Konfigurieren des AnyConnect VPN-Clients auf FTD: Freistellung für Hairpin und NAT

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der Remote Access VPN-Lösung von Cisco (AnyConnect) mit FirePOWER Threat Defense (FTD) v6.3 beschrieben, die von FMC verwaltet wird.

Voraussetzungen

Anforderungen

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

- Grundlegendes VPN für Remote-Zugriff, Secure Sockets Layer (SSL) und Internet Key Exchange Version 2 (IKEv2)
- AAA- (Basic Authentication, Authorization, and Accounting) und RADIUS-Kenntnisse
- Grundlegendes FMC-Wissen
- FTD-Basiswissen

Verwendete Komponenten

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

- Cisco FMC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

In diesem Dokument wird das Verfahren zur Konfiguration einer Cisco Remote Access VPN-Lösung (AnyConnect) auf Firepower Threat Defense (FTD), Version 6.3, beschrieben, die vom Firepower Management Center (FMC) verwaltet wird.

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

Dieses Dokument soll die Konfiguration auf FTD-Geräten behandeln. Wenn Sie das ASA-Konfigurationsbeispiel suchen, lesen Sie das Dokument: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html

Einschränkungen:

Derzeit werden diese Funktionen von FTD nicht unterstützt, sind jedoch weiterhin auf ASA-Geräten verfügbar:

- Doppelte AAA-Authentifizierung (verfügbar für FTD-Version 6.5)
- Dynamische Zugriffsrichtlinie
- Host-Scan
- ISE-Status
- RADIUS-CoA
- VPN Load Balancer
- Lokale Authentifizierung (verfügbar auf Firepower Device Manager 6.3). Cisco Bug-ID CSCvf92680)
- LDAP-Attributzuordnung (verfügbar über FlexConfig, Cisco Bug-ID CSCvd64585)
- AnyConnect-Anpassung
- AnyConnect-Skripte
- AnyConnect-Lokalisierung
- Anwendungsbasiertes VPN
- SCEP-Proxy
- WSA-Integration
- SAML SSO (Cisco Bug-ID CSCvq90789)
- Gleichzeitige dynamische IKEv2-Kryptografiezuordnung für RA und L2L VPN
- AnyConnect-Module (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security usw.) DART ist das einzige Modul, das standardmäßig auf dieser Version installiert ist.
- TACACS, Kerberos (KCD-Authentifizierung und RSA SDI)
- Browser-Proxy

Konfigurieren

Um den VPN-Assistenten für den Remote-Zugriff im FMC zu durchlaufen, müssen folgende Schritte ausgeführt werden:

Schritt 1: Importieren eines SSL-Zertifikats

Zertifikate sind für die Konfiguration von AnyConnect unerlässlich. Für SSL und IPSec werden nur RSA-basierte Zertifikate unterstützt.

ECDSA-Zertifikate (Elliptic Curve Digital Signature Algorithm) werden in IPSec unterstützt. Es ist jedoch nicht möglich, ein neues AnyConnect-Paket oder ein neues XML-Profil bereitzustellen, wenn ECDSA-basiertes Zertifikat verwendet wird.

Es kann für IPSec verwendet werden, aber Sie müssen die AnyConnect-Pakete zusammen mit dem XML-Profil vorab bereitstellen. Alle XML-Profilaktualisierungen müssen manuell auf jeden Client übertragen werden (Cisco Bug-ID CSCtx42595).

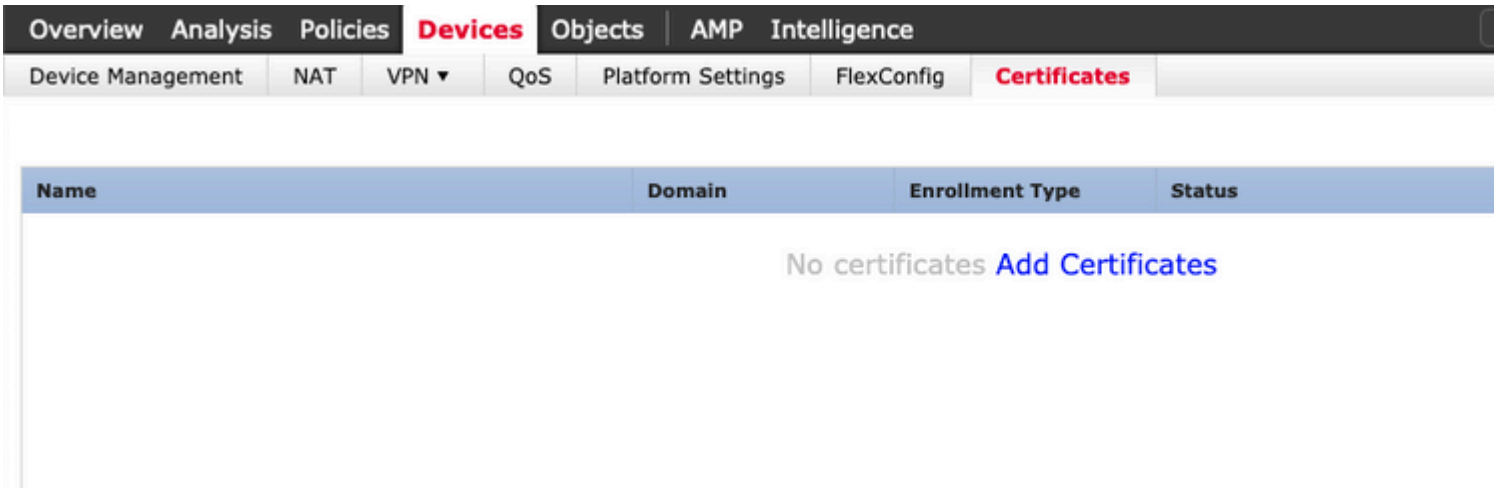
Darüber hinaus muss das Zertifikat eine Common Name (CN)-Erweiterung mit DNS-Name und/oder IP-Adresse enthalten, um Fehler aufgrund eines nicht vertrauenswürdigen Serverzertifikats in Webbrowsern zu vermeiden.

Hinweis: Auf FTD-Geräten ist das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) erforderlich, bevor die CSR (Certificate Signing Request) generiert wird.

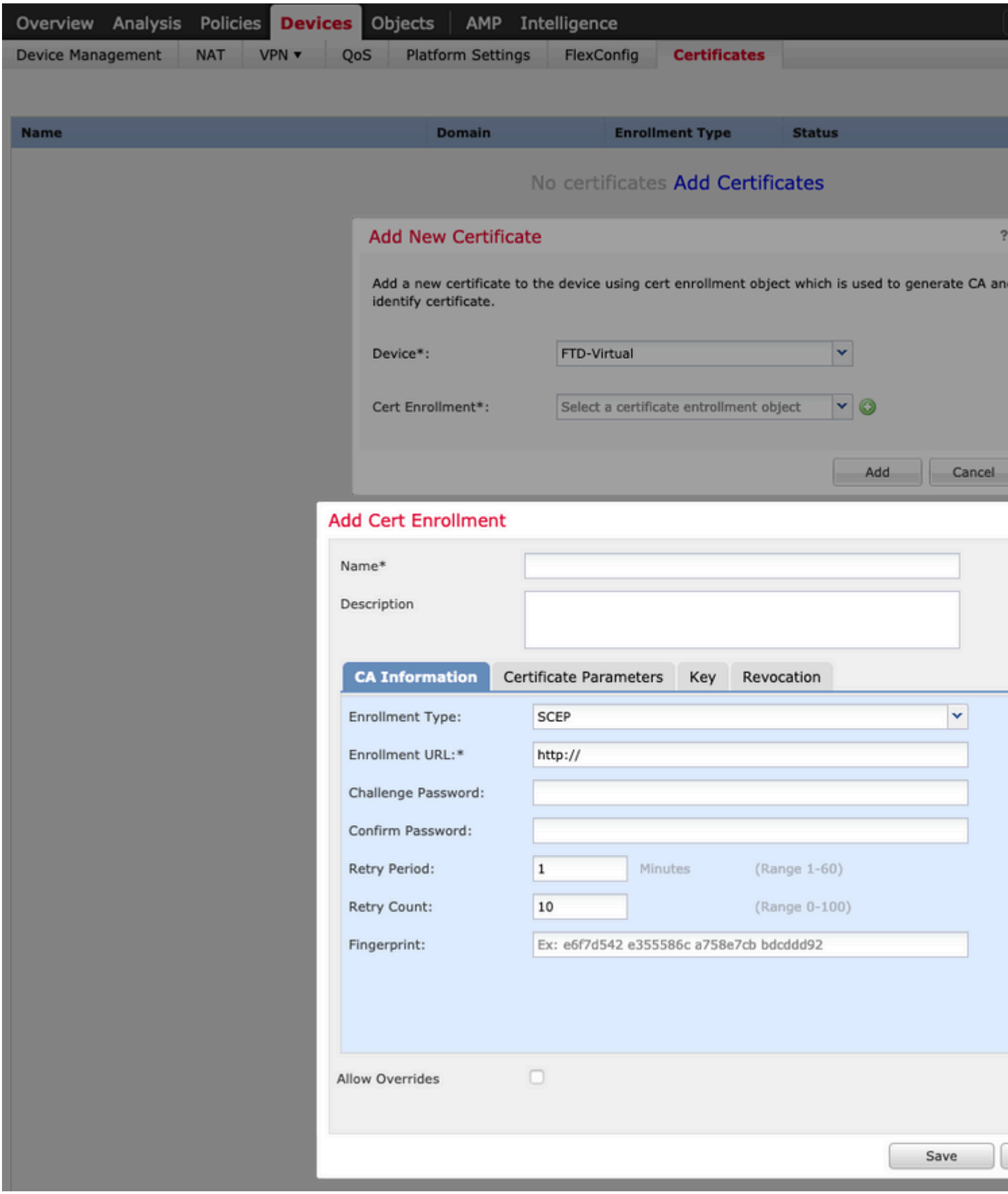
- Wenn der CSR auf einem externen Server (wie Windows Server oder OpenSSL) generiert wird, ist die **manuelle Registrierungsmethode** zum Scheitern verurteilt, da FTD die manuelle Schlüsselregistrierung nicht unterstützt.
- Es muss eine andere Methode wie PKCS12 verwendet werden.

Um ein Zertifikat für die FTD-Appliance mit der manuellen Registrierungsmethode zu erhalten, muss eine CSR generiert werden, diese mit einer Zertifizierungsstelle signieren und dann das Identitätszertifikat importieren.

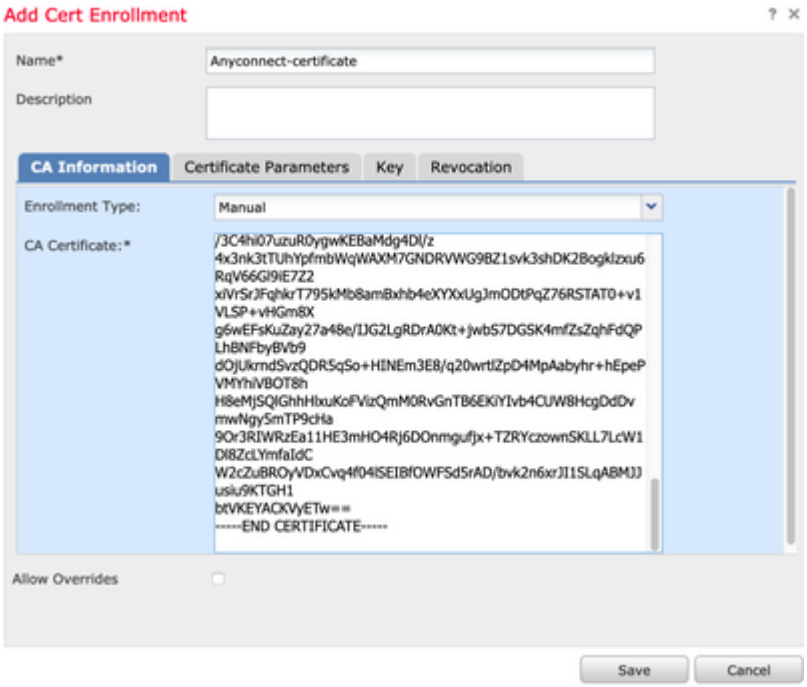
1. Navigieren Sie zu **Geräte > Zertifikate,** und wählen Sie **Hinzufügen** aus, wie im Bild dargestellt.



