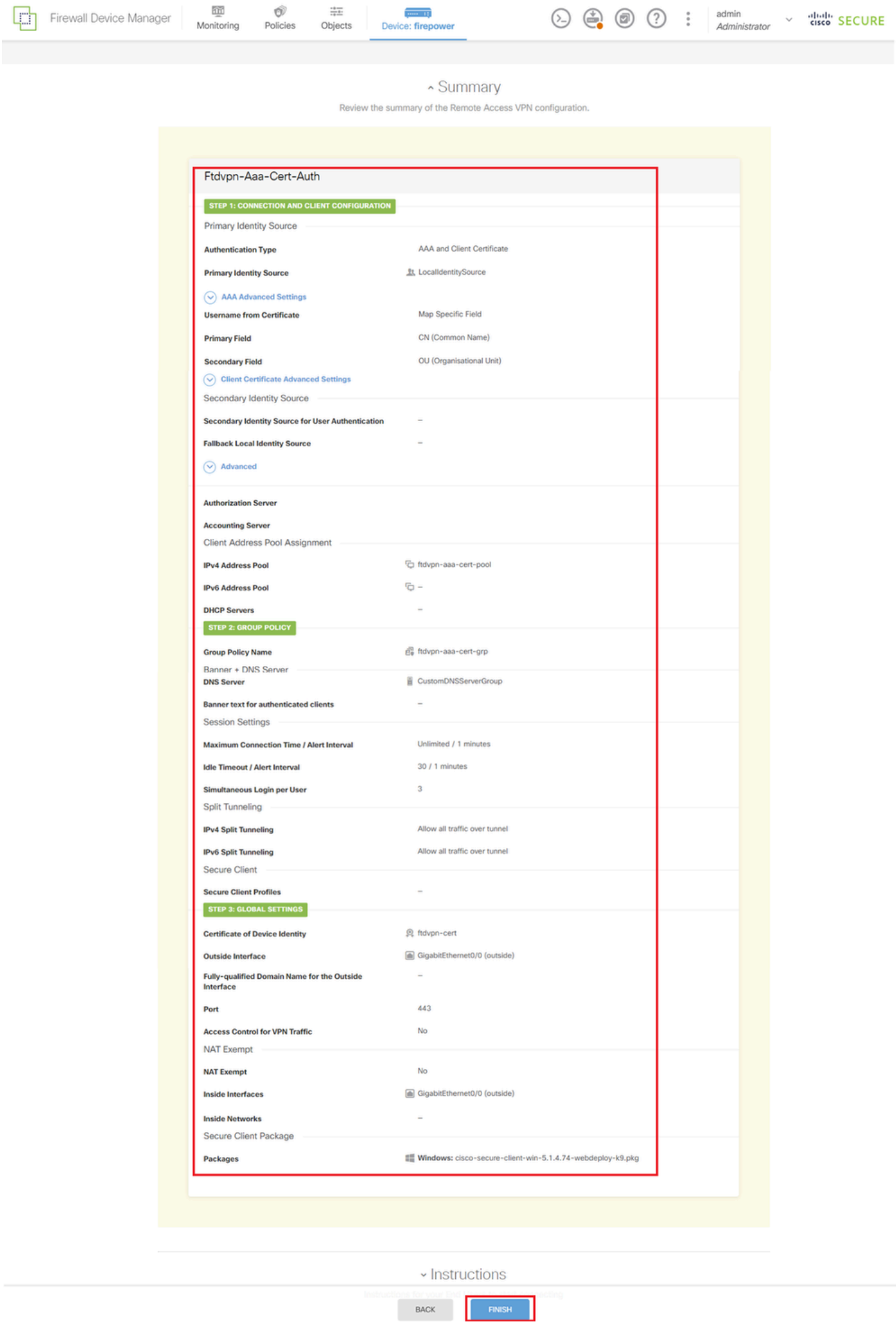
Hinweis: Die Funktion "NAT Exempt" (NAT ausschließen) ist in diesem Dokument deaktiviert. Standardmäßig ist die Option "Bypass Access Control policy for decrypted traffic" (sysopt permit-vpn) deaktiviert, d. h. der entschlüsselte VPN-Verkehr wird einer Richtlinienüberprüfung der Zugriffskontrolle unterzogen.



