Konfiguration eines Remote Access-VPN auf einem von FDM verwalteten FTD

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der Bereitstellung eines RA VPN auf FTD beschrieben, das vom internen FDM mit der Version 6.5.0 und höher verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Konfiguration des Remote Access Virtual Private Network (RA VPN) auf dem FirePOWER Device Manager (FDM) verfügen.

Lizenzierung

- Firepower Threat Defense (FTD), registriert beim Smart Licensing-Portal mit aktivierten exportgesteuerten Funktionen (um die Registerkarte für die RA VPN-Konfiguration zu aktivieren)
- Alle AnyConnect-Lizenzen aktiviert (APEX, Plus oder VPN Only)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FTD mit Version 6.5.0-115
- Cisco AnyConnect Secure Mobility Client Version 4.7.01076

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.

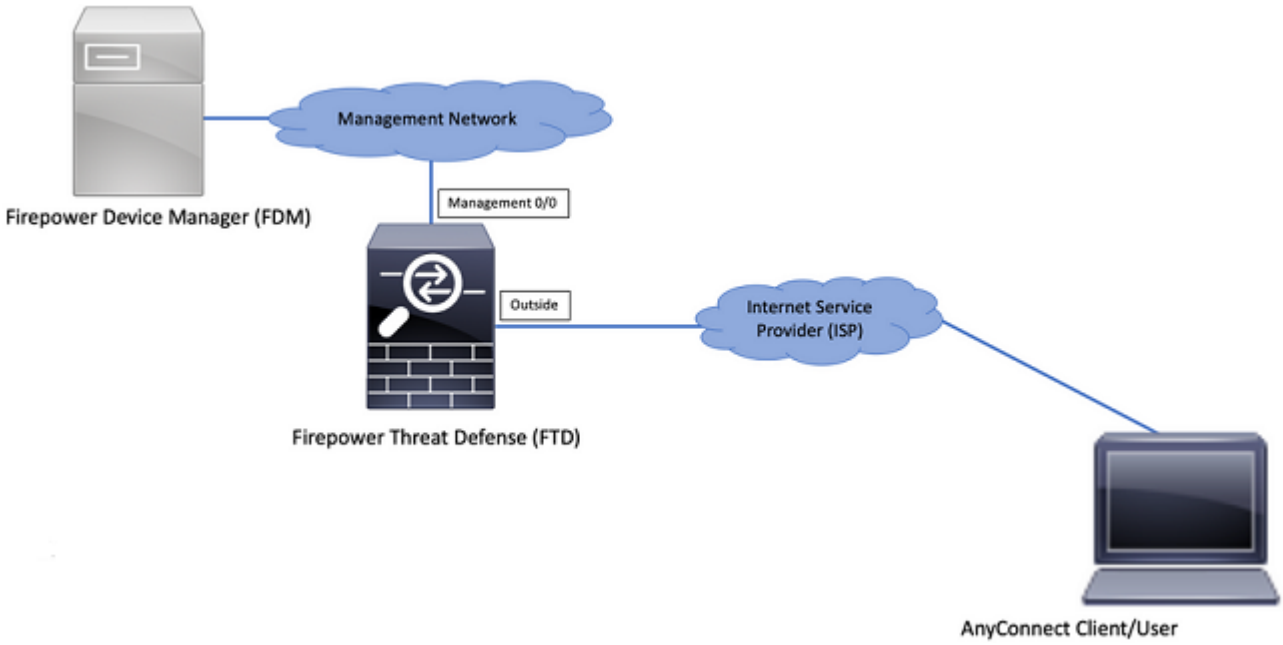
Hintergrundinformationen

Die Konfiguration von FTD über FDM bereitet Schwierigkeiten, wenn Sie versuchen, Verbindungen für AnyConnect-Clients über die externe Schnittstelle herzustellen, während der Zugriff auf die Verwaltung über dieselbe Schnittstelle erfolgt. Dies ist eine bekannte Beschränkung von FDM. Die Verbesserungsanfrage CSCvm76499 wurde für dieses Problem eingereicht.

Konfigurieren

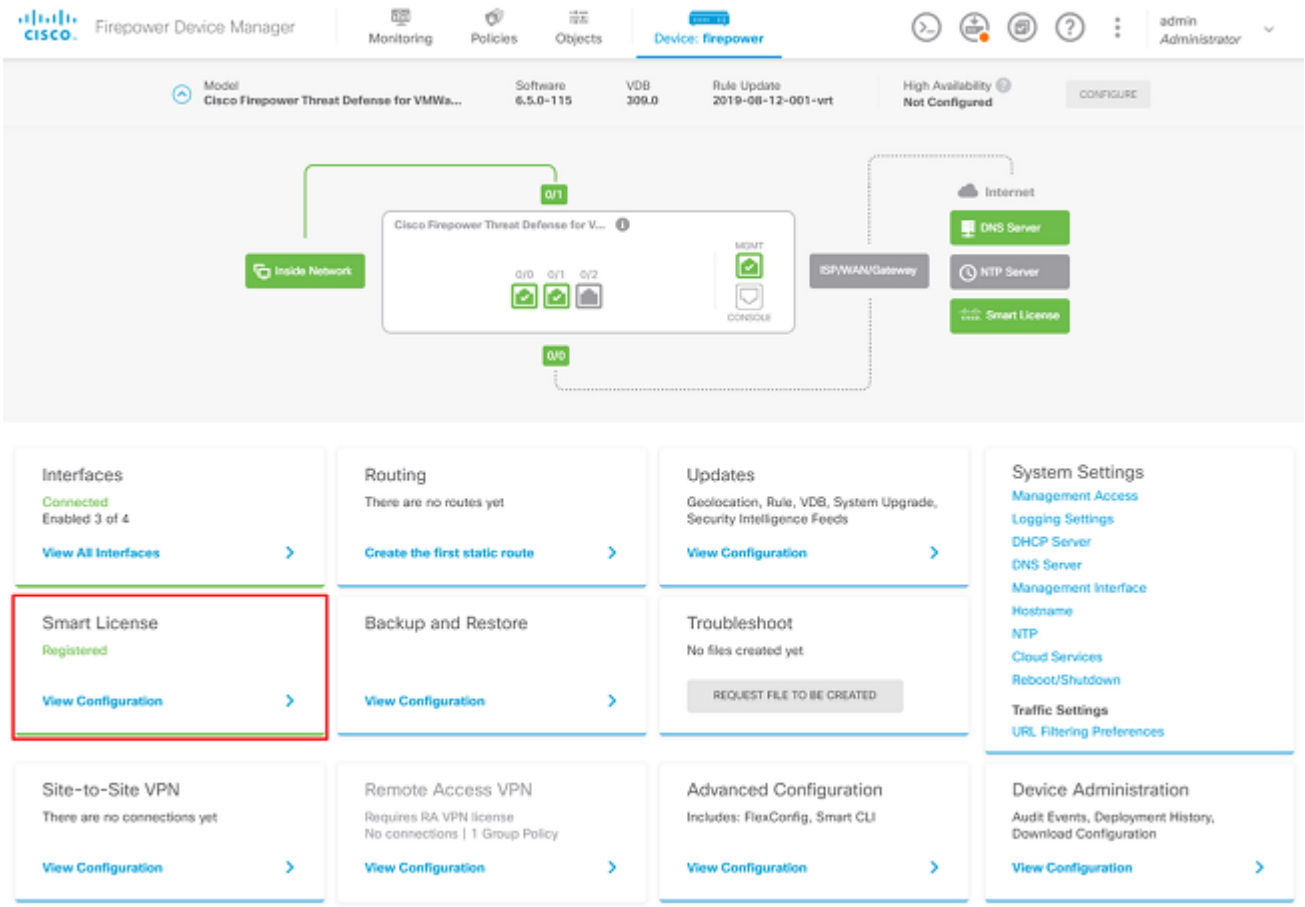
Netzwerkdiagramm

AnyConnect-Clientauthentifizierung unter Verwendung von Local.