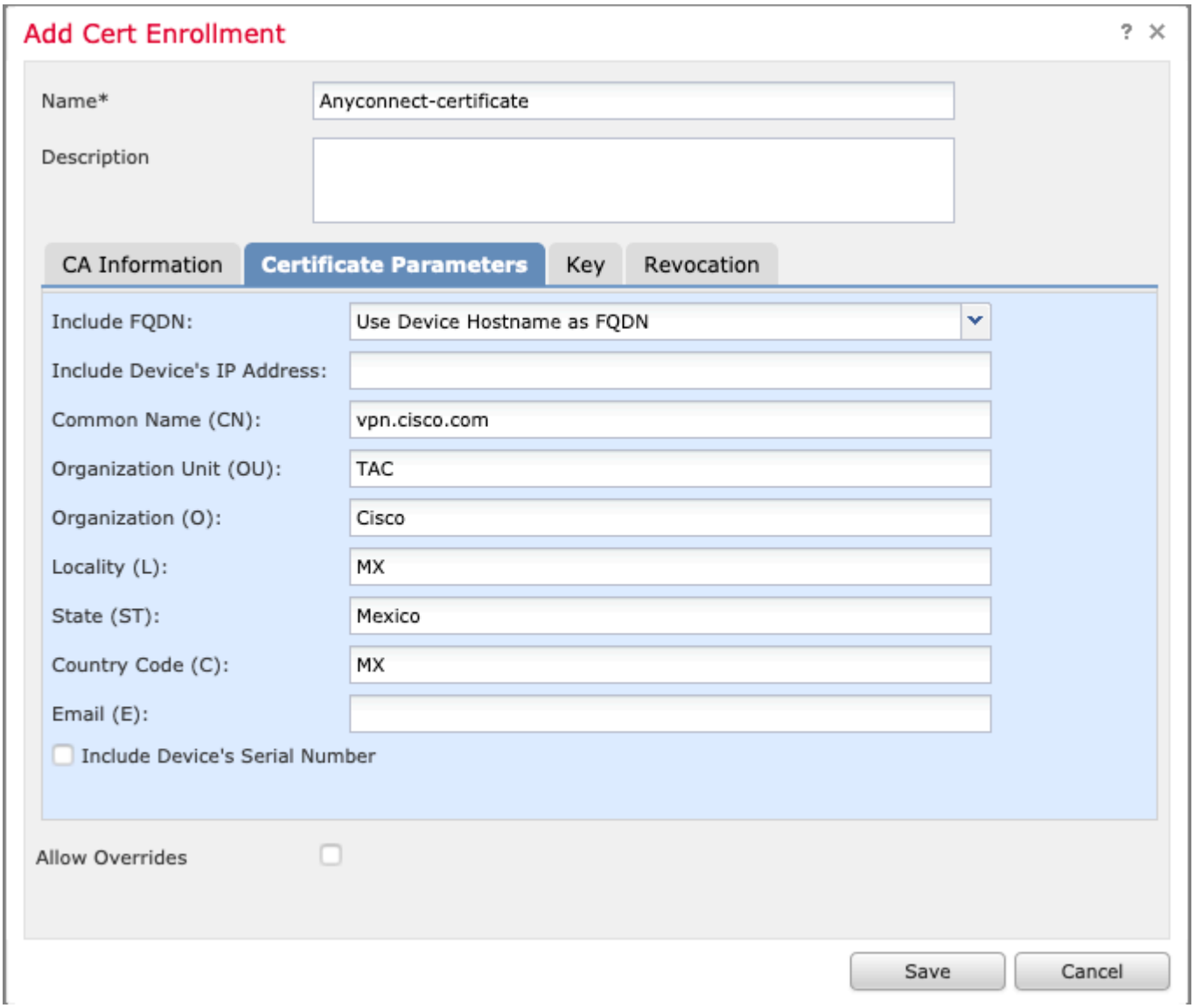
2. Wählen Sie das **Gerät aus**, und fügen Sie ein neues **Zertifikatregistrierungs**-Objekt hinzu, wie im Bild dargestellt.



3. Wählen Sie die manuelle **Registrierungsart**, und fügen Sie das CA-Zertifikat (das Zertifikat, das den CSR signieren soll) ein.

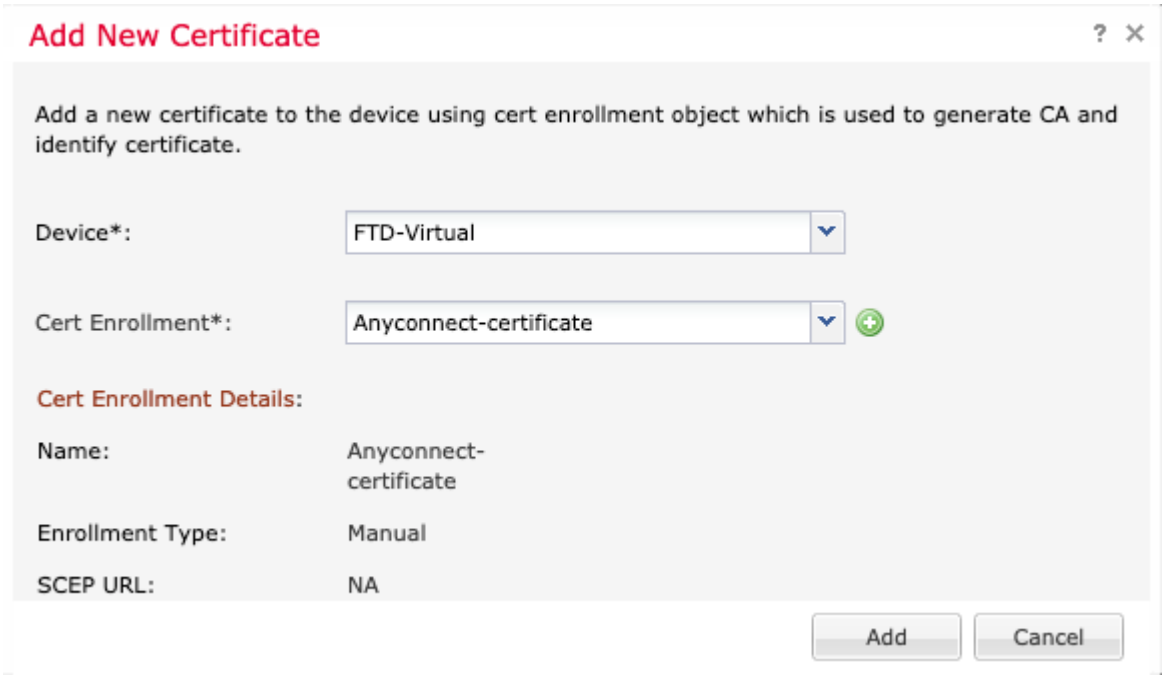


4. Wählen Sie die Registerkarte **Zertifikatsparameter** und wählen Sie "Benutzerdefinierter FQDN" für das Feld **FQDN einschließen** und füllen Sie die Zertifikatdetails aus, wie im Bild dargestellt.

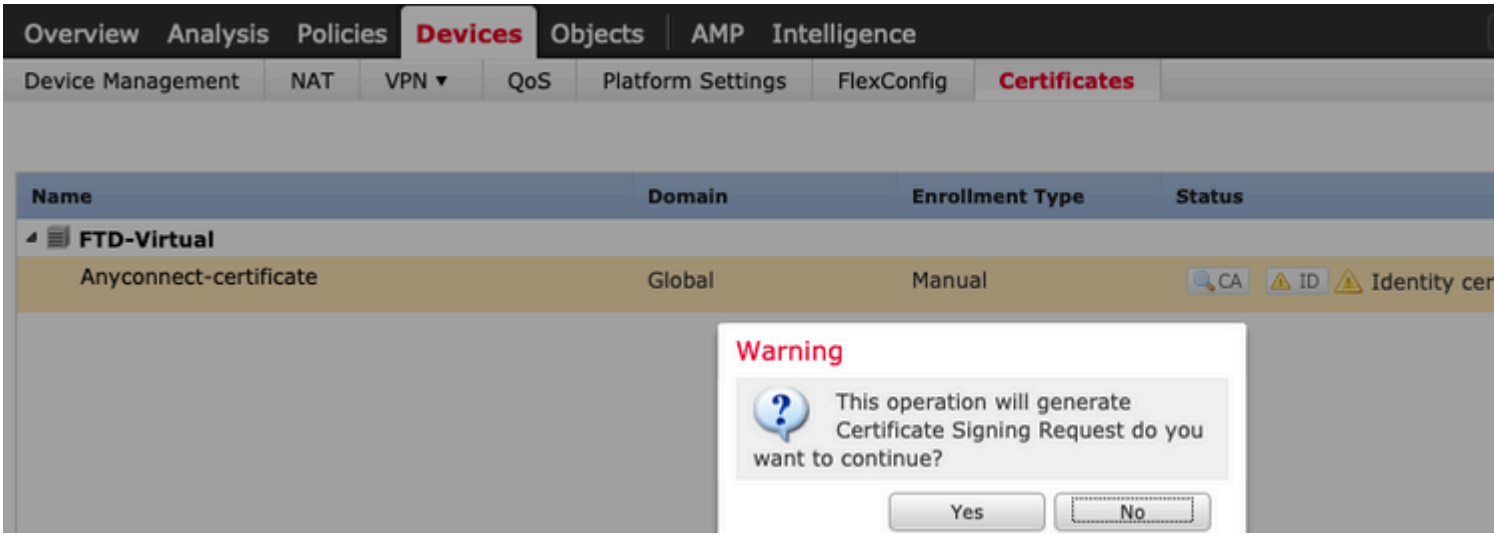


5. Wählen Sie die Registerkarte **Schlüssel**, und wählen Sie die Art der Taste, können Sie Name und Größe wählen. Für RSA sind mindestens 2048 Byte erforderlich.

6. Wählen Sie speichern, bestätigen Sie das **Gerät,** und wählen Sie unter **Zertifikatregistrierung** den soeben erstellten Vertrauenspunkt aus, und wählen Sie **Hinzufügen aus,** um das Zertifikat bereitzustellen.

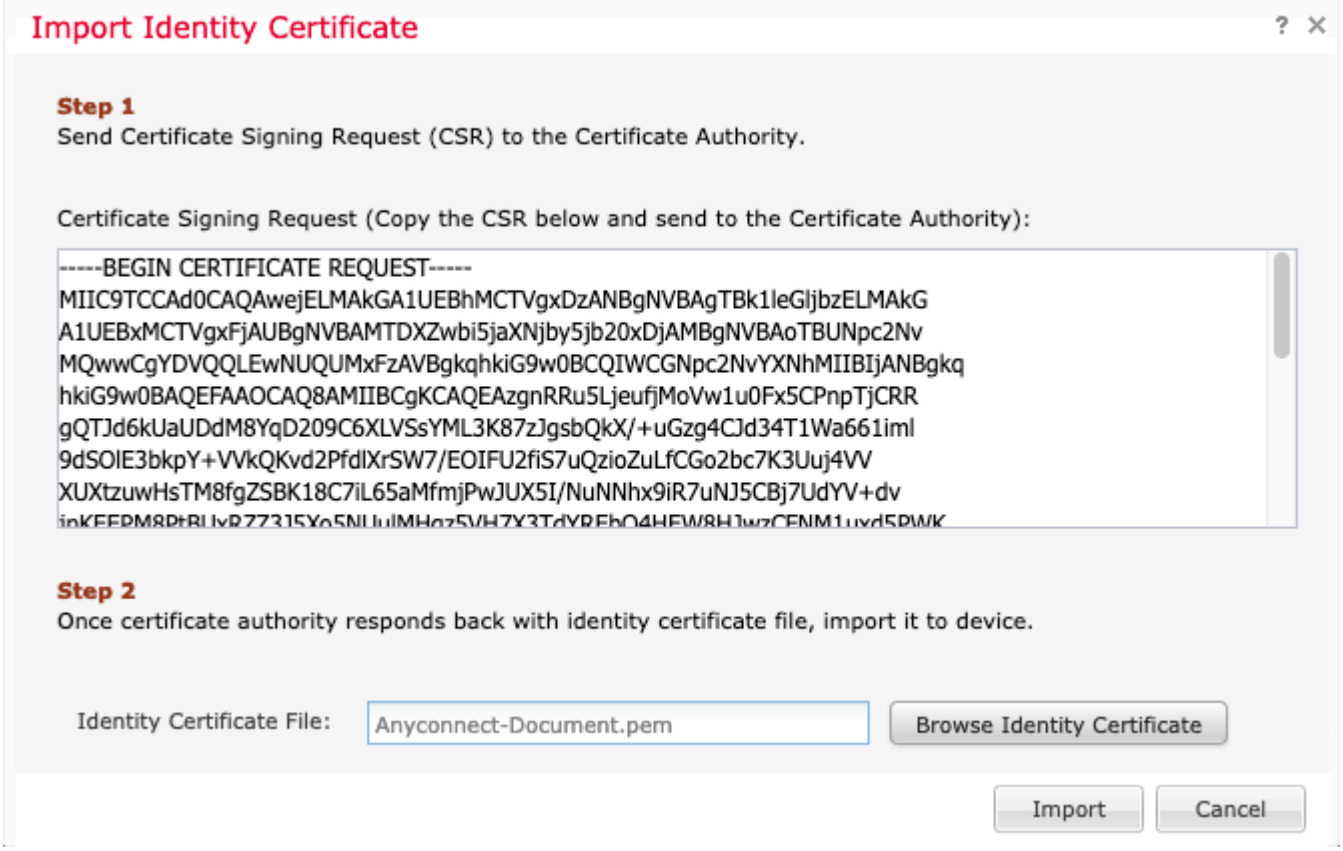


7. Wählen Sie in der Spalte **Status** das **ID**-Symbol, und wählen Sie **Ja**, um die CSR-Anfrage wie im Bild dargestellt zu erstellen.