Secure Client Image-Paket auswählen

Schritt 8: Zusammenfassung für Verbindungsprofil bestätigen

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



Einstellungen für Verbindungsprofil bestätigen

```
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
!
interface GigabitEthernet0/1
speed auto
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
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

// Defines a local user
username sslVPNClientCN password ***** pbkdf2

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
enrollment terminal
keypair ftdvpn-cert
validation-usage ssl-server
crl configure

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

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client ssl-server
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 enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
dns-server value 64.x.x.245 64.x.x.184
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 none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// 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

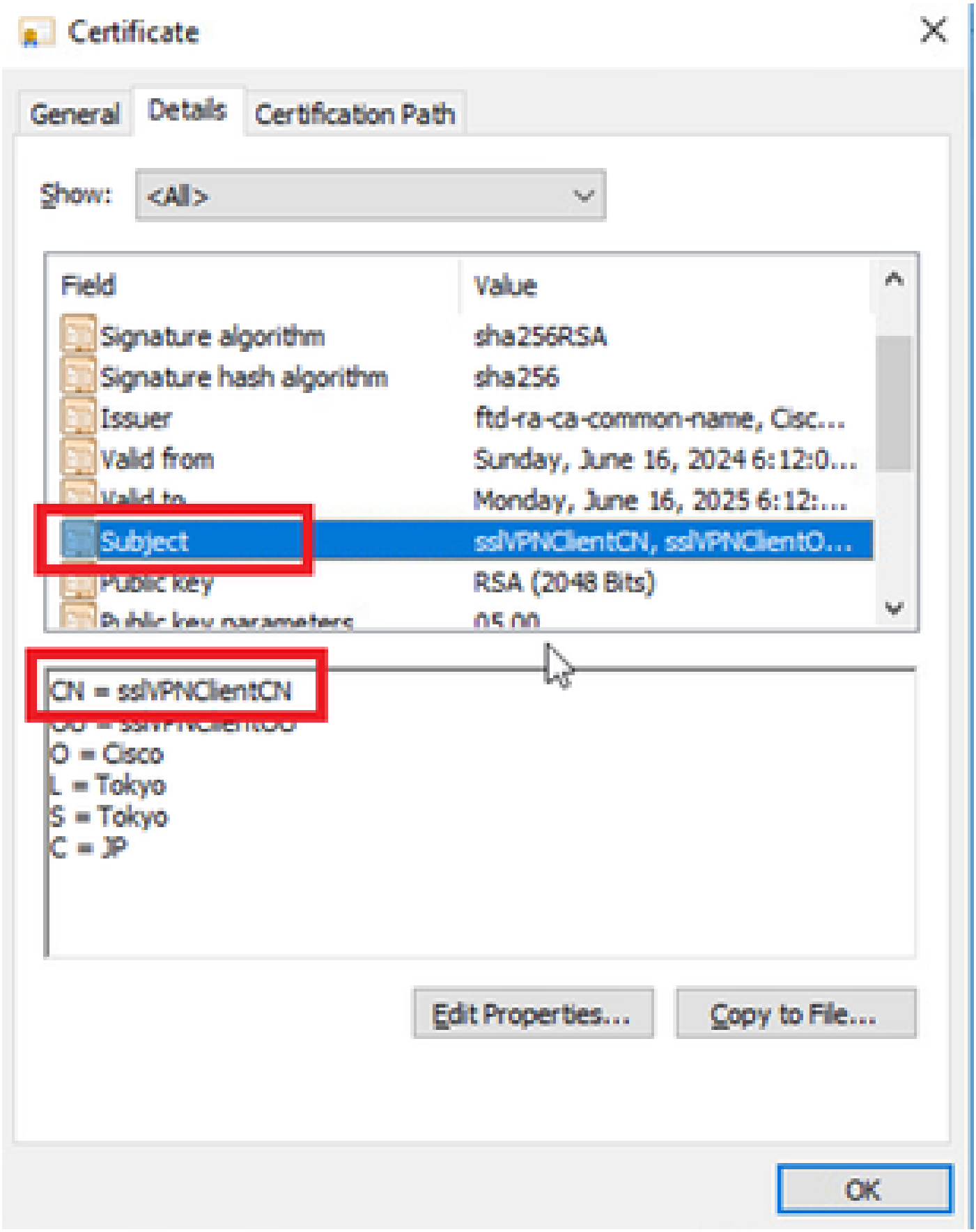