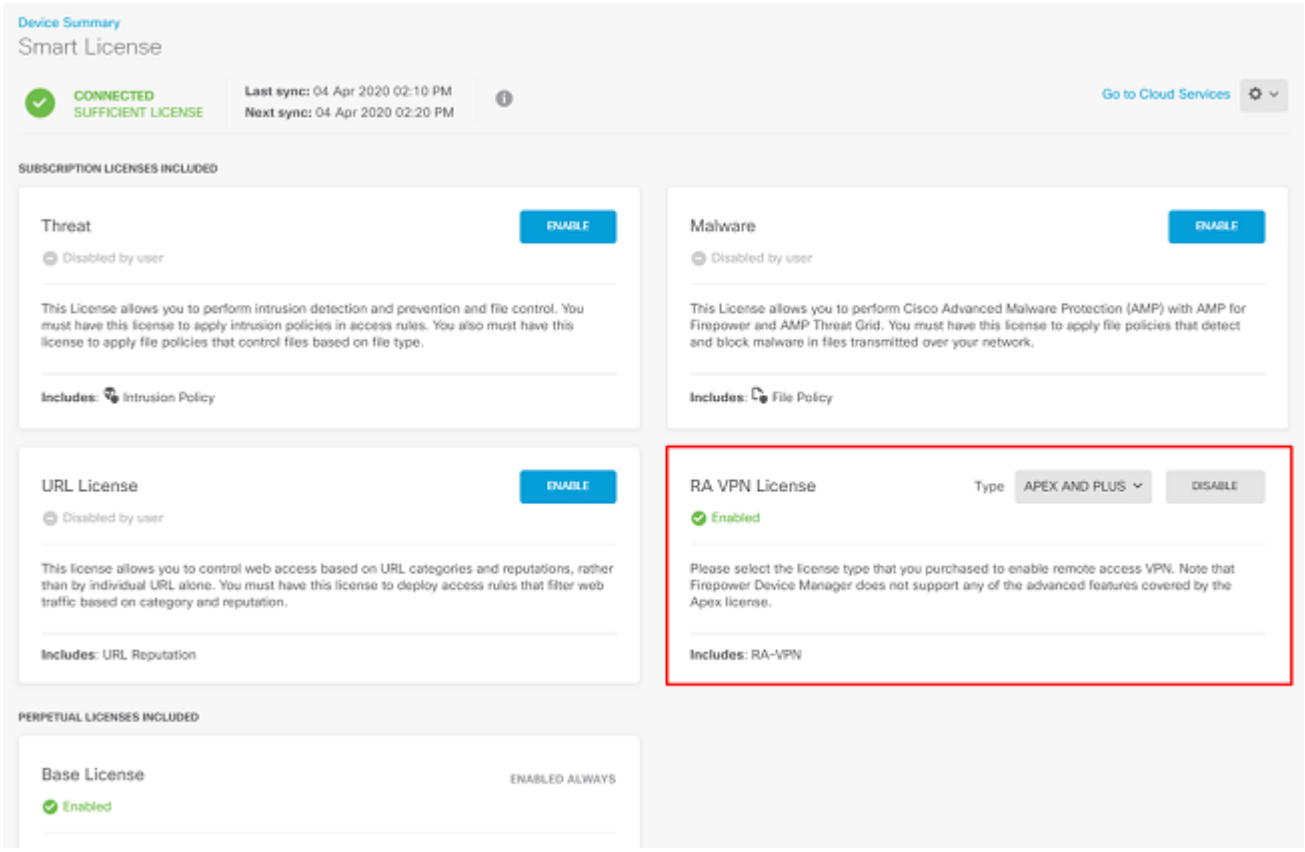


Überprüfen der Lizenzierung auf dem FTD

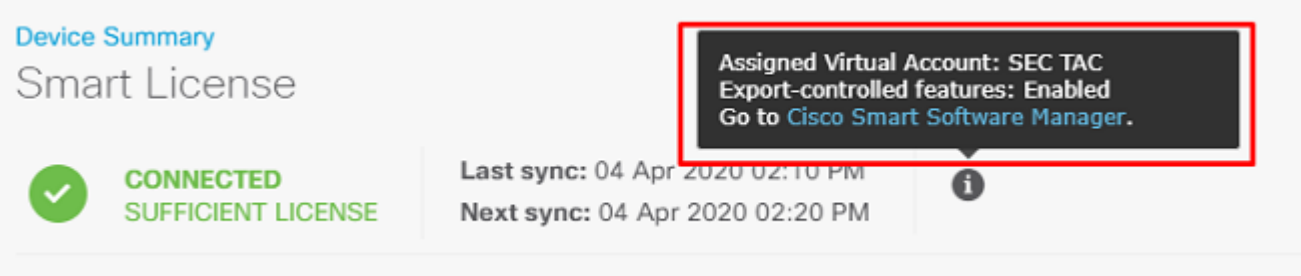
Schritt 1: Überprüfen Sie, ob das Gerät für die Smart Licensing-Funktion registriert ist, wie im Bild gezeigt:



Schritt 2: Überprüfen Sie, ob AnyConnect-Lizenzen auf dem Gerät aktiviert sind, wie im Bild gezeigt.

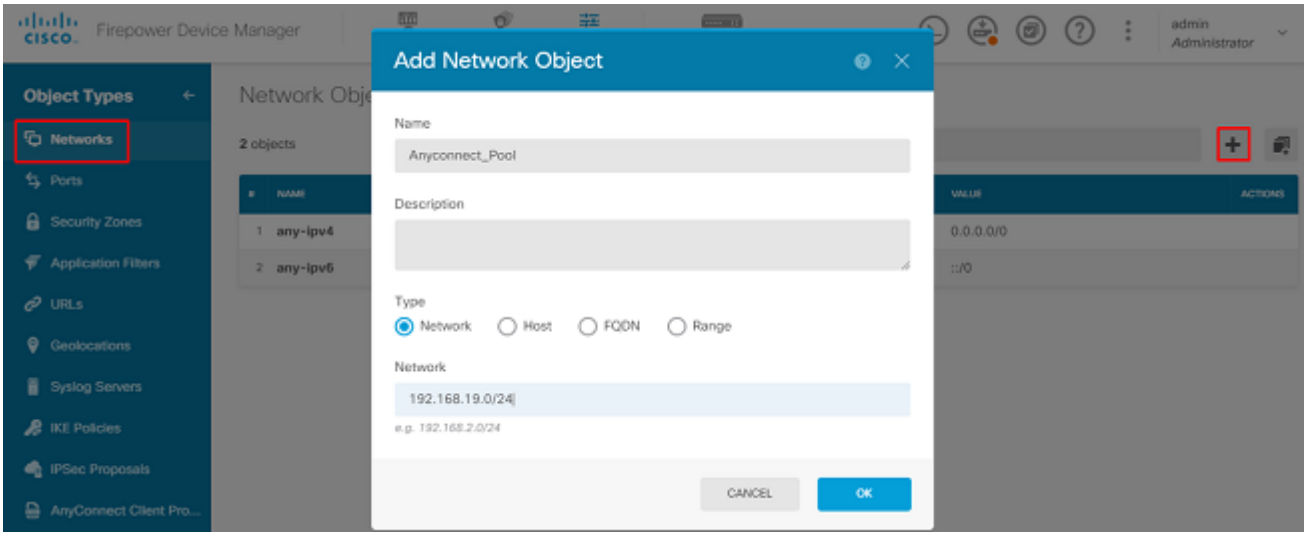


Schritt 3: Überprüfen Sie, ob die exportgesteuerten Funktionen im Token aktiviert sind, wie im Bild gezeigt:

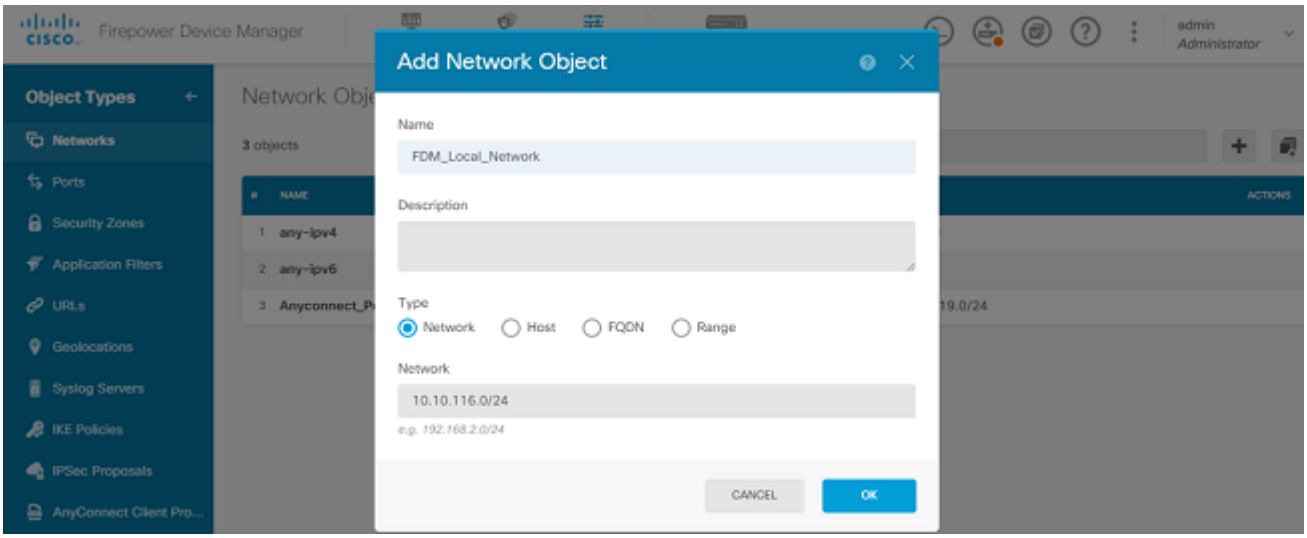


Geschützte Netzwerke definieren

Navigieren Sie zu Objects > Networks > Add new Network. Konfigurieren von VPN-Pool und LAN-Netzwerken über die FDM-GUI Erstellen Sie einen VPN-Pool für die lokale Adresszuweisung zu AnyConnect-Benutzern, wie im Bild gezeigt:

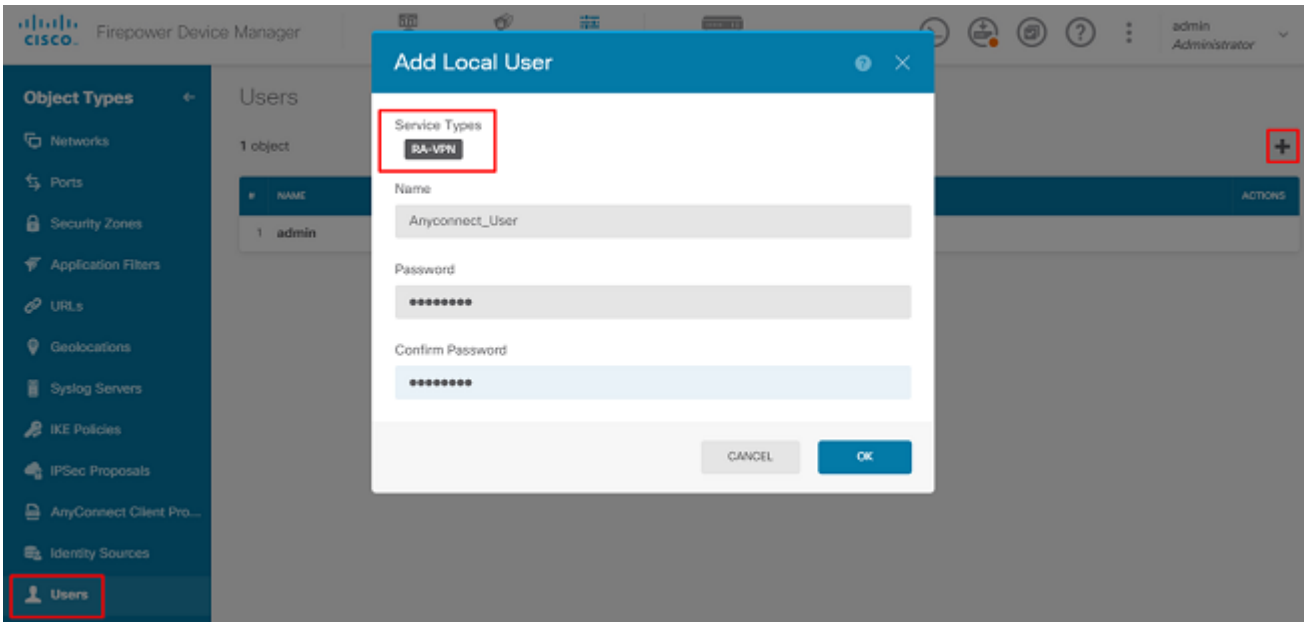


Erstellen Sie ein Objekt für das lokale Netzwerk hinter dem FDM-Gerät, wie im Bild gezeigt:



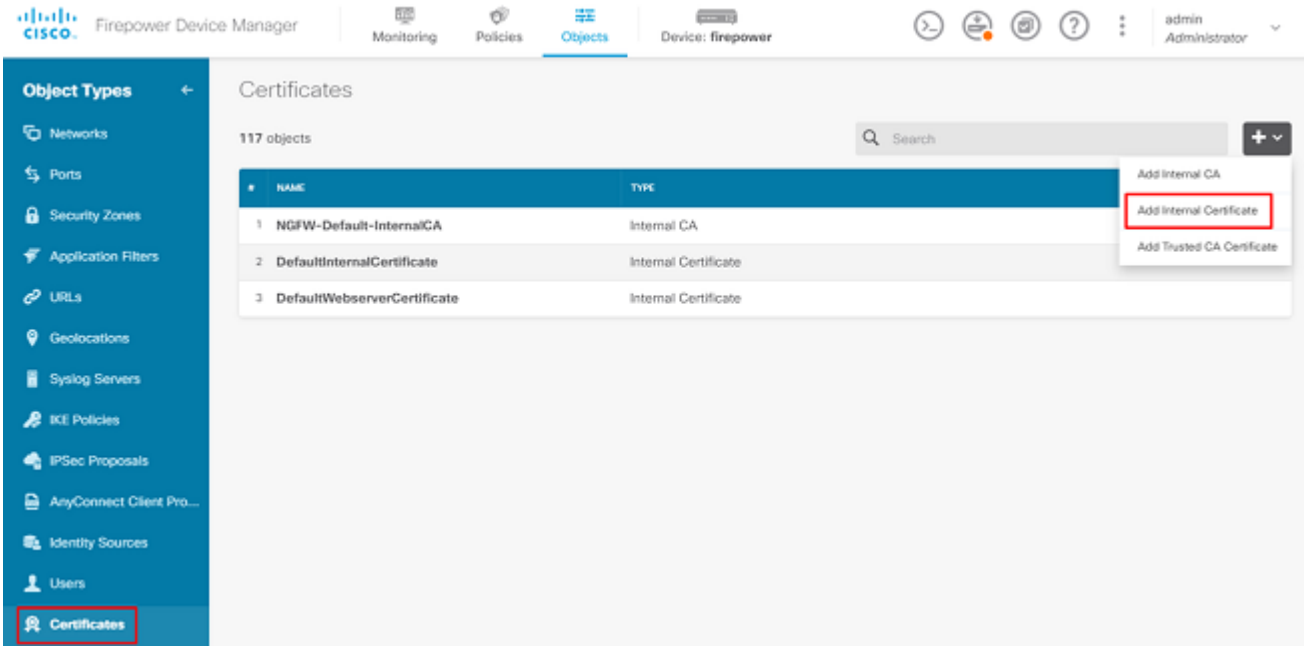
Lokale Benutzer erstellen

Navigieren Sie zu Objects > Users > Add User. Hinzufügen lokaler VPN-Benutzer, die über AnyConnect eine Verbindung zu FTD herstellen Erstellen Sie lokale Benutzer, wie im Bild gezeigt:

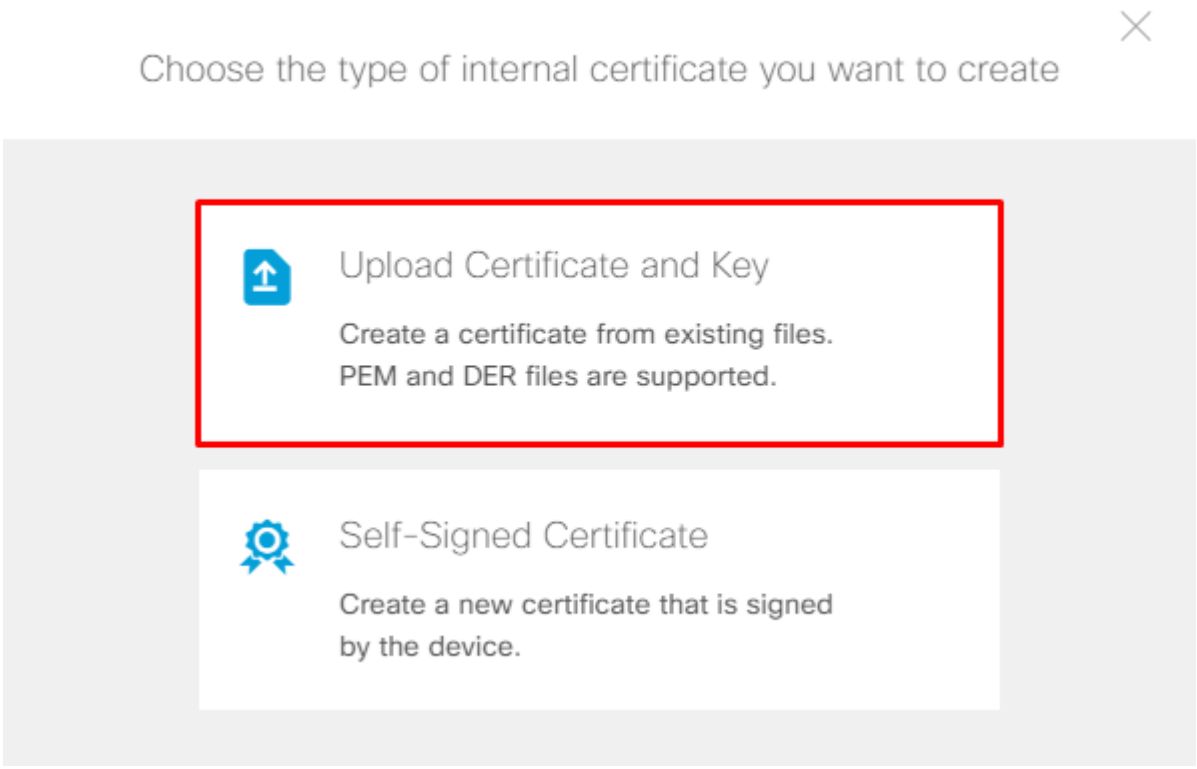


Zertifikat hinzufügen

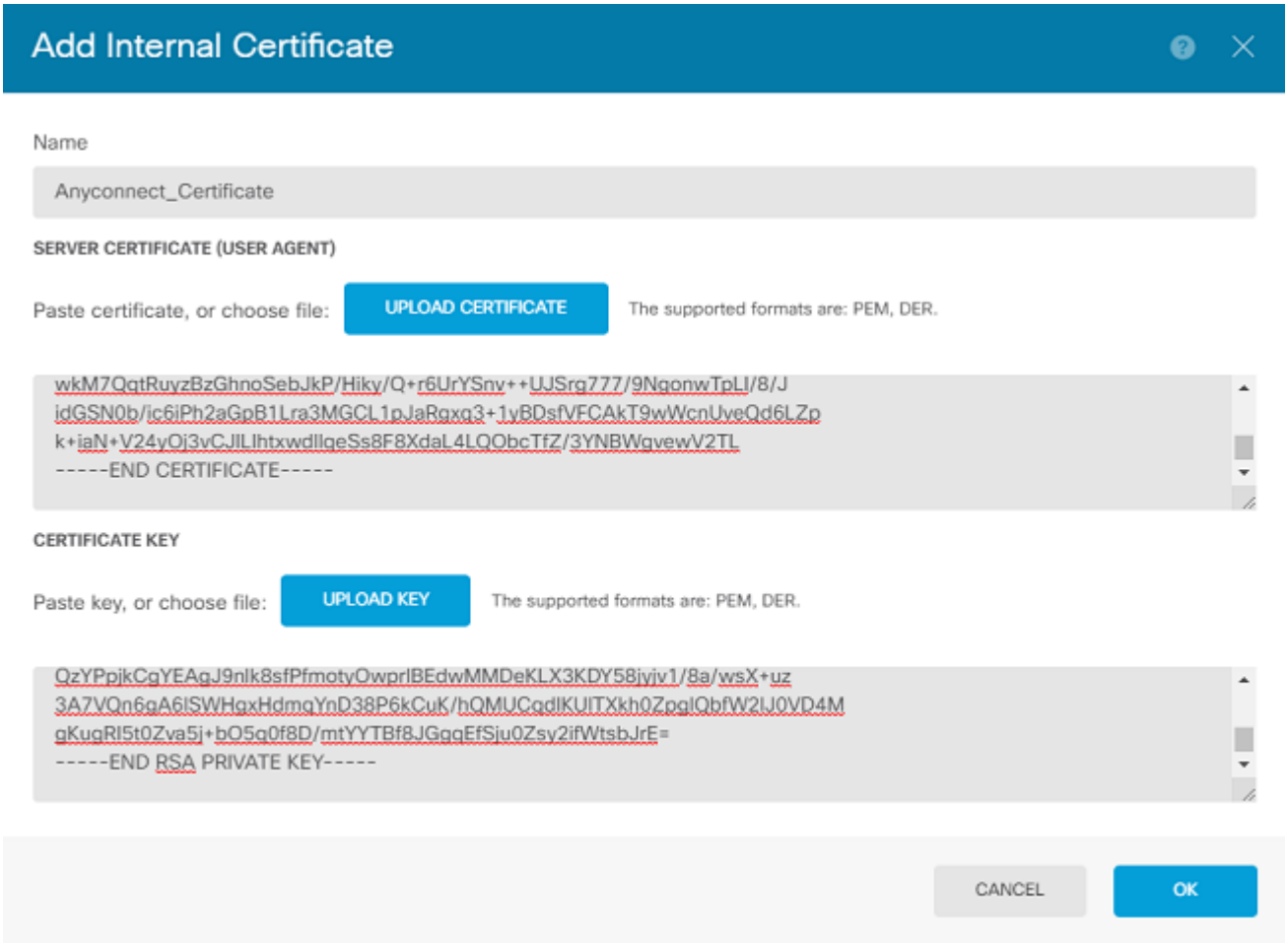
Navigieren Sie zu Objects > Certificates > Add Internal Certificate. Konfigurieren Sie ein Zertifikat wie im Bild gezeigt:



Laden Sie das Zertifikat und den privaten Schlüssel wie im Bild gezeigt hoch:

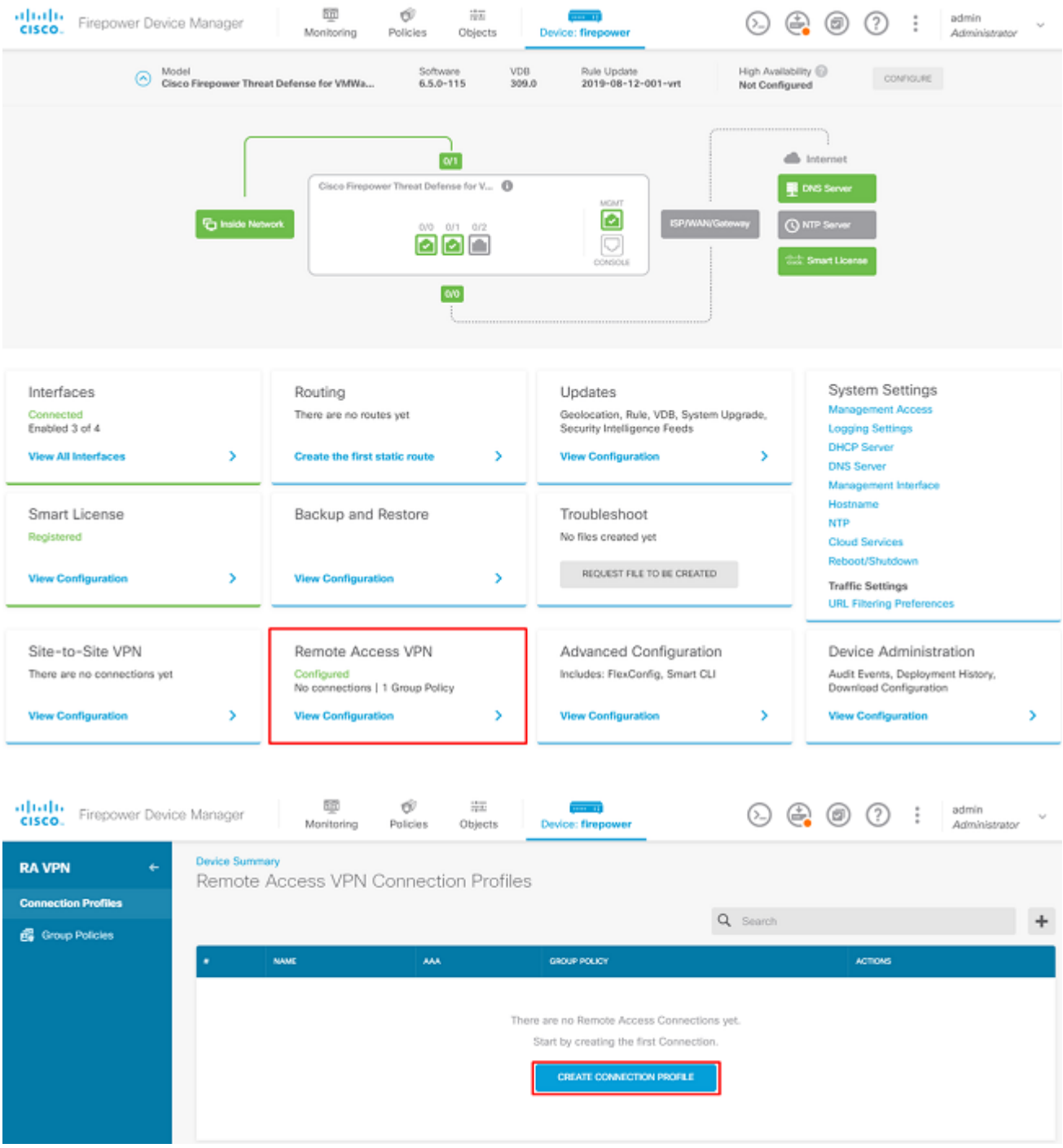


Das Zertifikat und der Schlüssel können durch Kopieren und Einfügen hochgeladen werden, oder durch die Upload-Schaltfläche für jede Datei, wie im Bild gezeigt:

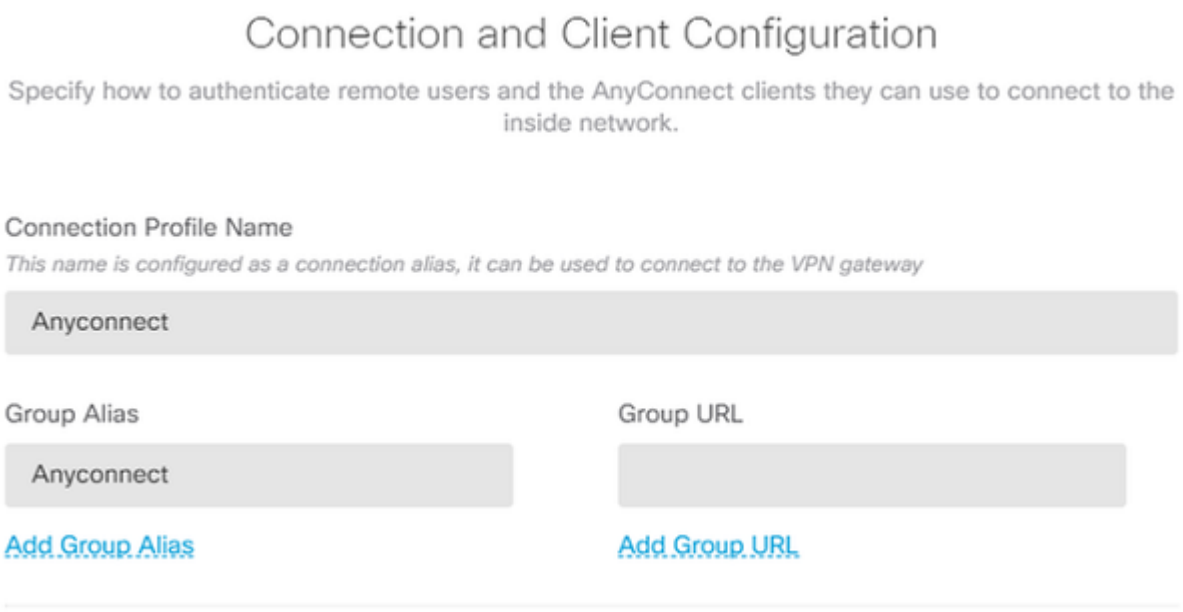


Konfigurieren des Remote Access-VPNs

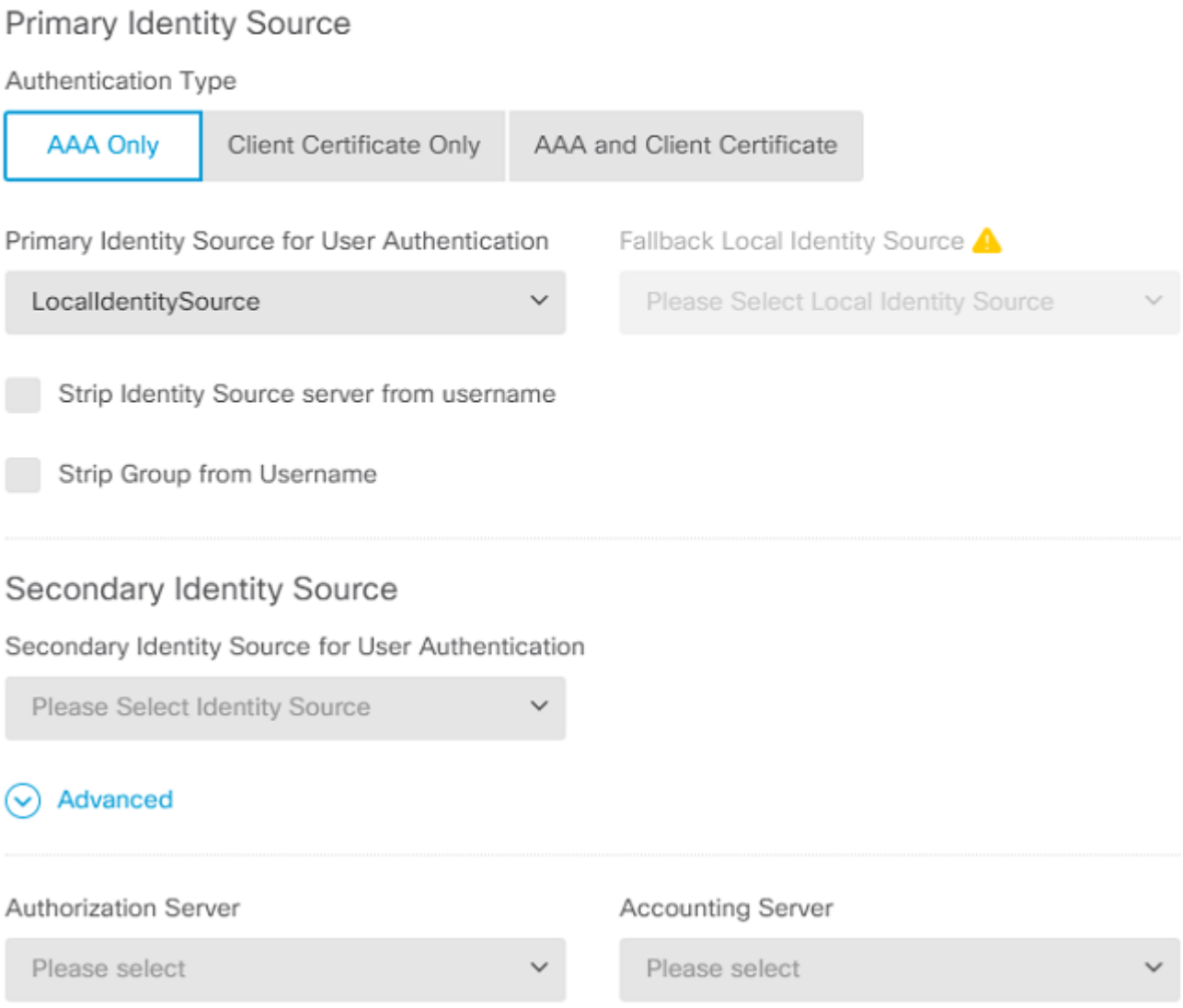
Navigieren Sie zu Remote Access VPN > Create Connection Profile. Navigieren Sie durch den RA VPN Wizard auf FDM, wie in der Abbildung dargestellt:



