Konfiguration von AnyConnect Remote Access VPN auf FTD

Inhalt

Einleitung

Dieses Dokument beschreibt eine Konfiguration für AnyConnect Remote Access VPN auf FTD.

Voraussetzungen

Anforderungen

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

- Grundlegendes VPN-, TLS- und IKEv2-Wissen
- AAA- (Basic Authentication, Authorization, and Accounting) und RADIUS-Kenntnisse
- Erfahrung mit FirePOWER Management Center

Verwendete Komponenten

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

- Cisco FTD 7.2.0

- Cisco FMC 7.2.1
- AnyConnect 4.10

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 verstehen.

Hintergrundinformationen

Dieses Dokument enthält ein Konfigurationsbeispiel für Firepower Threat Defense (FTD), Version 7.2.0 und höher, das es dem Remote-Access-VPN ermöglicht, Transport Layer Security (TLS) und Internet Key Exchange Version 2 (IKEv2) zu verwenden. Als Client kann Cisco AnyConnect verwendet werden, das auf mehreren Plattformen unterstützt wird.

Konfiguration

1. Voraussetzungen

So wechseln Sie durch den Remote Access-Assistenten im FirePOWER Management Center:

- Erstellen Sie ein Zertifikat, das für die Serverauthentifizierung verwendet wird.
- Konfigurieren Sie den RADIUS- oder LDAP-Server für die Benutzerauthentifizierung.
- Erstellen Sie einen Adresspool für VPN-Benutzer.
- Laden Sie AnyConnect-Images für verschiedene Plattformen hoch.

a) SSL-Zertifikat importieren

Zertifikate sind für die Konfiguration von AnyConnect unerlässlich. Um Fehler in Webbrowsern zu vermeiden, muss das Zertifikat über eine Erweiterung für den alternativen Antragstellernamen mit dem DNS-Namen und/oder der IP-Adresse verfügen.

> **Hinweis**: Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Fehlerinformationen.

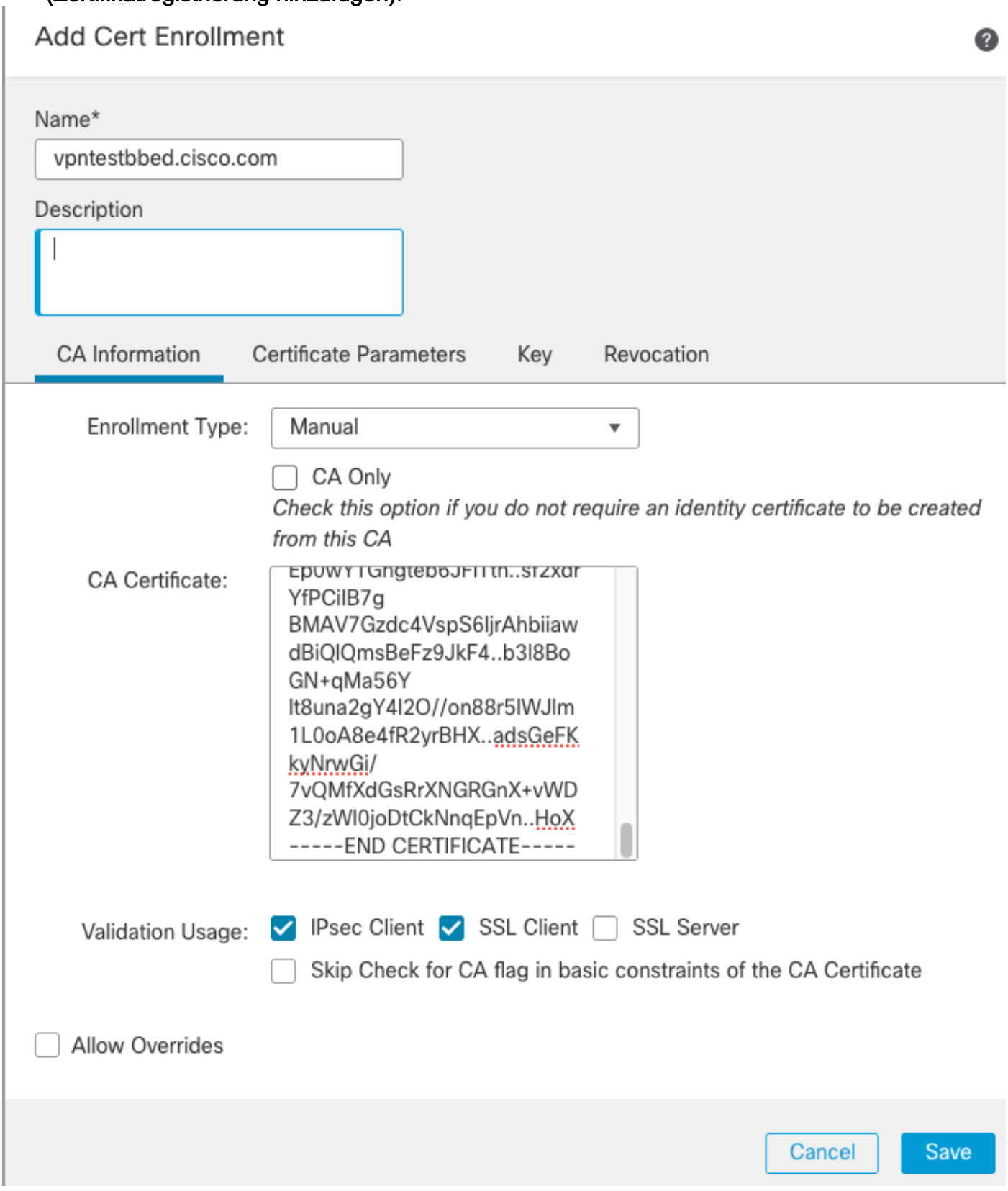
Die manuelle Zertifikatregistrierung unterliegt folgenden Einschränkungen:

- Auf FTD benötigen Sie das Zertifizierungsstellenzertifikat, bevor Sie die CSR-Anfrage erstellen.