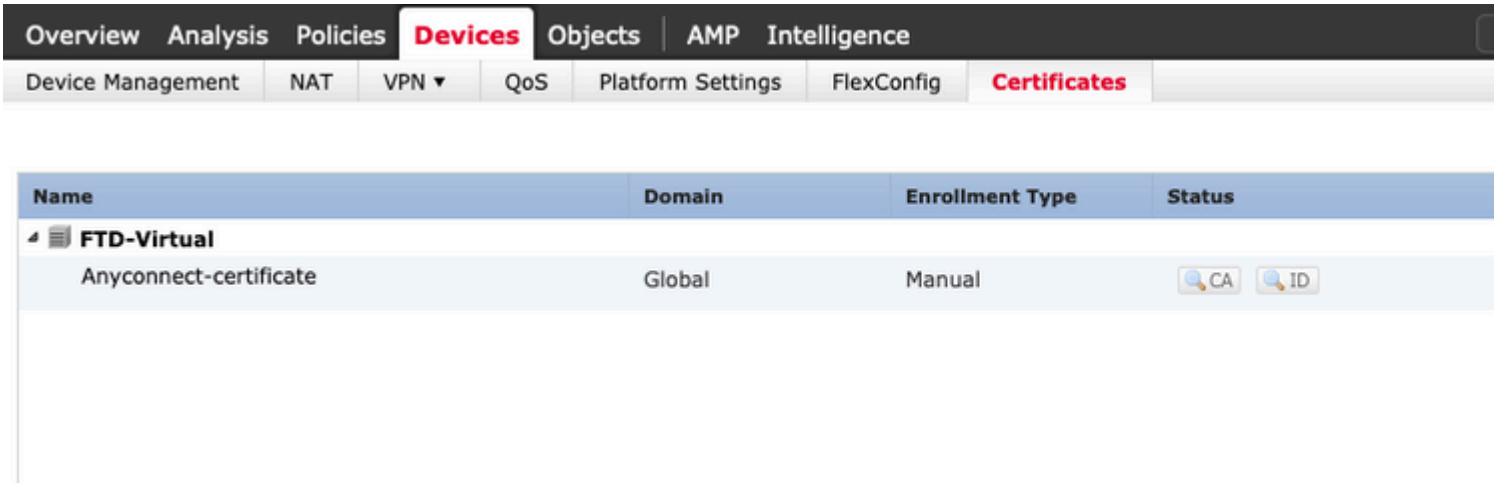


8. Kopieren Sie die CSR-Datei und signieren Sie sie mit Ihrer bevorzugten Zertifizierungsstelle (z. B. GoDaddy oder DigiCert).

9. Sobald das Identitätszertifikat von der Zertifizierungsstelle empfangen wurde (muss im Base64-Format vorliegen), wählen Sie **Identitätszertifikat durchsuchen** und suchen Sie das Zertifikat auf dem lokalen Computer. Wählen Sie **Importieren aus.**



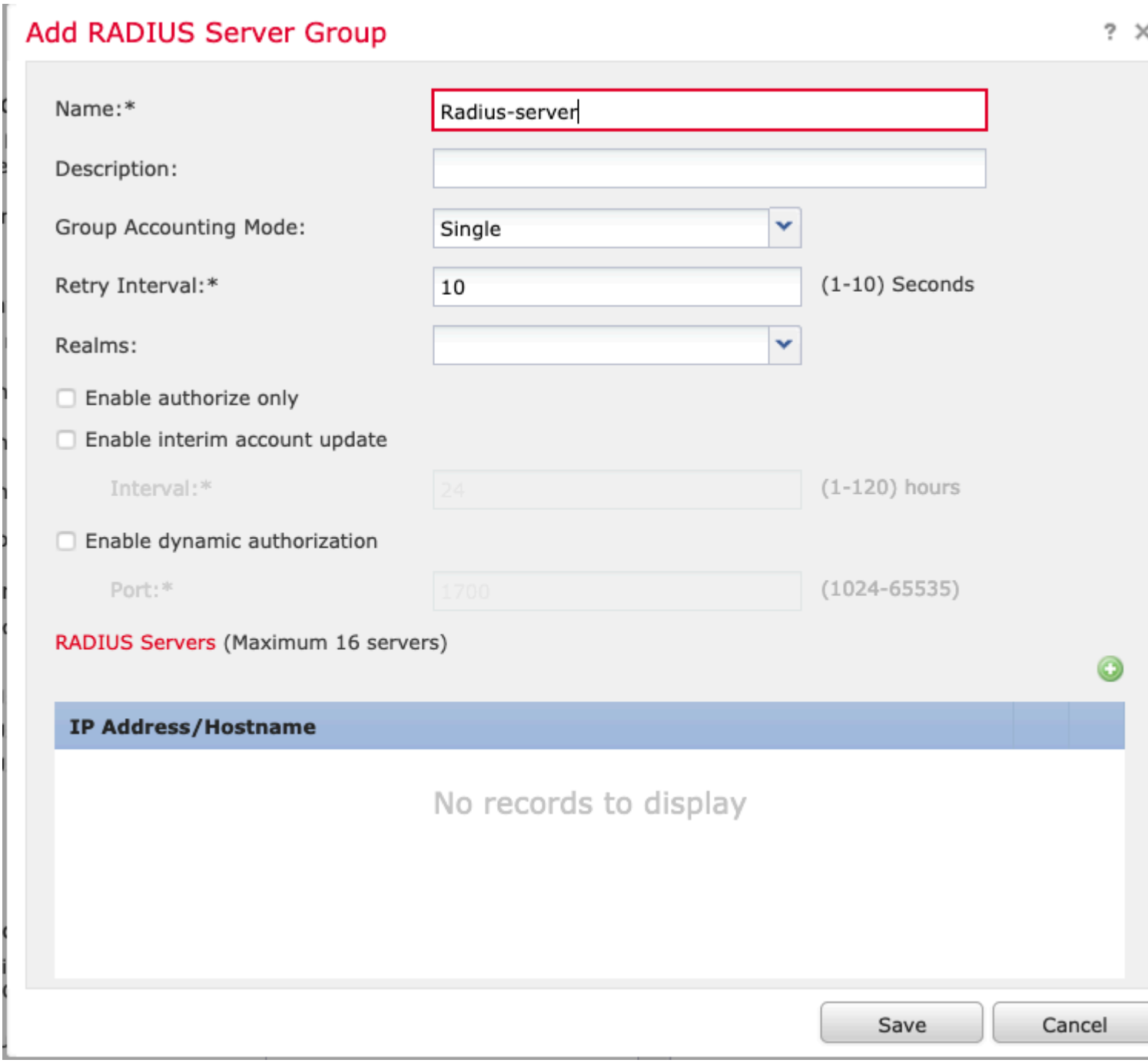
10. Nach dem Import stehen sowohl die CA- als auch die ID-Zertifikatdetails zur Anzeige zur Verfügung.



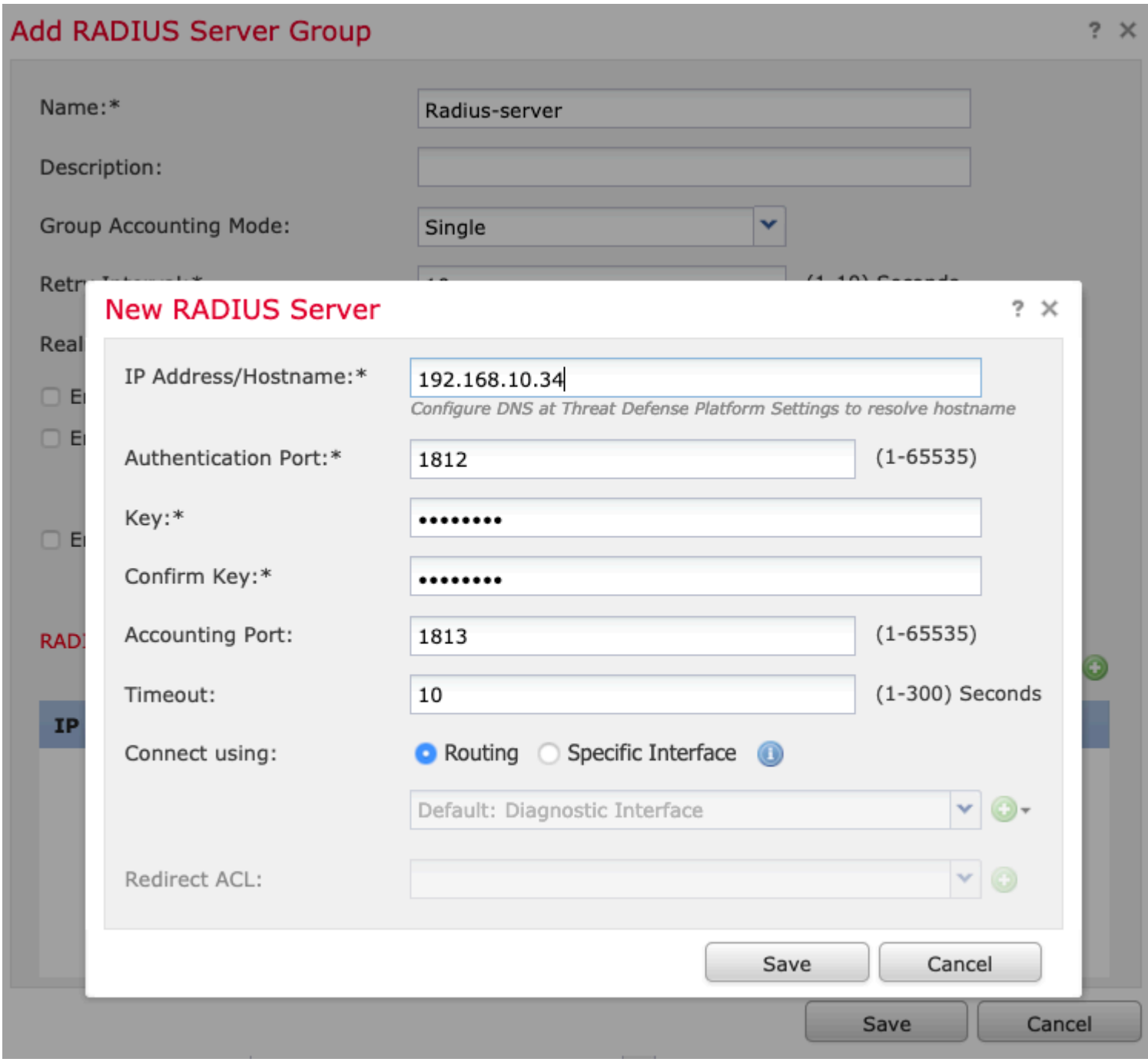
Schritt 2: Konfigurieren eines RADIUS-Servers

Auf von FMC verwalteten FTD-Geräten wird die lokale Benutzerdatenbank nicht unterstützt. Es muss eine andere Authentifizierungsmethode wie RADIUS oder LDAP verwendet werden.

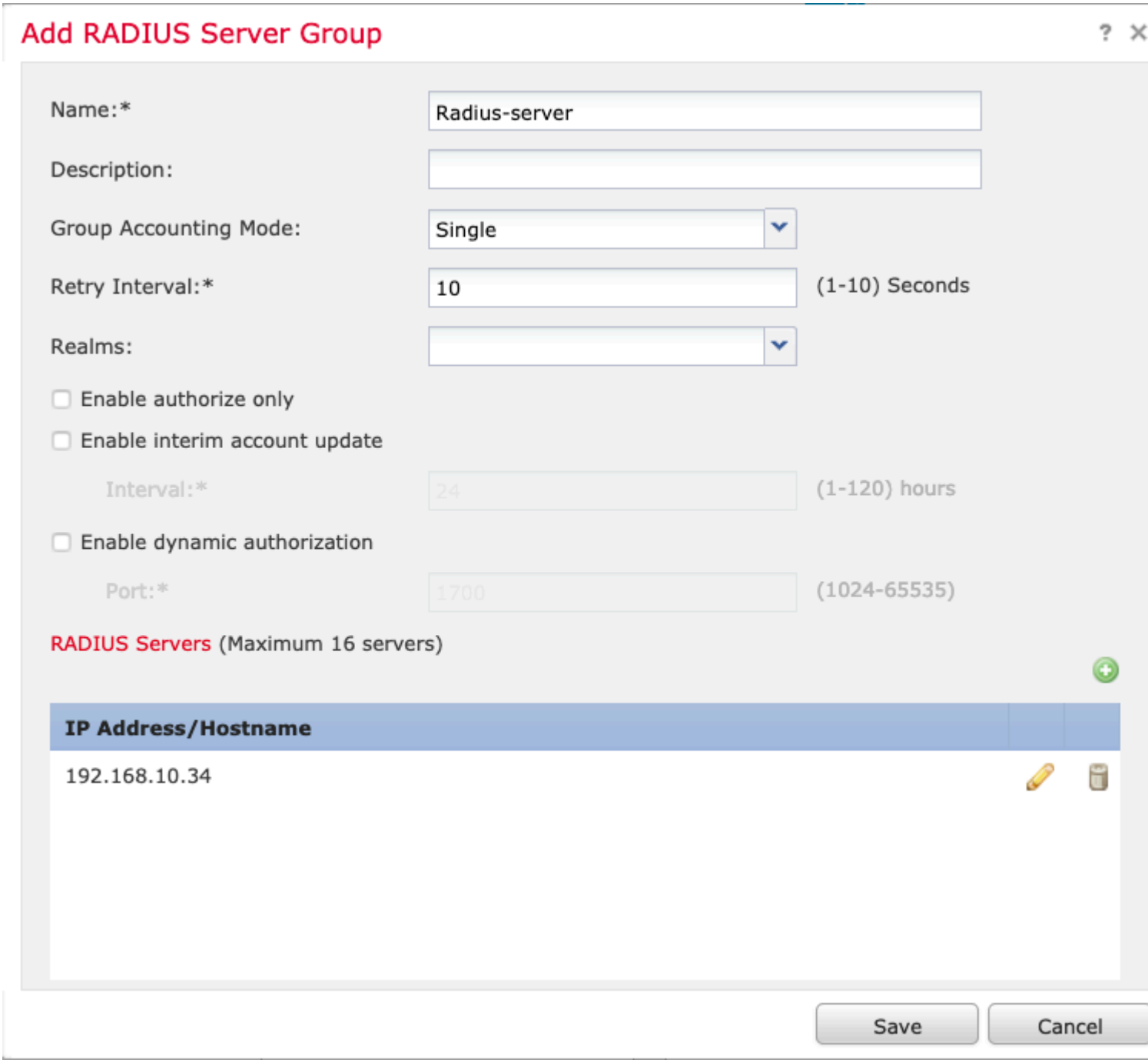
1. Navigieren Sie zu **Objekte** > **Objektverwaltung** > **RADIUS-Servergruppe** > **RADIUS-Servergruppe hinzufügen,** wie im Bild dargestellt.