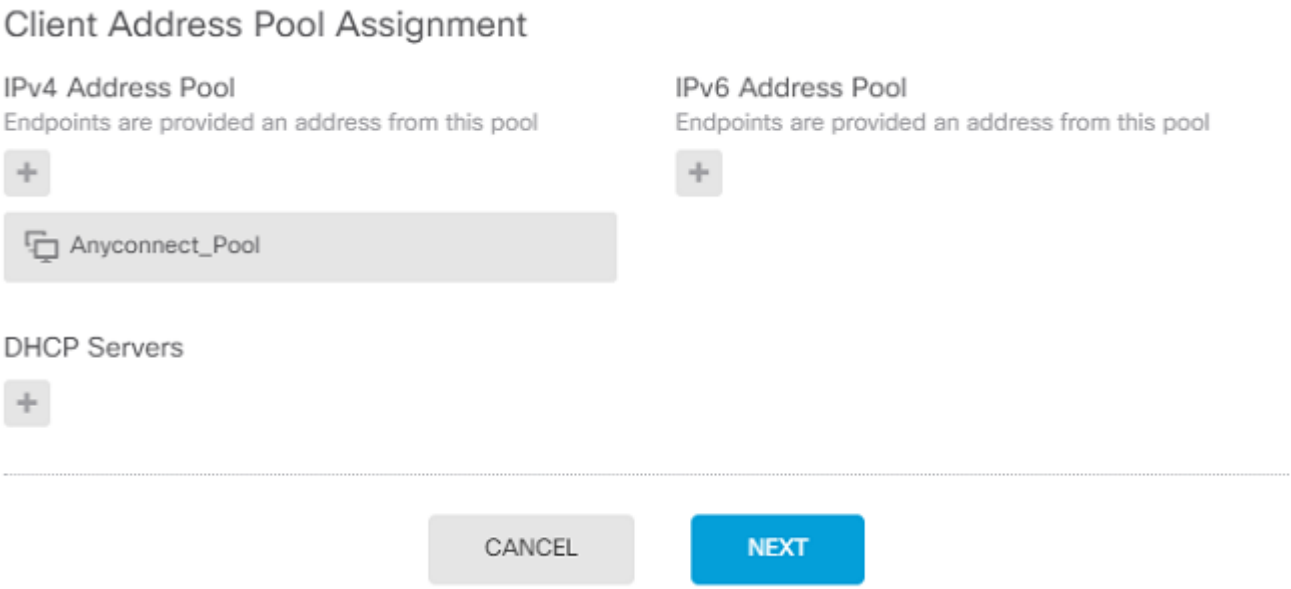
Erstellen Sie ein Verbindungsprofil, und starten Sie die Konfiguration wie im Bild gezeigt:



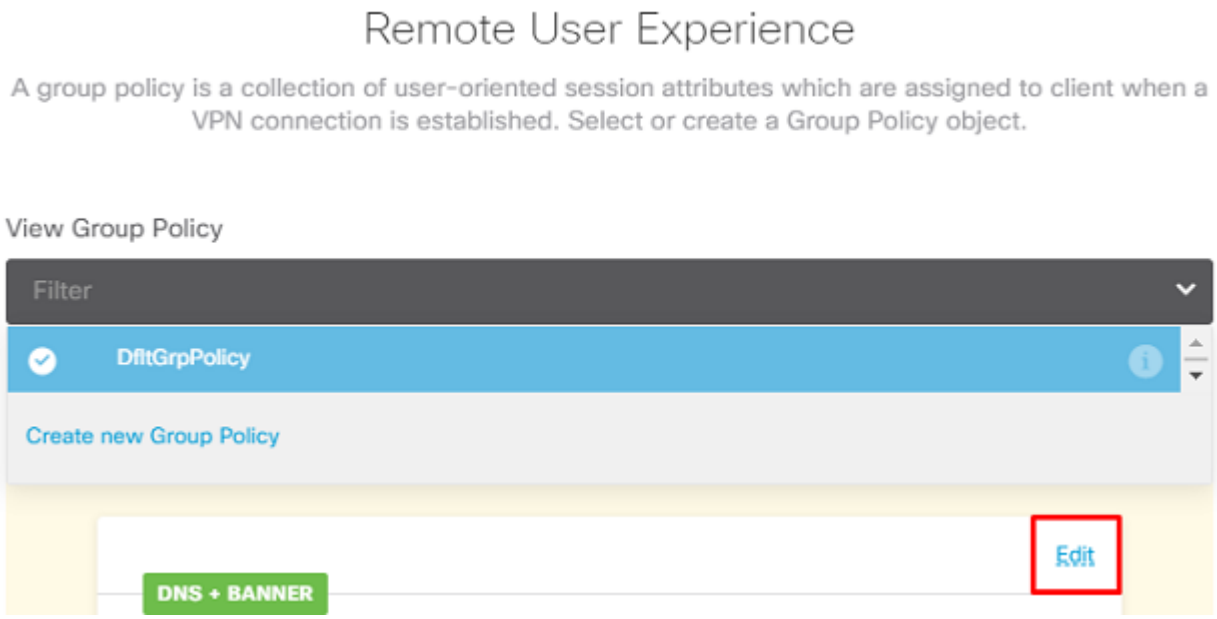
Wählen Sie die Authentifizierungsmethoden wie im Bild dargestellt aus. In diesem Leitfaden wird die lokale Authentifizierung verwendet.



Wählen Sie Anyconnect_Pool Objekt wie im Bild gezeigt:

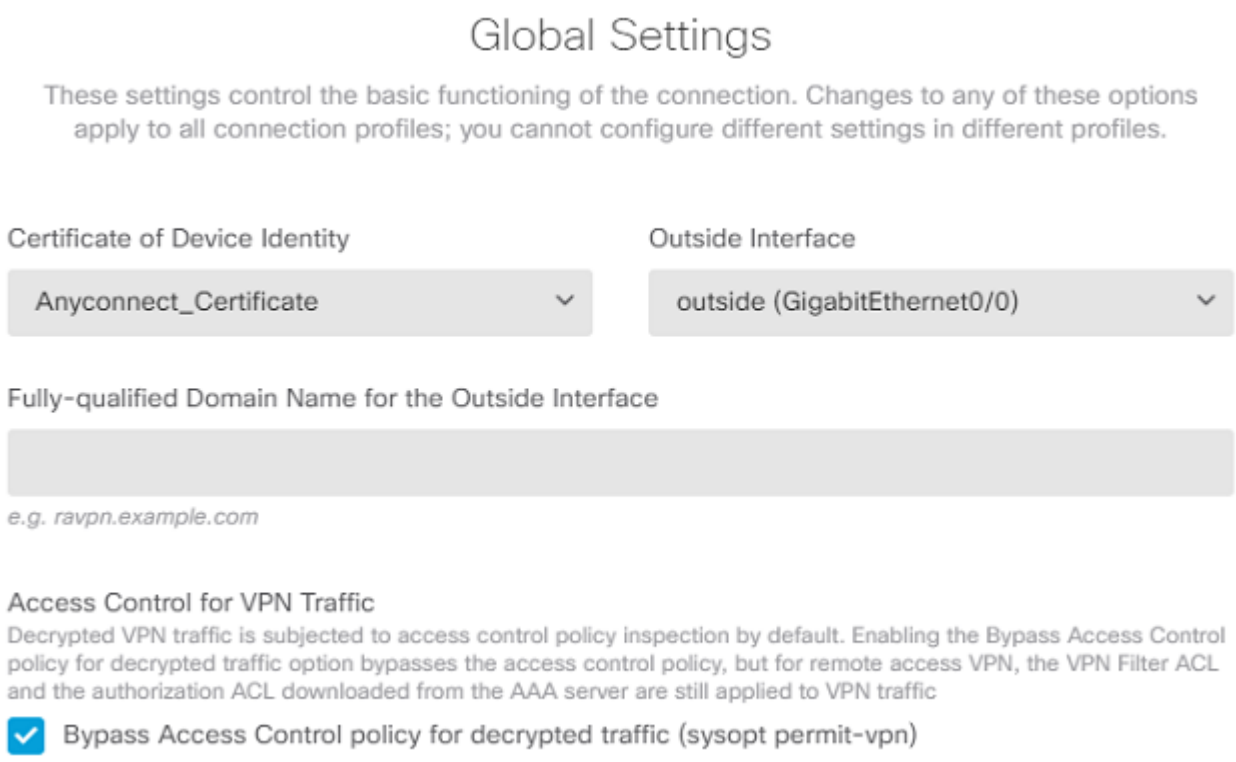


Auf der nächsten Seite wird eine Zusammenfassung der Standardgruppenrichtlinie angezeigt. Wenn Sie auf das Dropdown-Menü klicken und die Option auswählen, Create a new Group Policy. Für dieses Handbuch wird die Standardgruppenrichtlinie verwendet. Wählen Sie die Bearbeitungsoption oben in der Richtlinie aus, wie im Bild gezeigt:

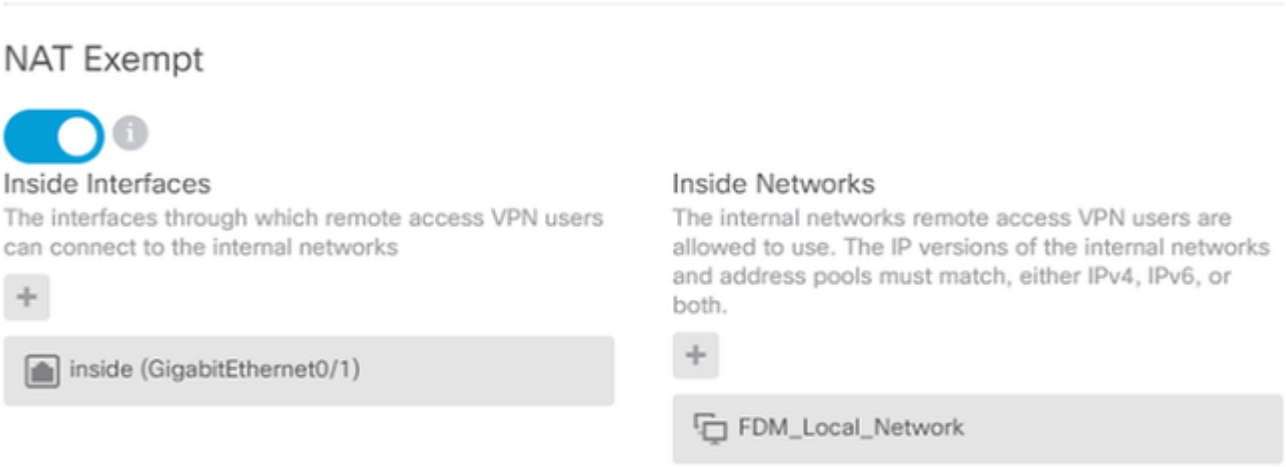


Fügen Sie in der Gruppenrichtlinie Split-Tunneling hinzu, sodass Benutzer, die mit Anyconnect verbunden sind, nur Datenverkehr senden, der über den Anyconnect-Client an das interne FTD-Netzwerk gerichtet ist, während der gesamte andere Datenverkehr aus der ISP-Verbindung des Benutzers ausgeht, wie im Bild gezeigt:

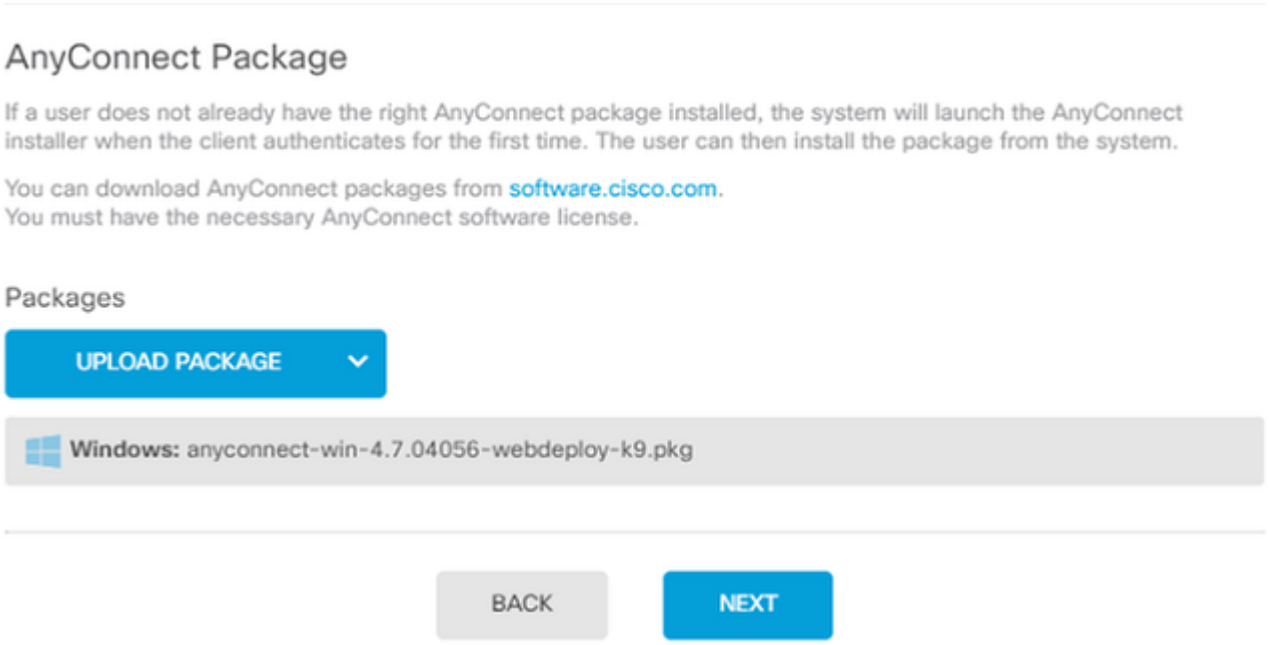
Wählen Sie auf der nächsten Seite Anyconnect_Certificate im Zertifikatabschnitt hinzugefügt. Wählen Sie anschließend die Schnittstelle aus, auf der das FTD AnyConnect-Verbindungen abhört. Wählen Sie die Richtlinie "Zugriffskontrolle umgehen" für entschlüsselten Datenverkehr (sysopt permit-vpn). Dies ist ein optionaler Befehl, wenn das sysopt permit-vpn ist nicht ausgewählt. Es muss eine Zugriffskontrollrichtlinie erstellt werden, die den Datenverkehr von den AnyConnect-Clients auf das interne Netzwerk zulässt, wie im folgenden Bild gezeigt:



Die NAT-Ausnahme kann manuell konfiguriert werden unter Policies > NAT oder wird automatisch vom Assistenten konfiguriert. Wählen Sie die interne Schnittstelle und die Netzwerke aus, die AnyConnect-Clients für den Zugriff benötigen, wie im Bild dargestellt.



Wählen Sie das AnyConnect-Paket für jedes Betriebssystem (Windows/Mac/Linux), mit dem Benutzer eine Verbindung herstellen können, wie im Bild gezeigt.

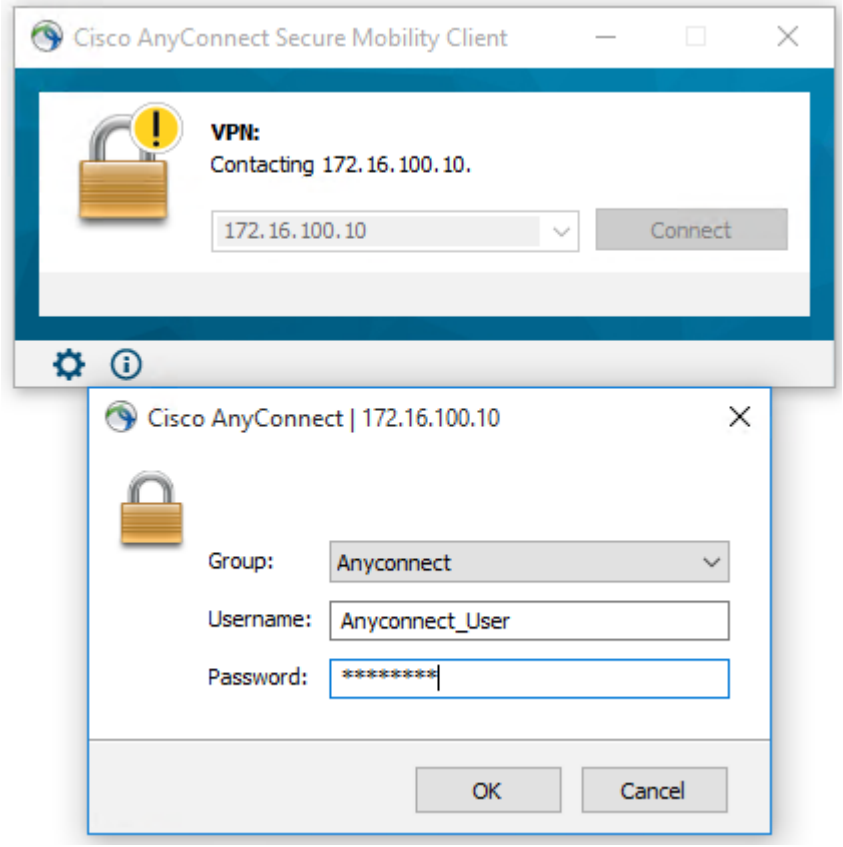


Die letzte Seite enthält eine Zusammenfassung der gesamten Konfiguration. Bestätigen Sie, dass die richtigen Parameter eingestellt wurden, und klicken Sie auf die Schaltfläche Finish (Fertig stellen), und stellen Sie die neue Konfiguration bereit.