Schritt 1: Clientzertifikat bestätigen

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

Clientzertifikat bestätigen

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

- Betreff: CN = sslVPNClientCN



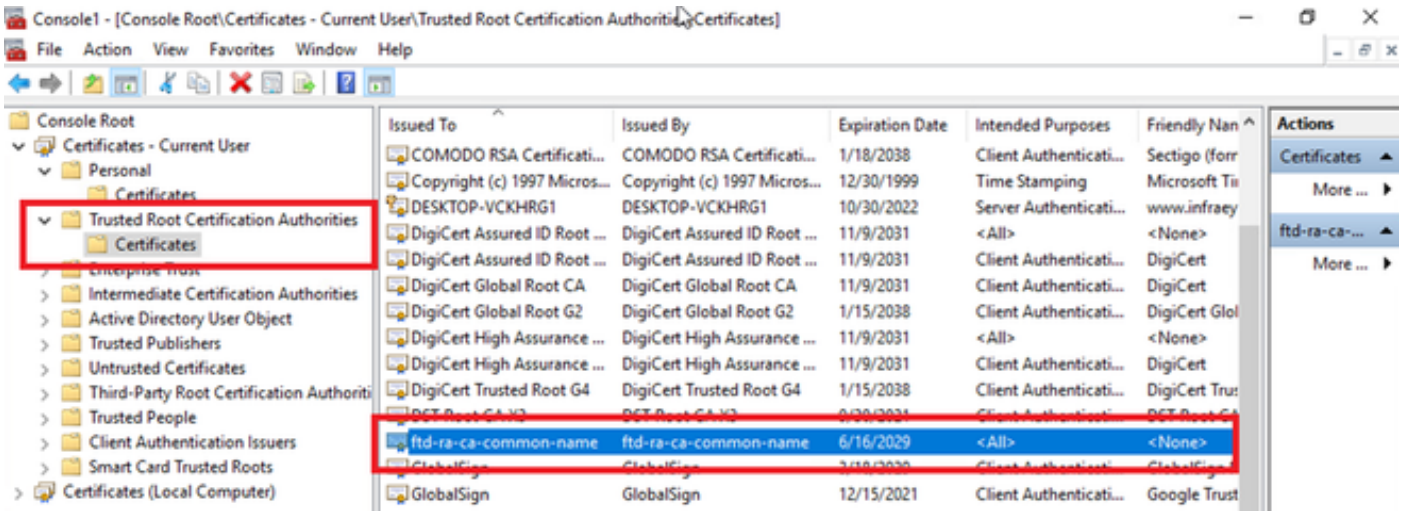
Details zum Clientzertifikat

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

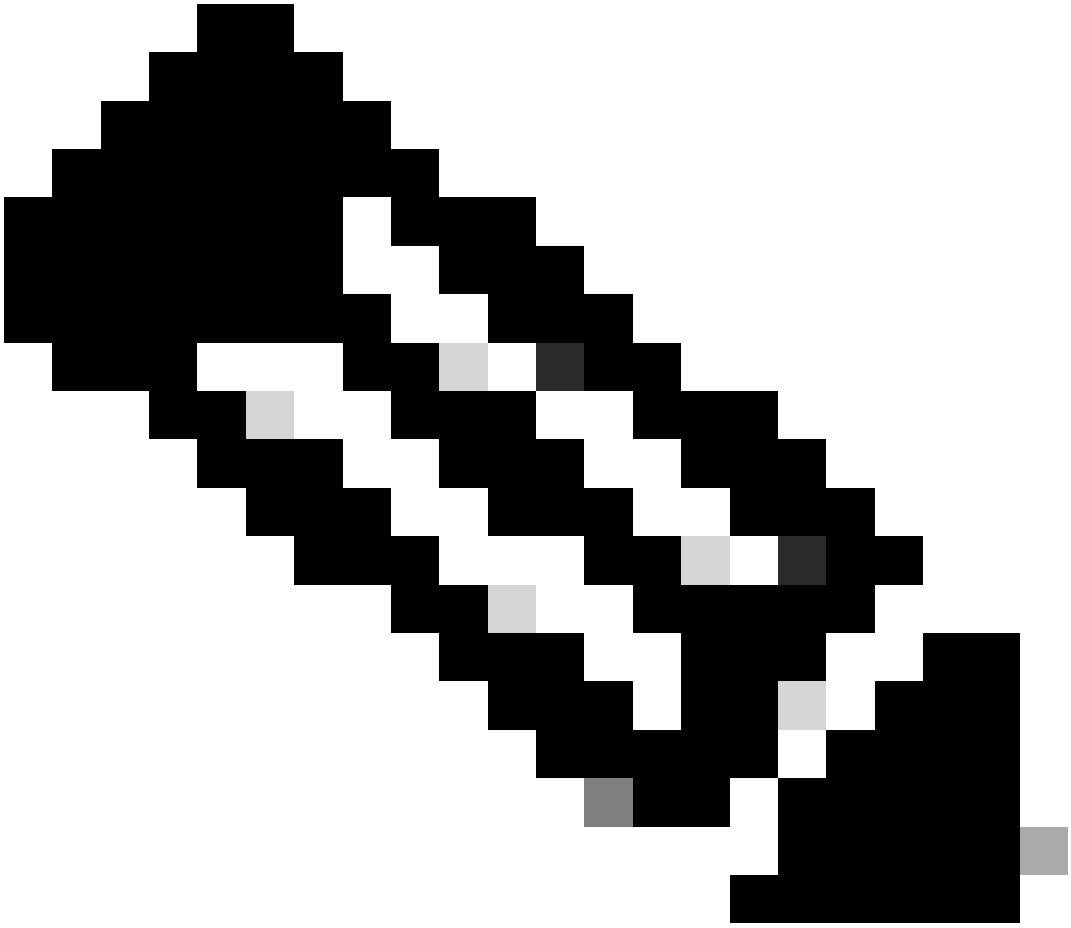


Zertifizierungsstelle bestätigen

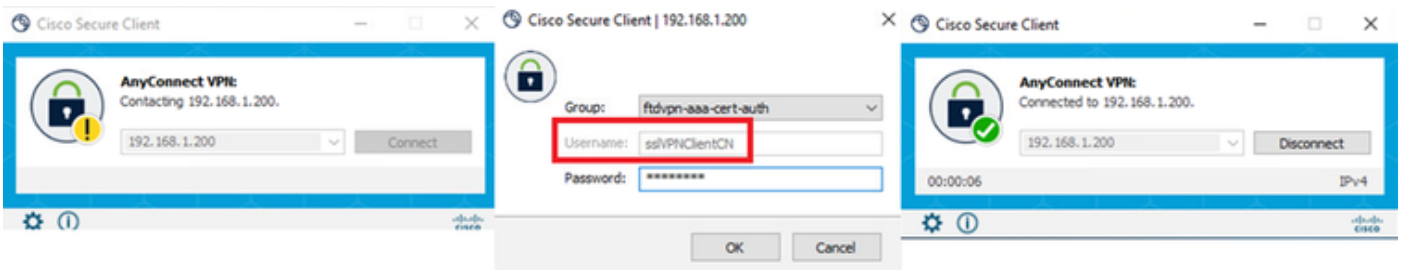
Überprüfung

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 Clientzertifikats in diesem Dokument extrahiert.