2. Weisen Sie der **Radius-Servergruppe** einen Namen zu, und fügen Sie die Radius-Server-IP-Adresse zusammen mit einem gemeinsamen geheimen Schlüssel hinzu (der gemeinsame geheime Schlüssel ist erforderlich, um die FTD mit dem Radius-Server zu koppeln). Wählen Sie **Speichern,** wenn dieses Formular wie im Bild dargestellt ausgefüllt wurde.



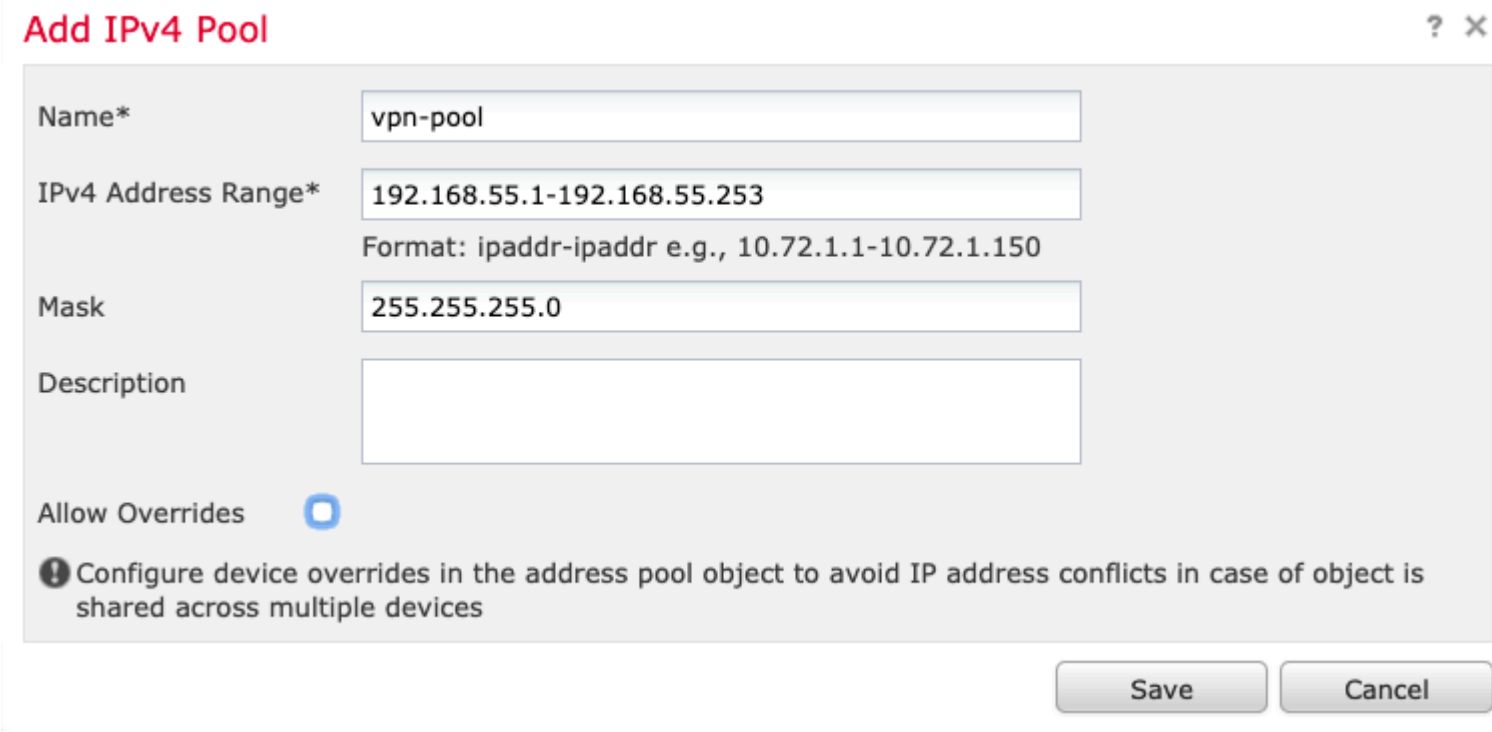
3. Die RADIUS-Serverinformationen sind jetzt in der RADIUS-Serverliste verfügbar, wie im Bild dargestellt.



Schritt 3: IP-Pool erstellen

1. Navigieren Sie zu **Objekte** > **Objektverwaltung** > **Adresspools** > **IPv4-Pools hinzufügen**.

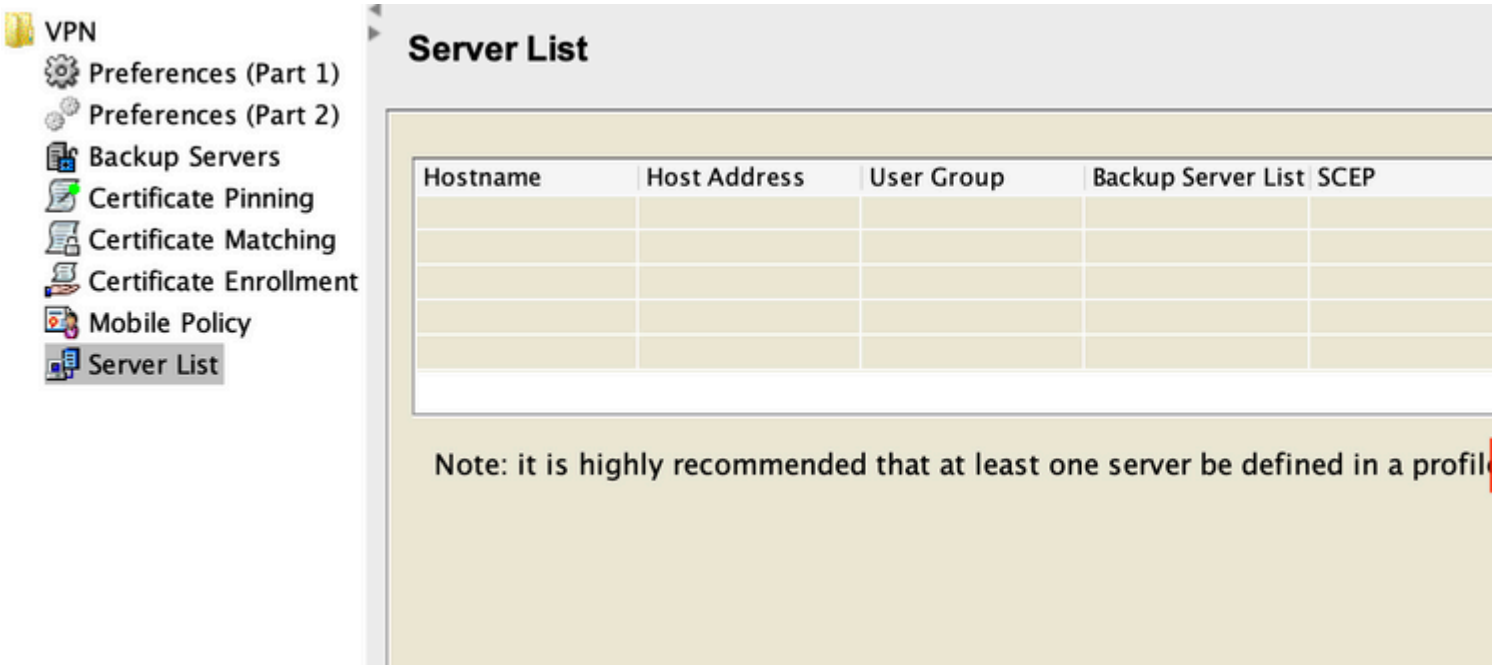
2. Weisen Sie den Namen und den Bereich der IP-Adressen, **Maske** Feld ist nicht erforderlich, aber es kann wie im Bild angezeigt angegeben werden.



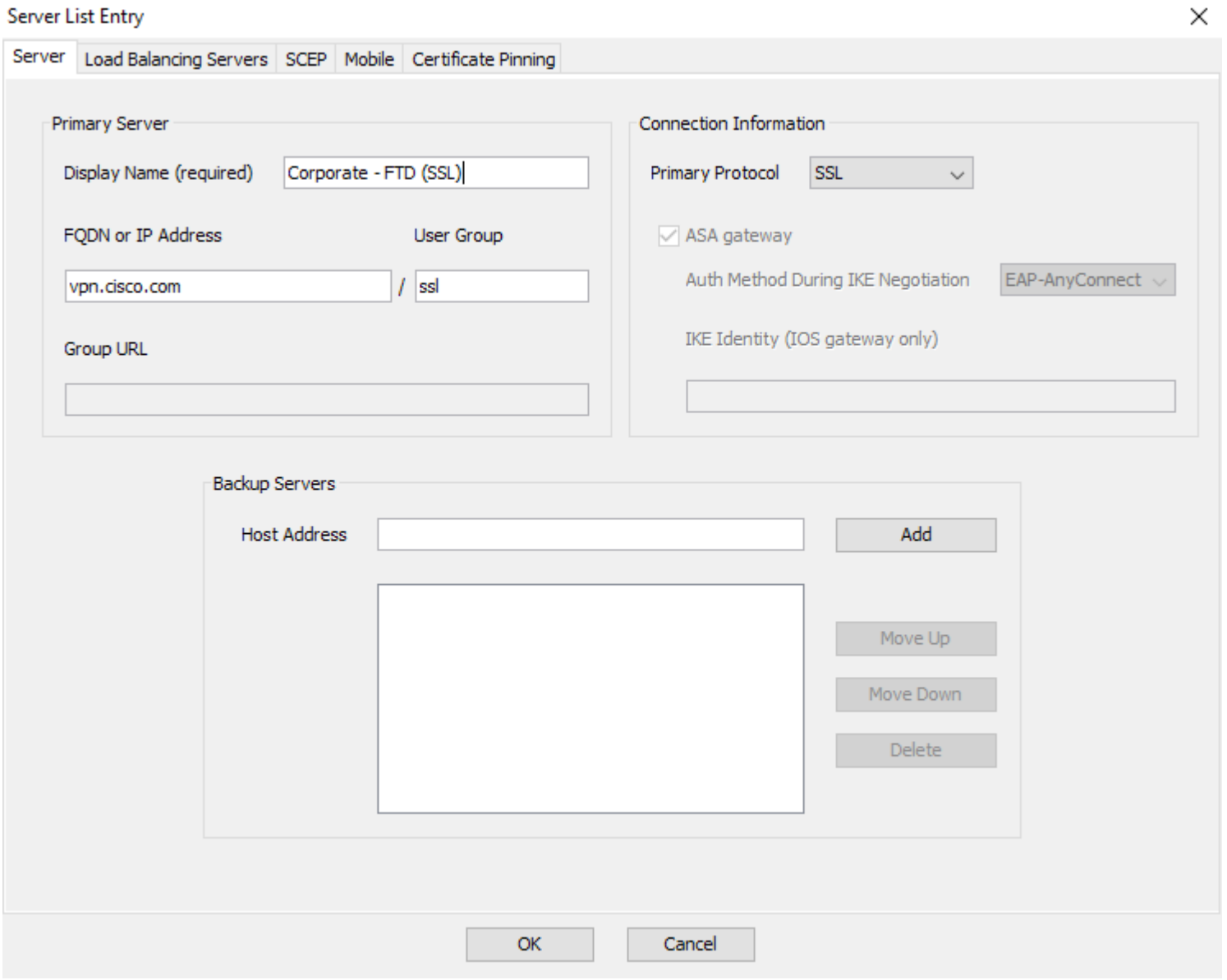
Schritt 4: XML-Profil erstellen

1. Laden Sie das **Profil-Editor**-Tool von Cisco.com herunter, und führen Sie die Anwendung aus.

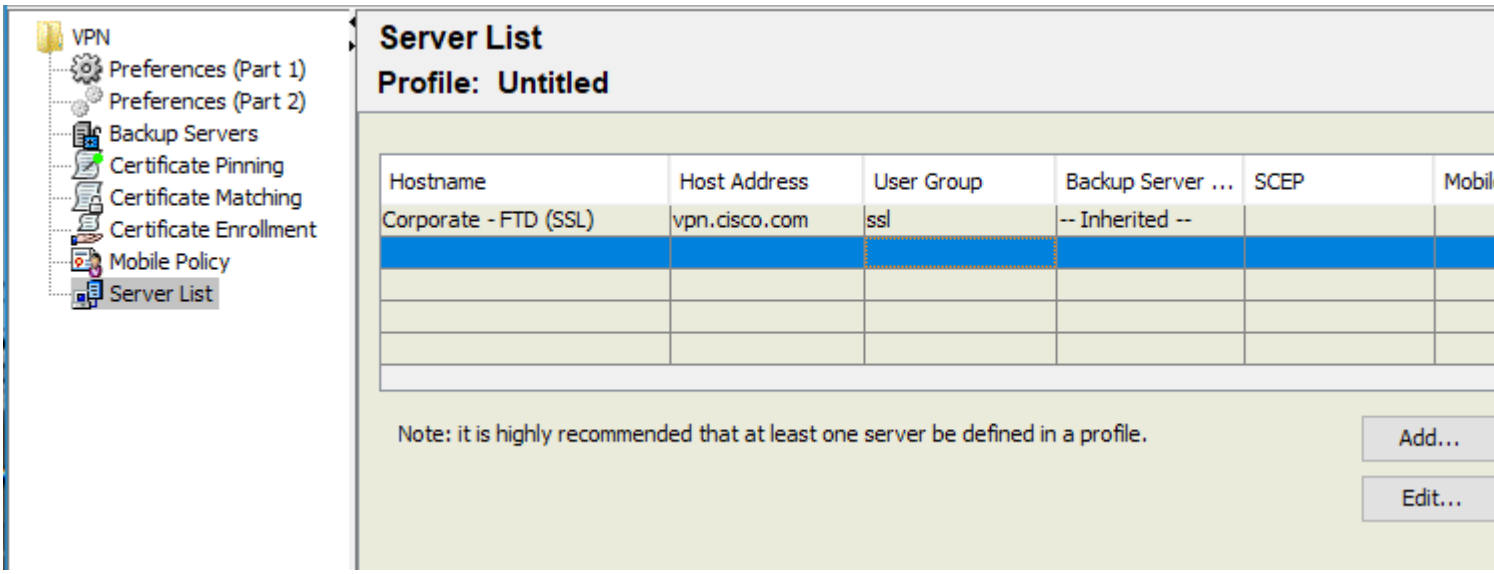
2. Navigieren Sie im Profil-Editor zu **Serverliste,** und wählen Sie **Hinzufügen** aus, wie im Bild dargestellt.