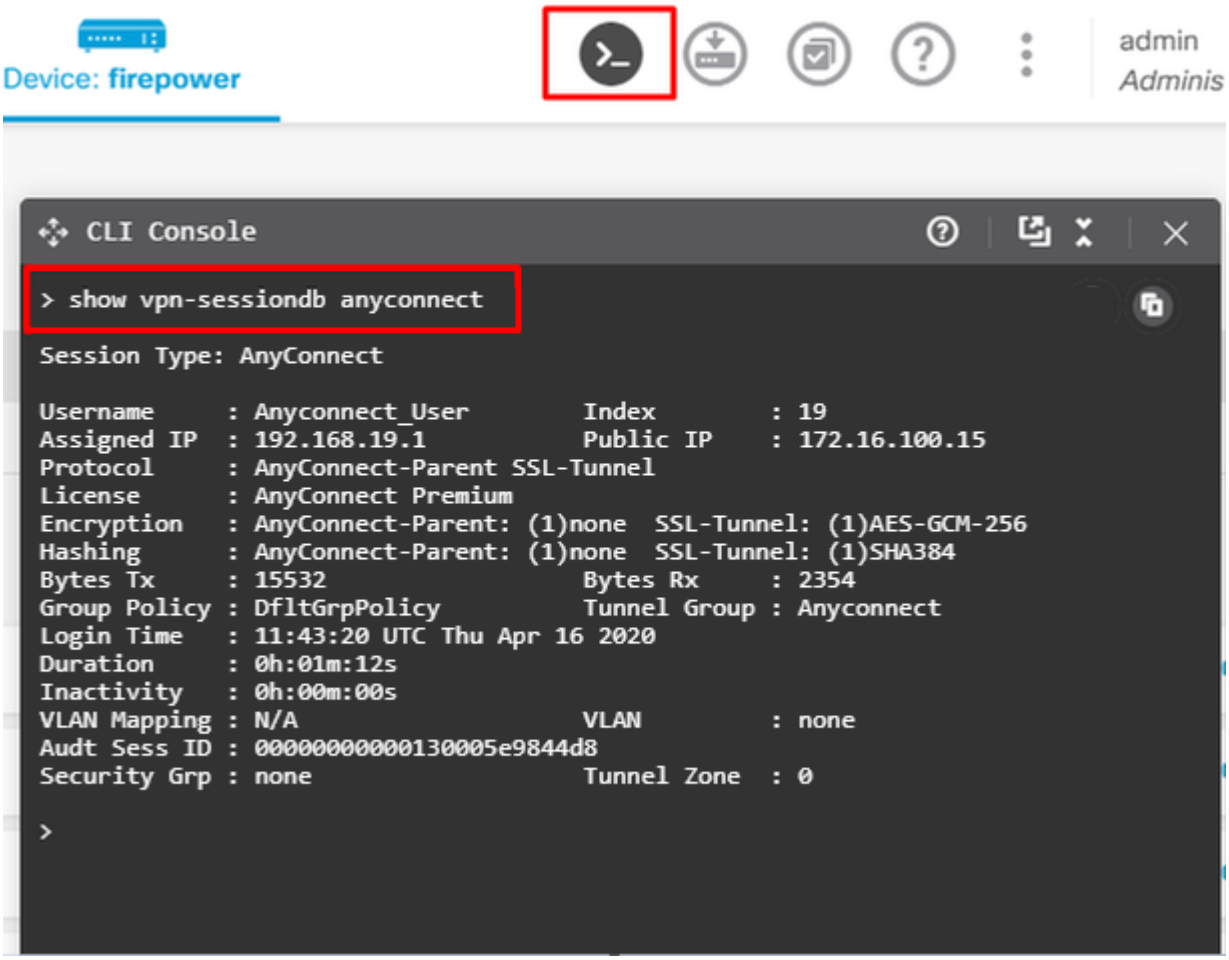
Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Versuchen Sie nach der Bereitstellung der Konfiguration, eine Verbindung herzustellen. Wenn Sie über einen FQDN verfügen, der zur externen IP-Adresse des FTD aufgelöst wird, geben Sie diesen im Feld AnyConnect-Verbindung ein. In diesem Beispiel wird die externe IP-Adresse des FTD verwendet. Verwenden Sie den Benutzernamen/das Kennwort, die/das im Objektbereich von FDM erstellt wurde, wie im Bild dargestellt.



Ab FDM 6.5.0 ist es nicht mehr möglich, die AnyConnect-Benutzer über die FDM-GUI zu überwachen. Die einzige Option besteht darin, die AnyConnect-Benutzer über die CLI zu überwachen. Die CLI-Konsole der FDM-GUI kann ebenfalls verwendet werden, um zu überprüfen, ob Benutzer verbunden sind. Verwenden Sie diesen Befehl, Show vpn-sessiondb anyconnect.



Derselbe Befehl kann direkt über die CLI ausgeführt werden.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Anyconnect_User        Index        : 15
Assigned IP  : 192.168.19.1           Public IP    : 172.16.100.15
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     : 38830                  Bytes Rx     : 172
Group Policy : DfltGrpPolicy          Tunnel Group : Anyconnect
Login Time   : 01:08:10 UTC Thu Apr 9 2020
Duration     : 0h:00m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000f0005e8e757a
Security Grp : none                   Tunnel Zone  : 0
```

Fehlerbehebung

In diesem Abschnitt finden Sie die Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Wenn ein Benutzer nicht in der Lage ist, über SSL eine Verbindung zum FTD herzustellen, gehen Sie folgendermaßen vor, um die SSL-Aushandlungsprobleme zu isolieren:

1. Überprüfen Sie, ob die IP-Adresse außerhalb von FTD über den Computer des Benutzers angepingt werden kann.
2. Verwenden Sie einen externen Sniffer, um zu überprüfen, ob der TCP-Drei-Wege-Handshake erfolgreich ist.

Probleme mit dem AnyConnect-Client

Dieser Abschnitt enthält Richtlinien zur Behebung der zwei häufigsten AnyConnect VPN Client-Probleme. Eine Anleitung zur Fehlerbehebung für den AnyConnect Client finden Sie hier: AnyConnect VPN Client Troubleshooting Guide.

Anfängliche Verbindungsprobleme

Wenn ein Benutzer erste Verbindungsprobleme hat, aktivieren Sie Debuggen. webvpn AnyConnect auf der FTD und analysieren Sie die Debug-Meldungen. Die Debugging-Vorgänge müssen über die CLI des FTD ausgeführt werden. Verwenden Sie den Befehl debug webvpn anyconnect 255.

Sammeln Sie ein DART-Paket vom Client-Computer, um die Protokolle von AnyConnect abzurufen. Anleitungen zum Sammeln eines DART-Pakets finden Sie hier: Sammeln von DART-Paketen.

Datenverkehrsspezifische Probleme

Wenn eine Verbindung erfolgreich hergestellt wird, der Datenverkehr jedoch über den SSL VPN-Tunnel ausfällt, überprüfen Sie anhand der Datenverkehrsstatistiken auf dem Client, ob der Datenverkehr vom Client empfangen und übertragen wird. Detaillierte Client-Statistiken sind in allen Versionen von AnyConnect verfügbar. Wenn der Client anzeigt, dass Datenverkehr gesendet und empfangen wird, überprüfen Sie den FTD auf empfangenen und übertragenen Datenverkehr. Wenn die FTD einen Filter anwendet, wird der Filtername angezeigt, und Sie können die ACL-Einträge überprüfen, ob Ihr Datenverkehr verloren geht. Häufige Datenverkehrsprobleme bei Benutzern:

- Routingprobleme hinter dem FTD - das interne Netzwerk kann Pakete nicht zu den zugewiesenen IP-Adressen und VPN-Clients zurückleiten.
- Zugriffskontrolllisten blockieren Datenverkehr
- Network Address Translation wird für VPN-Datenverkehr nicht umgangen

Weitere Informationen zu Remote Access-VPNs auf dem von FDM verwalteten FTD finden Sie im vollständigen Konfigurationsleitfaden: Remote Access FTD verwaltet von FDM.

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.