VPN-Verbindung initiieren

Schritt 2: 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.

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4
Assigned IP : 172.16.1.40 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 : 29072 Bytes Rx : 44412
Pkts Tx : 10 Pkts Rx : 442
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 11:47:42 UTC Sat Jun 29 2024
Duration : 1h:09m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

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

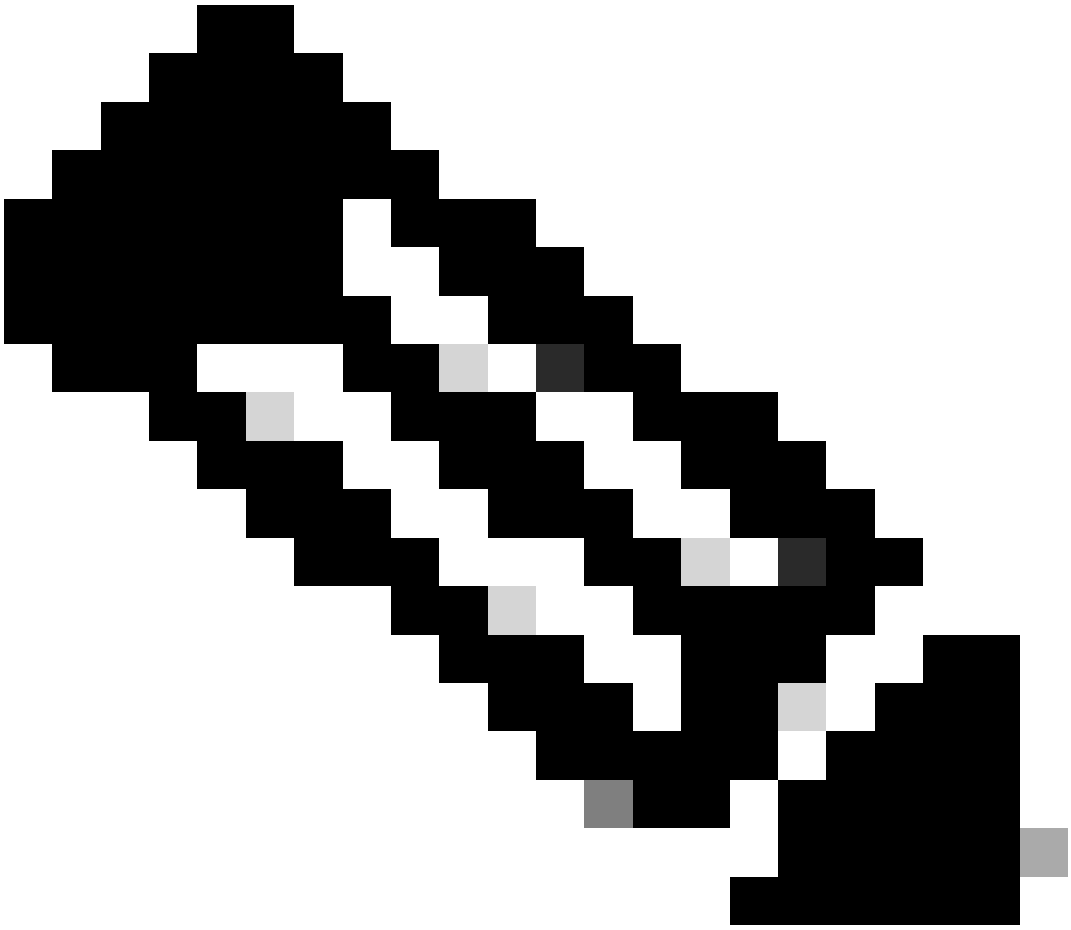
AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 49779 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 7 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 14356 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7178 Bytes Rx : 10358
Pkts Tx : 1 Pkts Rx : 118
Pkts Tx Drop : 0 Pkts Rx Drop : 0

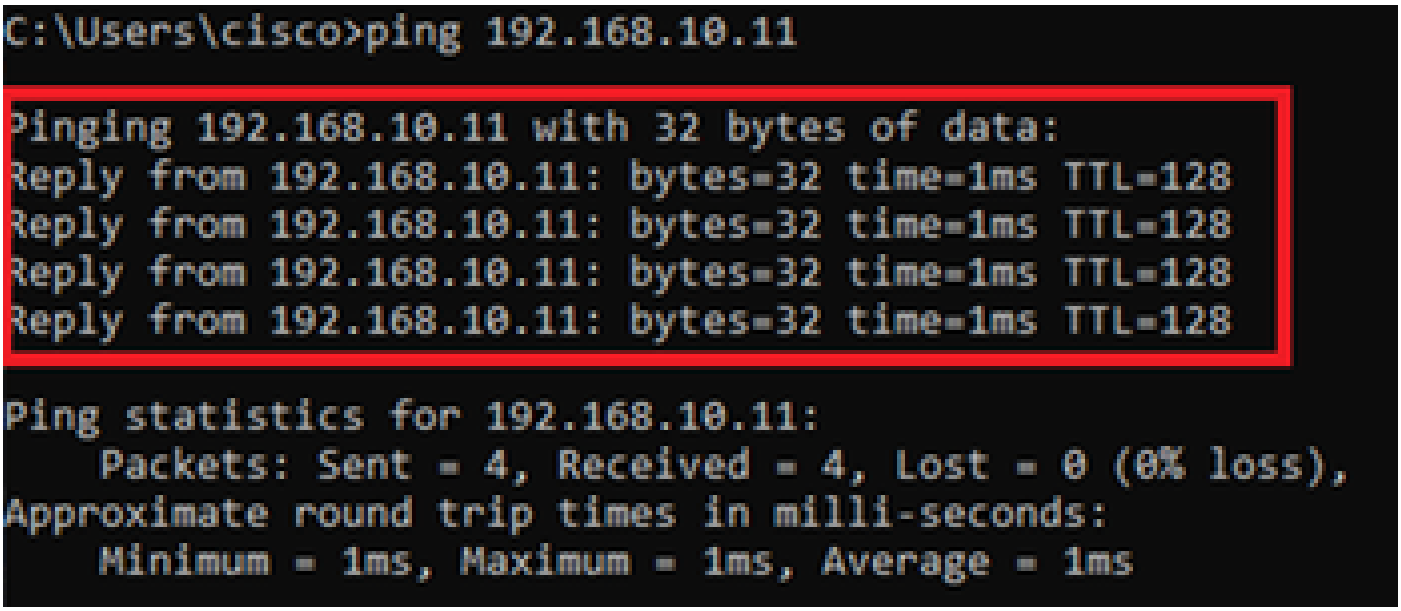
Schritt 3: Kommunikation mit Server bestätigen

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

erfolgreich ist.



Hinweis: Da die Option "Bypass Access Control policy for decrypted traffic" (sysopt permit-vpn) in Schritt 7 deaktiviert ist, müssen Sie Zugriffskontrollregeln erstellen, die Ihrem IPv4-Adresspool den Zugriff auf den Server ermöglichen.



Ping erfolgreich

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

firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo reply

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 im Lina-Modul.

// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientCN

// Extract username from the CN (Common Name) field

Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3]
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication
Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 29 2024 11:29:53: %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

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.