3. Weisen Sie einen **Anzeigenamen, einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder eine IP-Adresse zu,** und wählen Sie **OK**, wie im Bild dargestellt.



4. Der Eintrag ist nun im Menü **Serverliste** sichtbar:



5. Navigieren Sie zu **Datei** > **Speichern unter.**

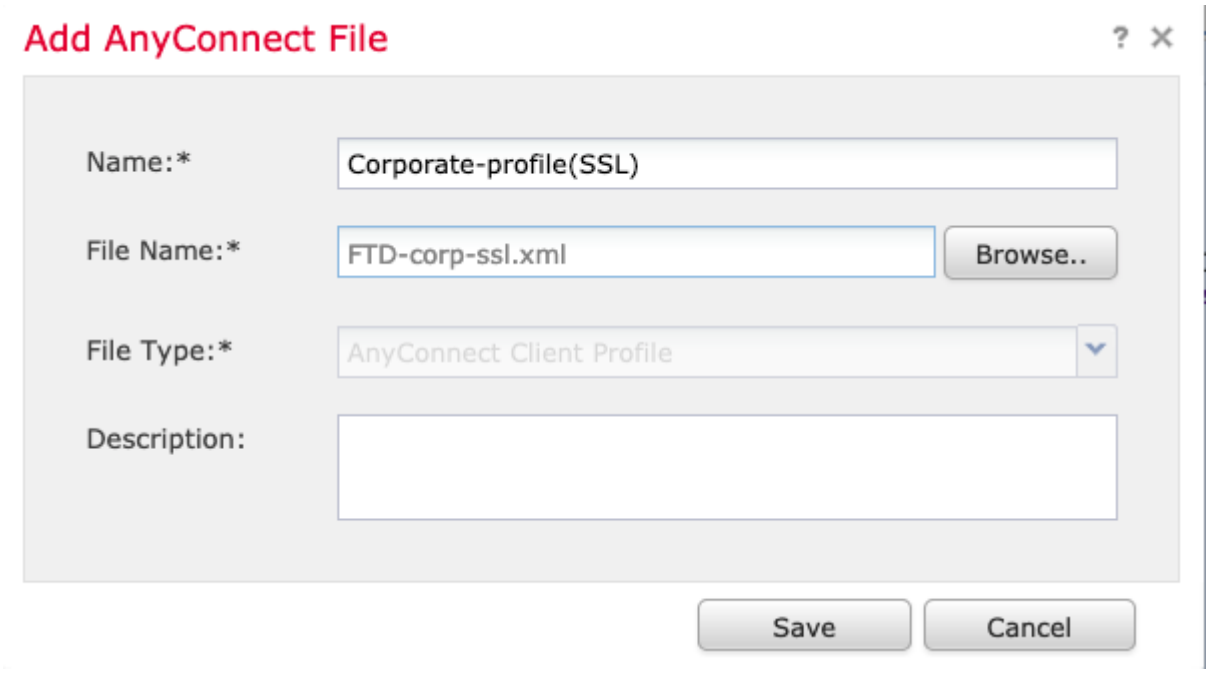
Hinweis: Speichern Sie das Profil mit einem leicht identifizierbaren Namen mit der Erweiterung **.xml**.

Schritt 5: Anyconnect XML-Profil hochladen

1. Navigieren Sie im FMC zu Objects > **Object Management** > **VPN** > **AnyConnect File** > **Add AnyConnect File** (Objekte > Objektverwaltung > **VPN** > AnyConnect-Datei hinzufügen)**.**

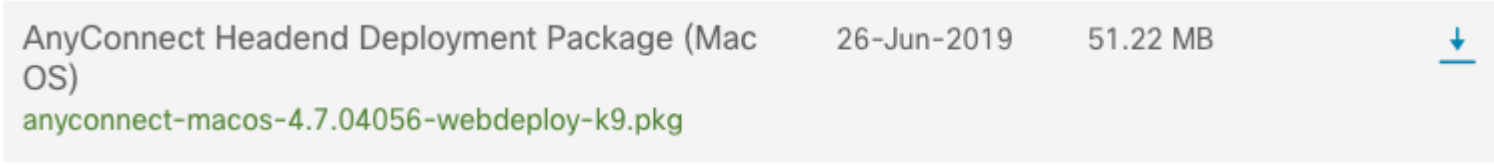
2. Weisen Sie dem Objekt einen **Namen** zu, und klicken Sie auf **Durchsuchen,** suchen Sie im lokalen System nach dem Clientprofil, und wählen Sie **Speichern aus**.

Achtung: Wählen Sie **Anyconnect Client Profile** als Dateityp aus.



Schritt 6: AnyConnect-Images hochladen

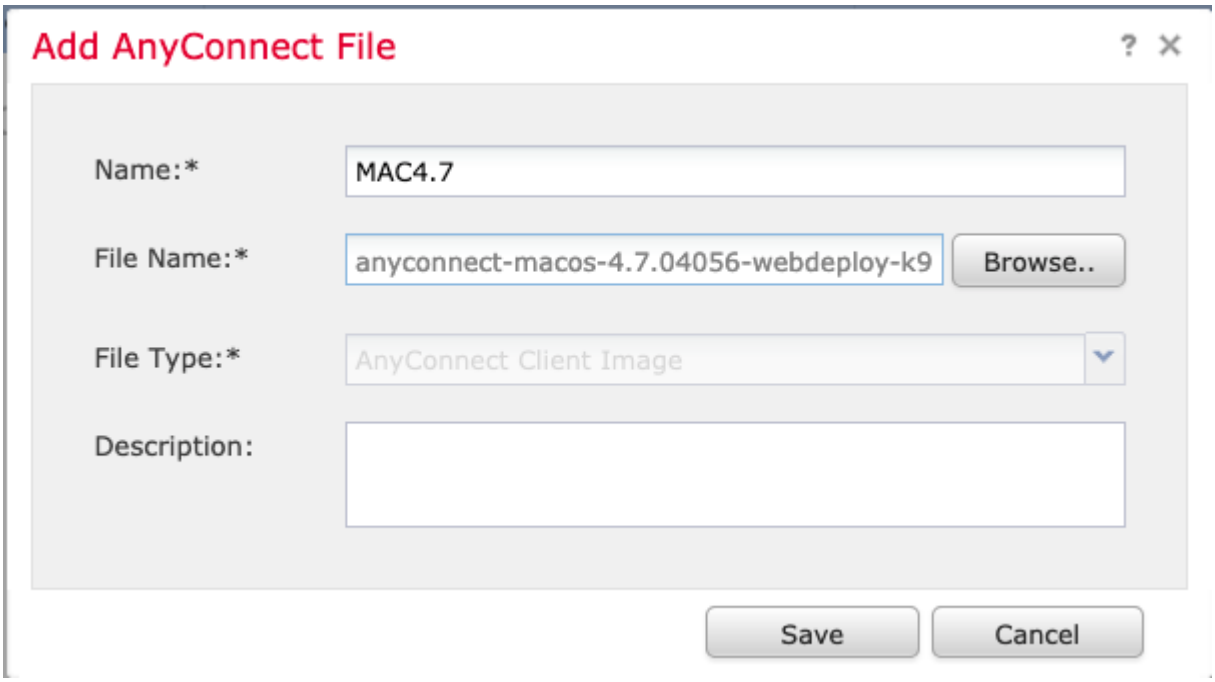
1. Laden Sie die webdeploy (**.pkg)**-Images von der Cisco Downloads-Webseite herunter.



2. Navigieren Sie zu Objects > **Object Management** > **VPN** > **AnyConnect File** > **Add AnyConnect File** (Objekte > Objektverwaltung **> VPN** > AnyConnect-Datei hinzufügen)**.**

3. Weisen Sie der Paketdatei Anyconnect einen Namen zu, und wählen Sie die **.pkg**-Datei auf Ihrem lokalen System aus, sobald die Datei ausgewählt ist.

4. Wählen Sie **Speichern**.



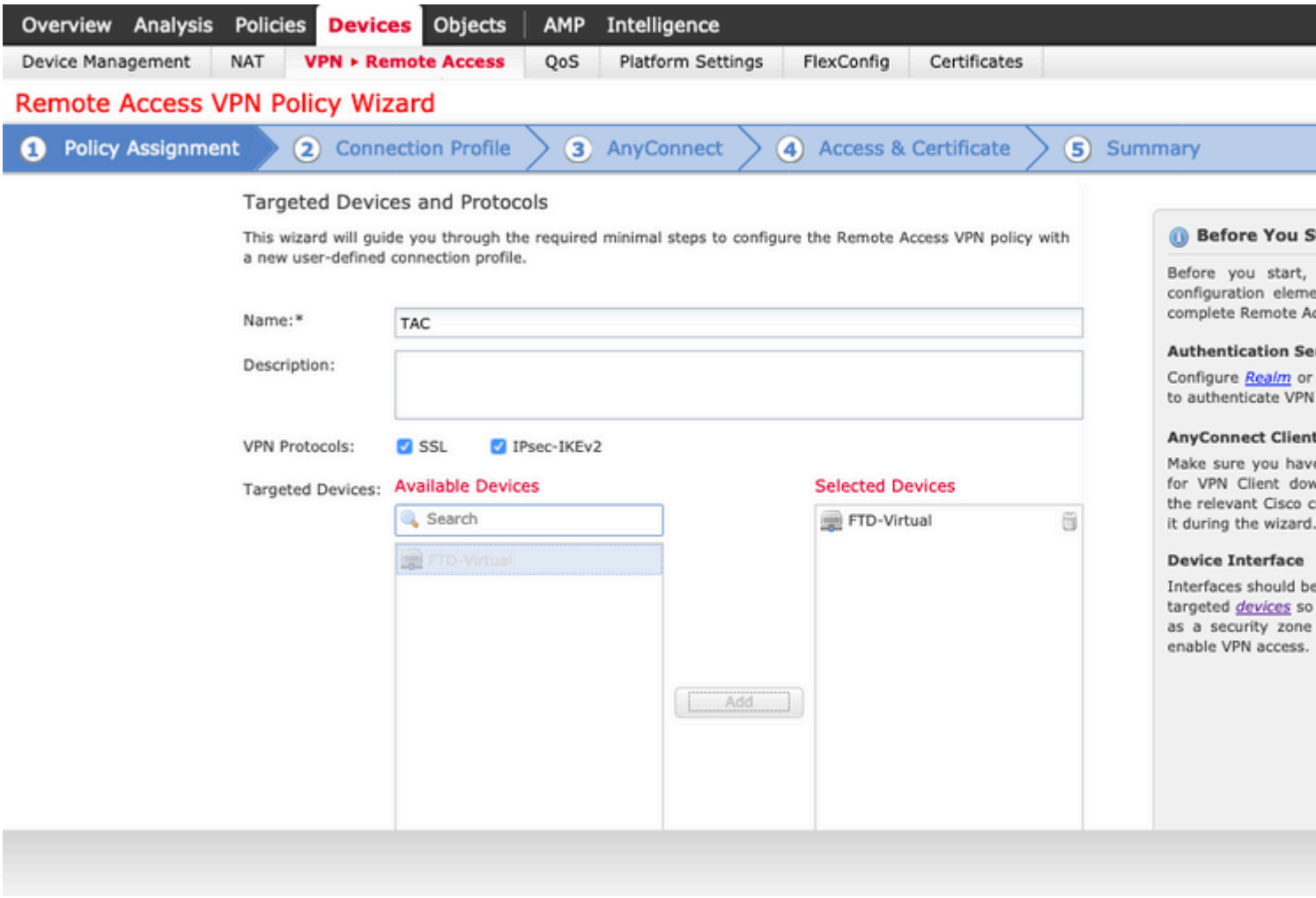
Hinweis: Je nach Ihren Anforderungen (Windows, Mac, Linux) können zusätzliche Pakete hochgeladen werden.

Schritt 7. Remotezugriff-VPN-Assistent

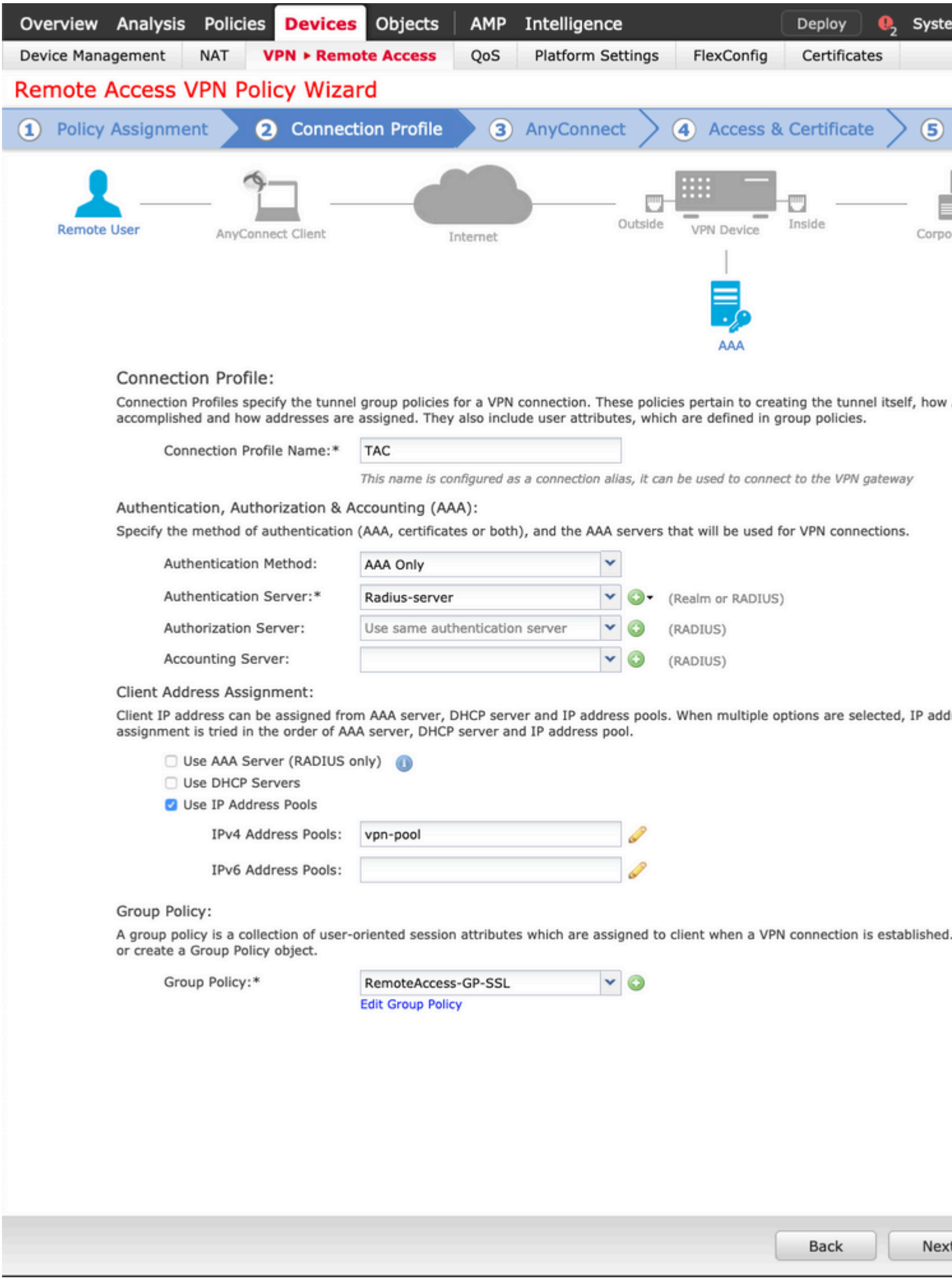
Auf der Grundlage der vorherigen Schritte kann der RAS-Assistent entsprechend ausgeführt werden.

1. Navigieren Sie zu **Geräte** > **VPN** > **RAS**.

2. Weisen Sie den Namen der RAS-Richtlinie zu, und wählen Sie ein FTD-Gerät unter **Available Devices (Verfügbare Geräte) aus**.

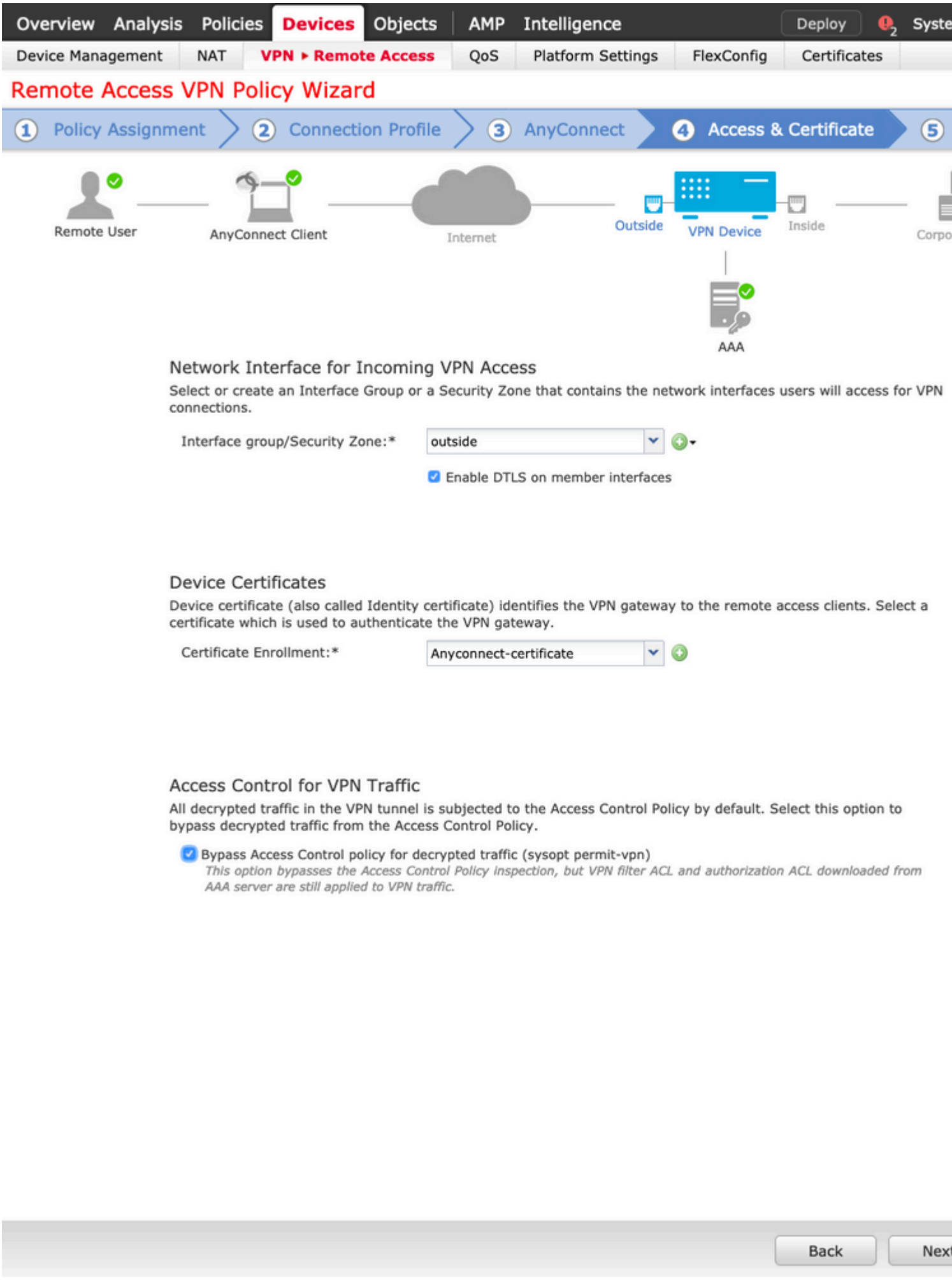


3. Weisen Sie den **Namen** des **Verbindungsprofils zu (**der Name des Verbindungsprofils ist der Name der Tunnelgruppe), und wählen Sie **Authentifizierungsserver** und **Adresspools,** wie im Bild dargestellt.



4. Wählen Sie das Symbol +, um eine **Gruppenrichtlinie** zu erstellen.

In diesem Szenario ist das FTD so konfiguriert, dass es keinen VPN-Datenverkehr untersucht. Umgehen Sie die Option Access Control Policies (ACP) (Zugriffskontrollrichtlinien) umgehen wird umgeschaltet.



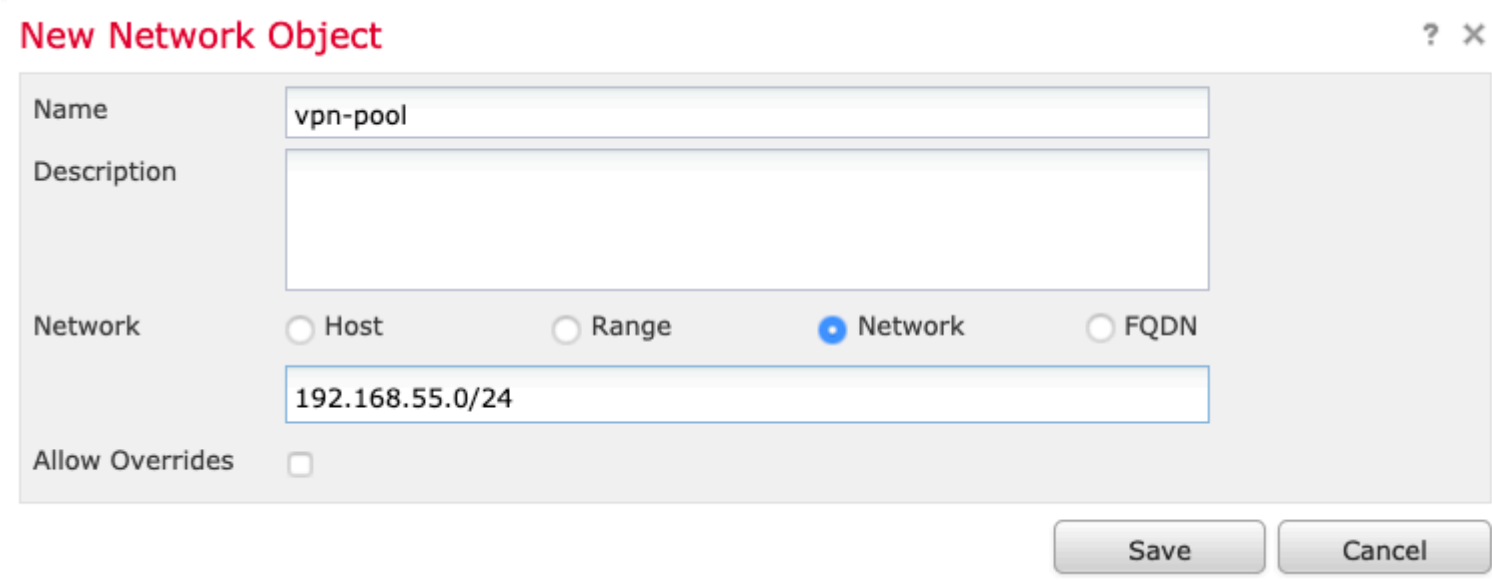
10. Wählen Sie **Beenden** und **Bereitstellen** der Änderungen:

Sämtliche VPN-, SSL-Zertifikate und AnyConnect-Pakete betreffende Konfigurationen werden per P

ist eine bevorzugte Übersetzungsmethode, um zu verhindern, dass Datenverkehr an das Internet weitergeleitet wird, wenn er über einen VPN-Tunnel (Remote-Zugriff oder Site-to-Site) fließen soll.

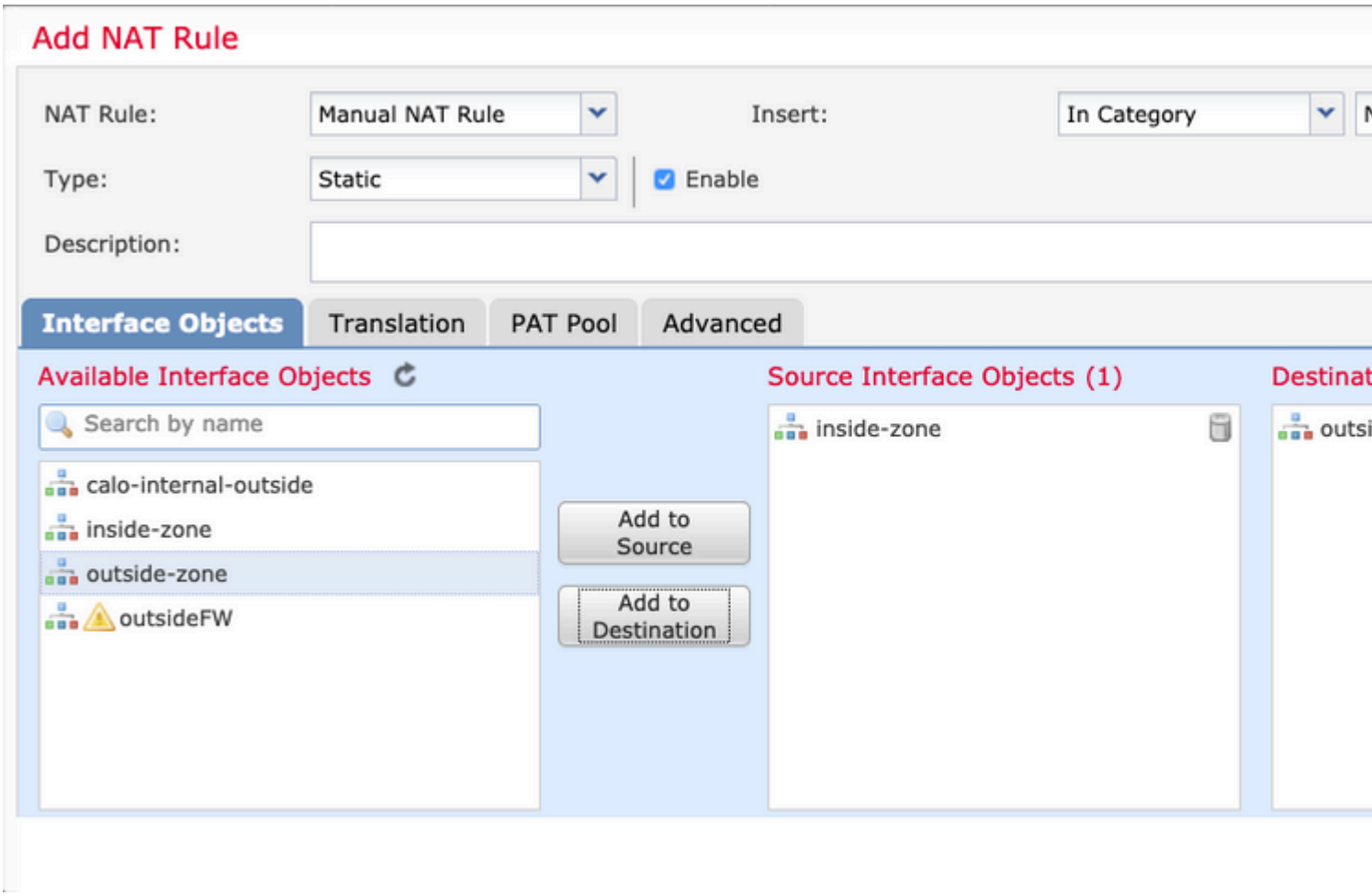
Dies ist erforderlich, wenn der Datenverkehr aus Ihrem internen Netzwerk ohne Übersetzung über die Tunnel fließen soll.

1. Navigieren Sie zu **Objekte > Netzwerk > Netzwerk hinzufügen > Objekt hinzufügen,** wie im Bild dargestellt.

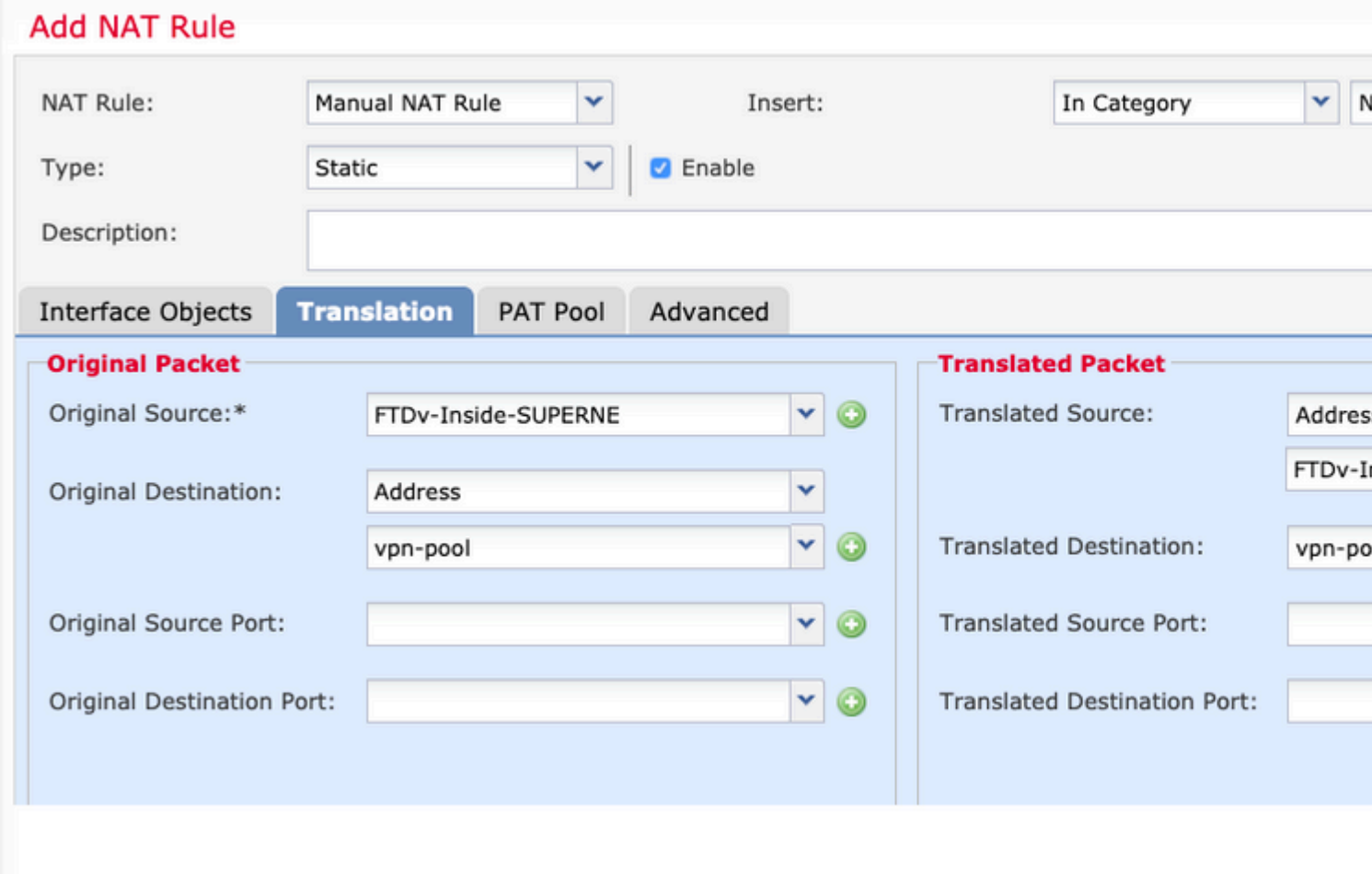


2. Navigieren Sie zu **Device > NAT,** wählen Sie die NAT-Richtlinie aus, die vom betreffenden Gerät verwendet wird, und erstellen Sie eine neue Anweisung**.**

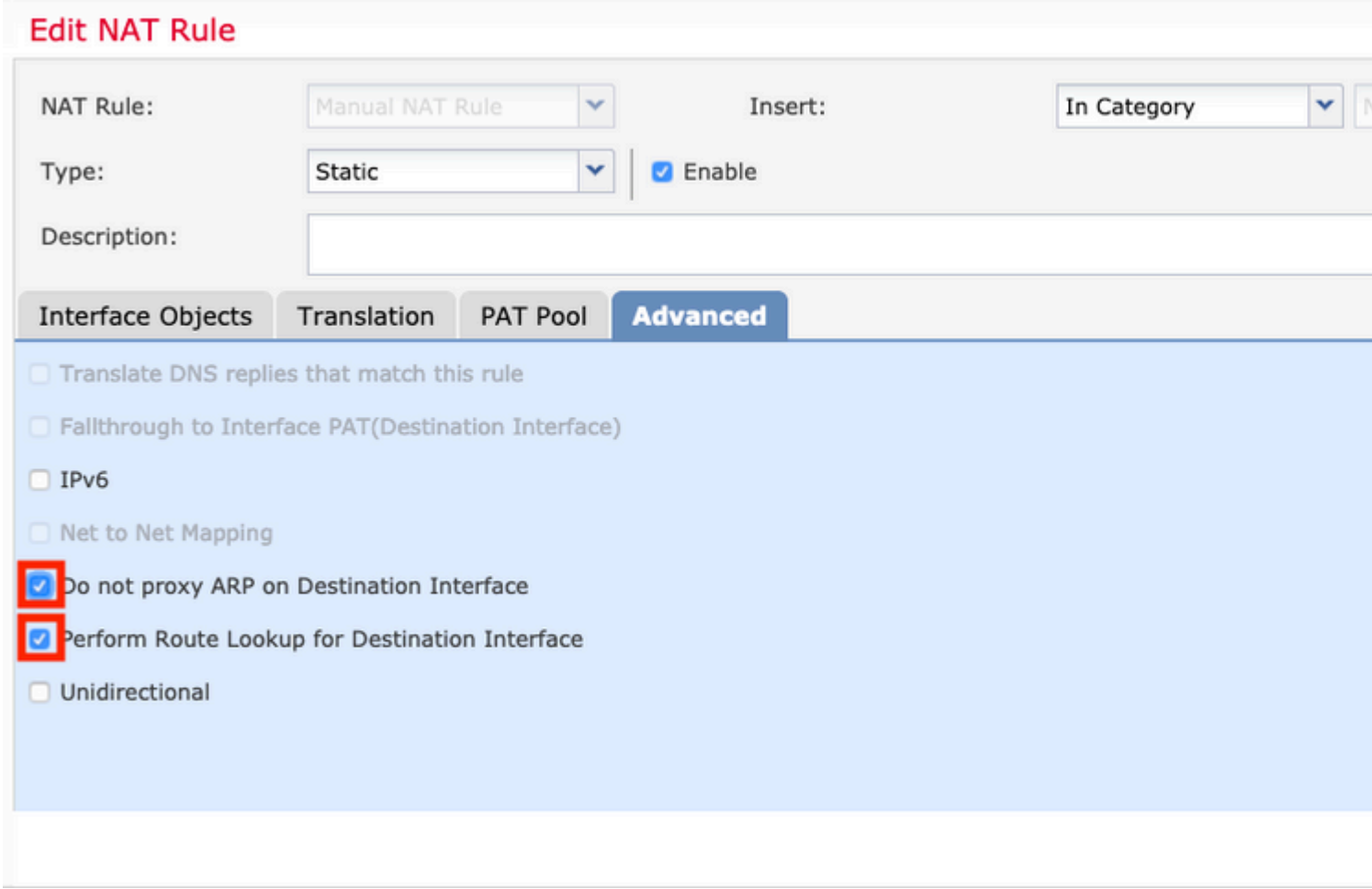
Hinweis: Der Datenverkehrsfluss verläuft von innen nach außen.



3. Wählen Sie die internen Ressourcen hinter dem FTD (**ursprüngliche Quelle** und **übersetzte Quelle)** und das Ziel als lokalen IP-Pool für die Anyconnect-Benutzer (**ursprüngliches Ziel** und **übersetztes Ziel), wie im** Bild dargestellt.

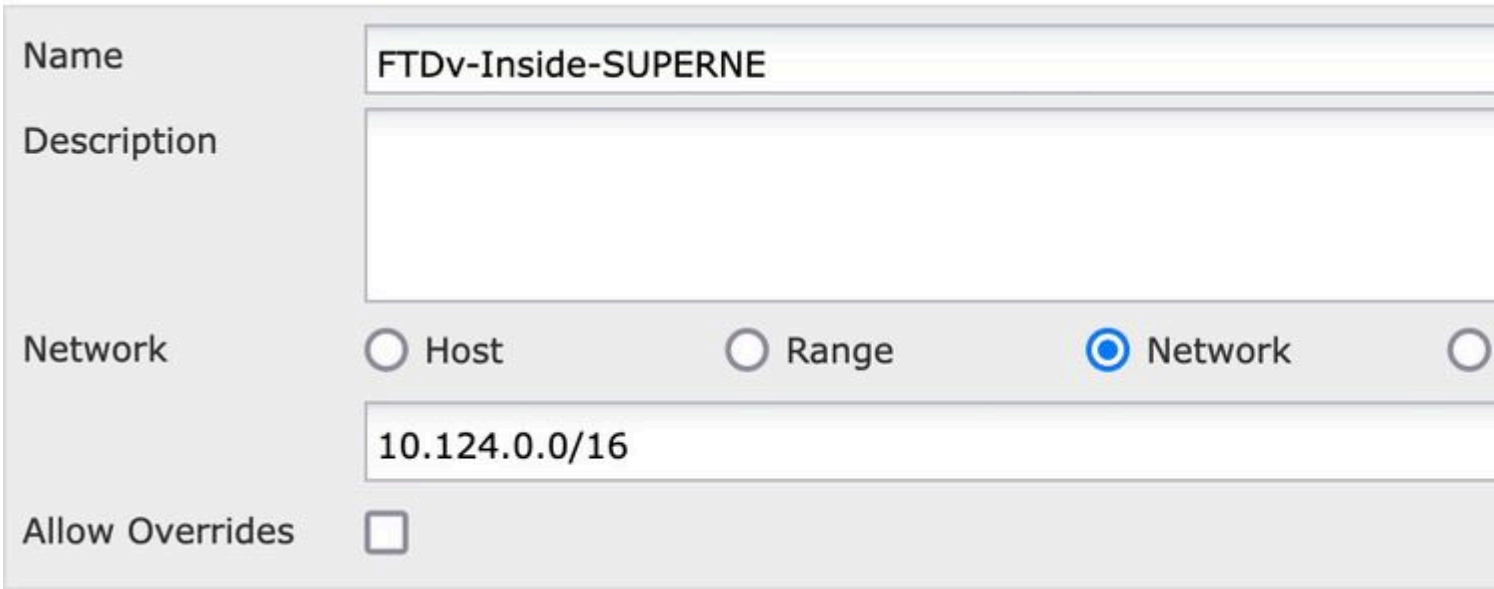


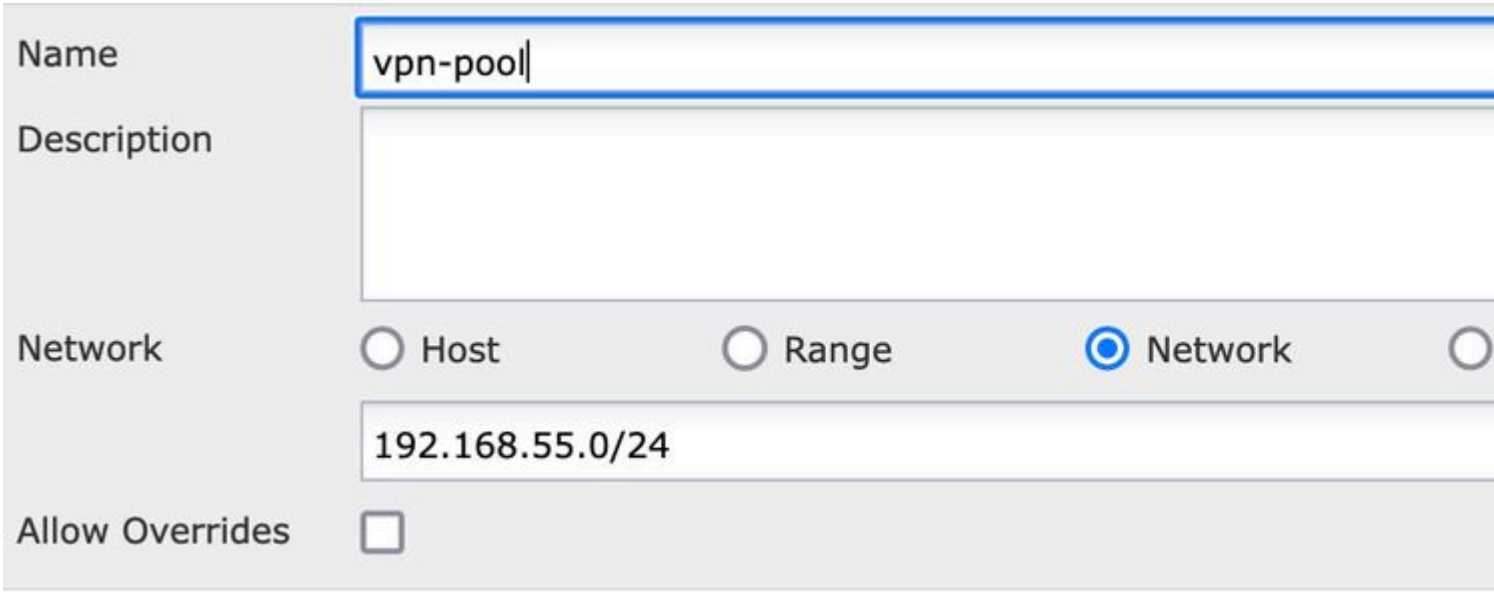
4. Stellen Sie sicher, dass Sie die Optionen umschalten (wie im Bild gezeigt), um "**no-proxy-arp**" und "**route-lookup**" in der NAT-Regel zu aktivieren, wählen Sie **OK,** wie im Bild gezeigt.



5. Dies ist das Ergebnis der NAT-Ausnahmekonfiguration.

Die im vorherigen Abschnitt verwendeten Objekte sind die unten beschriebenen.





Schritt 2: Haarnadelkonfiguration

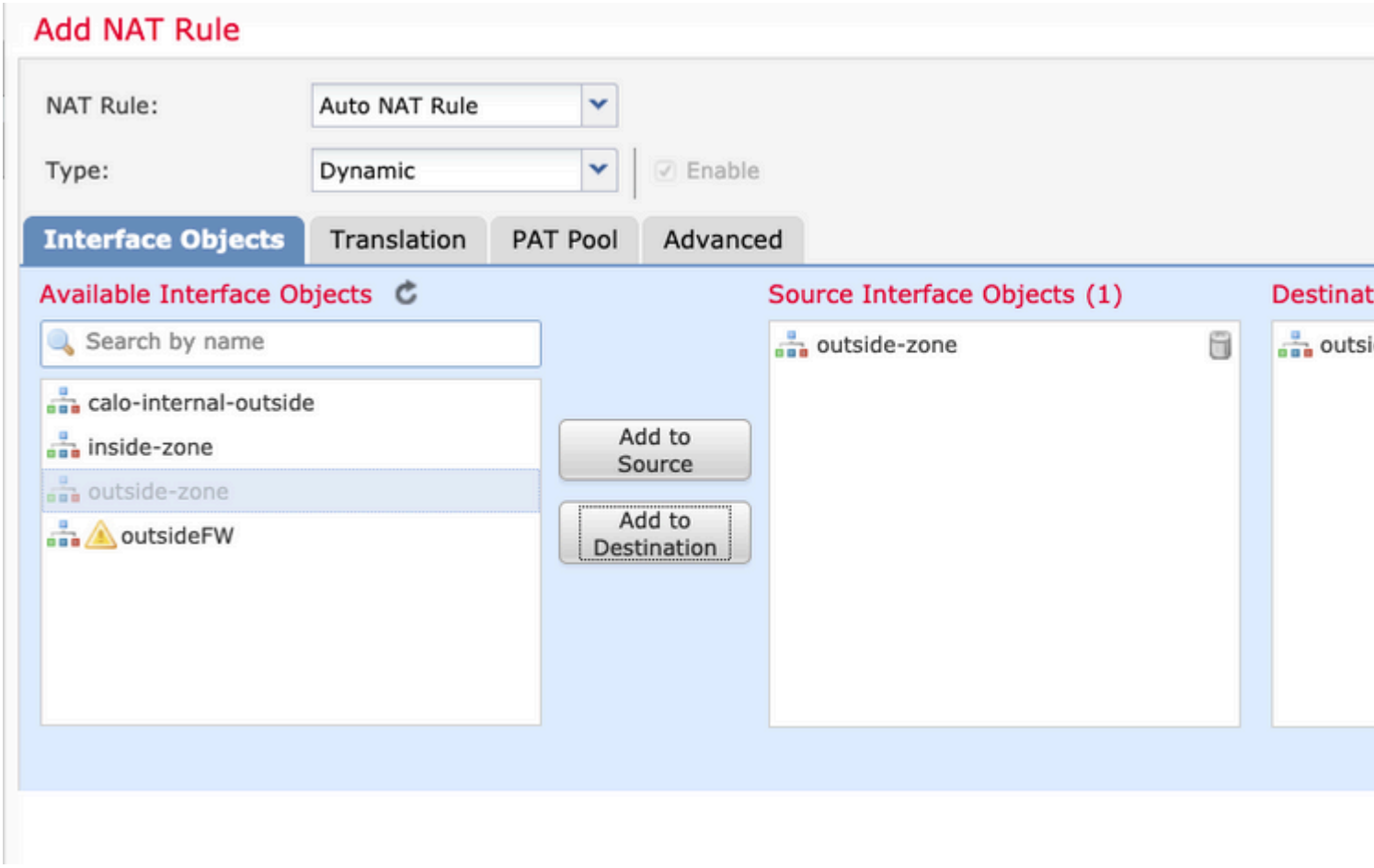
Dies wird auch als **Kehrtwende** bezeichnet und ist eine Übersetzungsmethode, die es dem Datenverkehr ermöglicht, über dieselbe Schnittstelle zu fließen, über die der Datenverkehr empfangen wird.

Wenn beispielsweise AnyConnect mit einer **vollständigen Tunnel-**Split-Tunnel-Richtlinie konfiguriert ist, erfolgt der Zugriff auf die internen Ressourcen gemäß der NAT-Freistellungsrichtlinie. Wenn der Anyconnect-Client-Datenverkehr eine externe Website im Internet erreichen soll, ist die Hairpin-NAT (oder Kehrtwende) dafür zuständig, den Datenverkehr von außen nach außen zu routen.

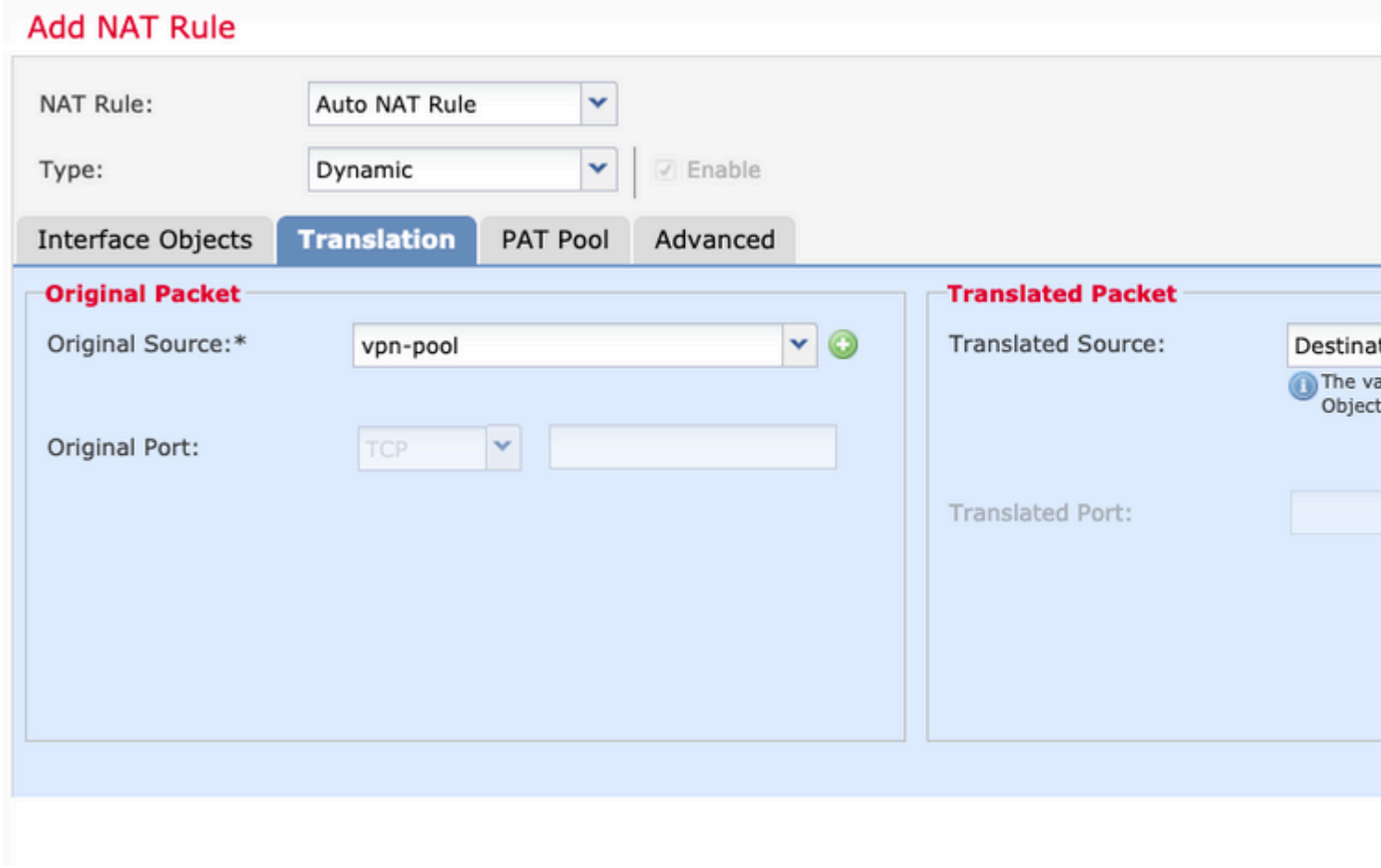
Vor der NAT-Konfiguration muss ein VPN-Poolobjekt erstellt werden.

1. Erstellen Sie eine neue NAT-Anweisung, wählen Sie im Feld **NAT Rule (NAT-Regel)** die Option **Auto NAT Rule (Automatische NAT-Regel)** und wählen Sie **Dynamic (Dynamisch)** als NAT-**Typ aus**.

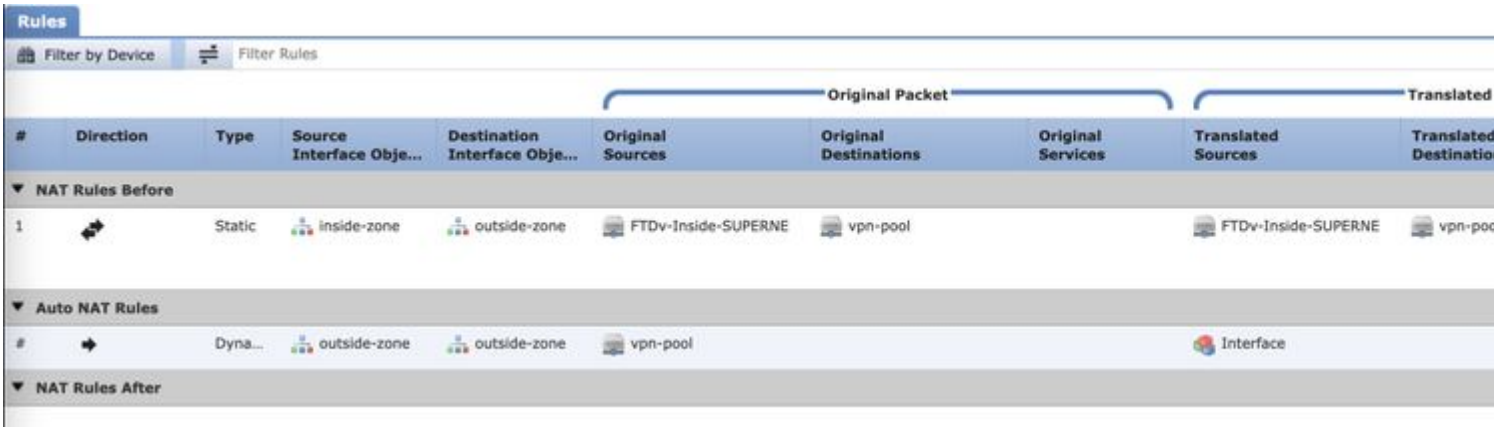
2. Wählen Sie die gleiche Schnittstelle für die **Quell-** und Zielschnittstellenobjekte (außen):



3. Wählen Sie auf der Registerkarte Übersetzung als **Originalquelle** das Objekt vpn-pool aus, und wählen Sie **Destination Interface IP** als **übersetzte Quelle aus**, und wählen Sie **OK,** wie im Bild gezeigt.



4. Dies ist die Zusammenfassung der NAT-Konfiguration im Bild.



5. Klicken Sie auf **Speichern** und **Bereitstellen, um** die Änderungen vorzunehmen.

Überprüfung

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

Führen Sie diese Befehle in der FTD-Befehlszeile aus.

- **sh crypto ca zertifikate**
- **show running-config ip local pool**
- **show running-config webvpn**
- **show running-config tunnel-group**

- **show running-config group-policy**
- **show running-config ssl**
- **show running-config nat**

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.</>

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.