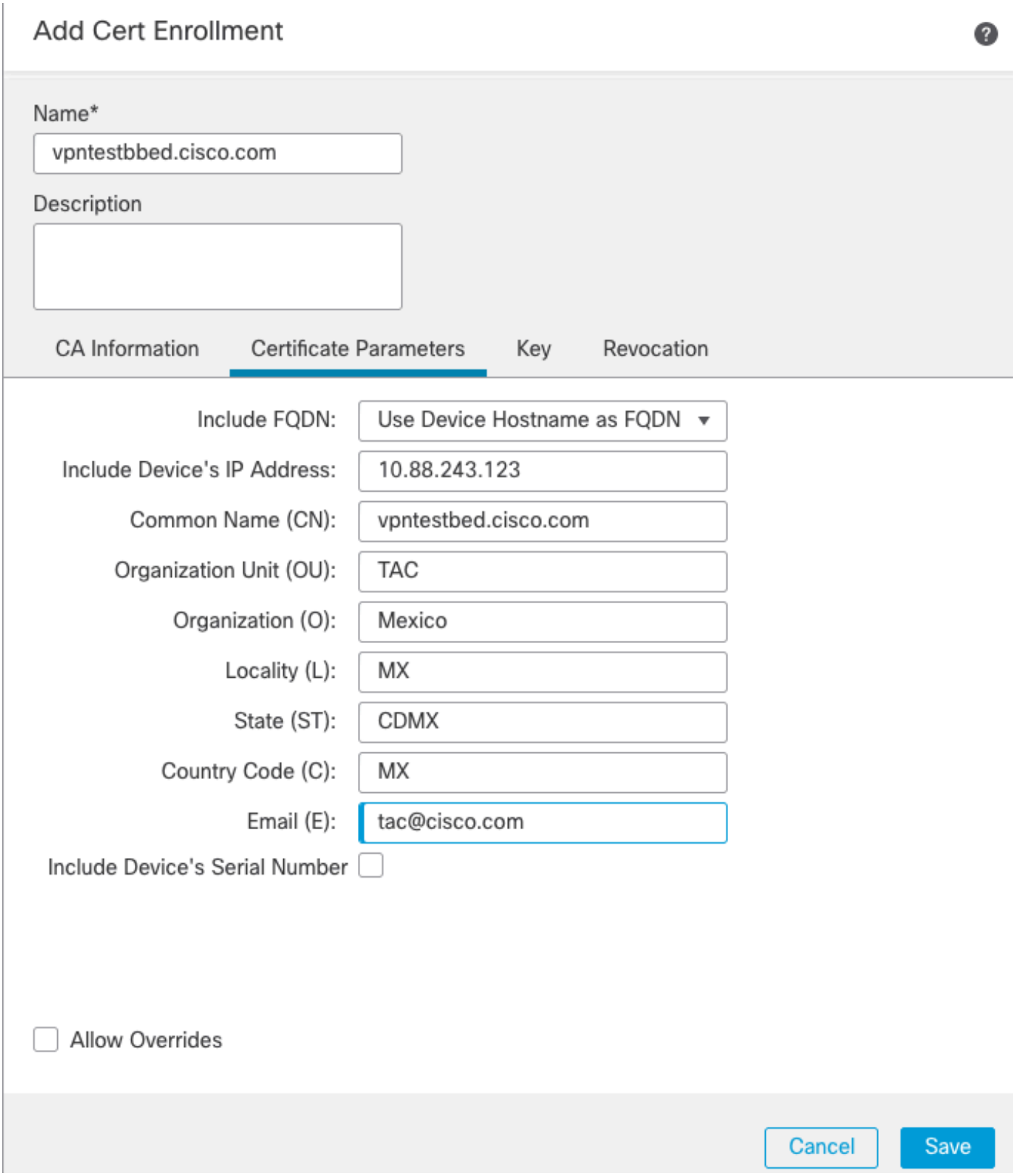
- Wenn der CSR extern generiert wird, schlägt die manuelle Methode fehl, es muss eine andere Methode verwendet werden (PKCS12).

Es gibt verschiedene Methoden, um ein Zertifikat auf der FTD-Appliance zu erhalten. Die sichere und einfache Methode besteht jedoch darin, eine Zertifikatsanforderung (Certificate Signing Request, CSR) zu erstellen, sie mit einer Zertifizierungsstelle (Certificate Authority, CA) zu signieren und dann ein Zertifikat zu importieren, das für einen öffentlichen Schlüssel ausgestellt wurde, der in der CSR enthalten war. So gehen Sie vor:

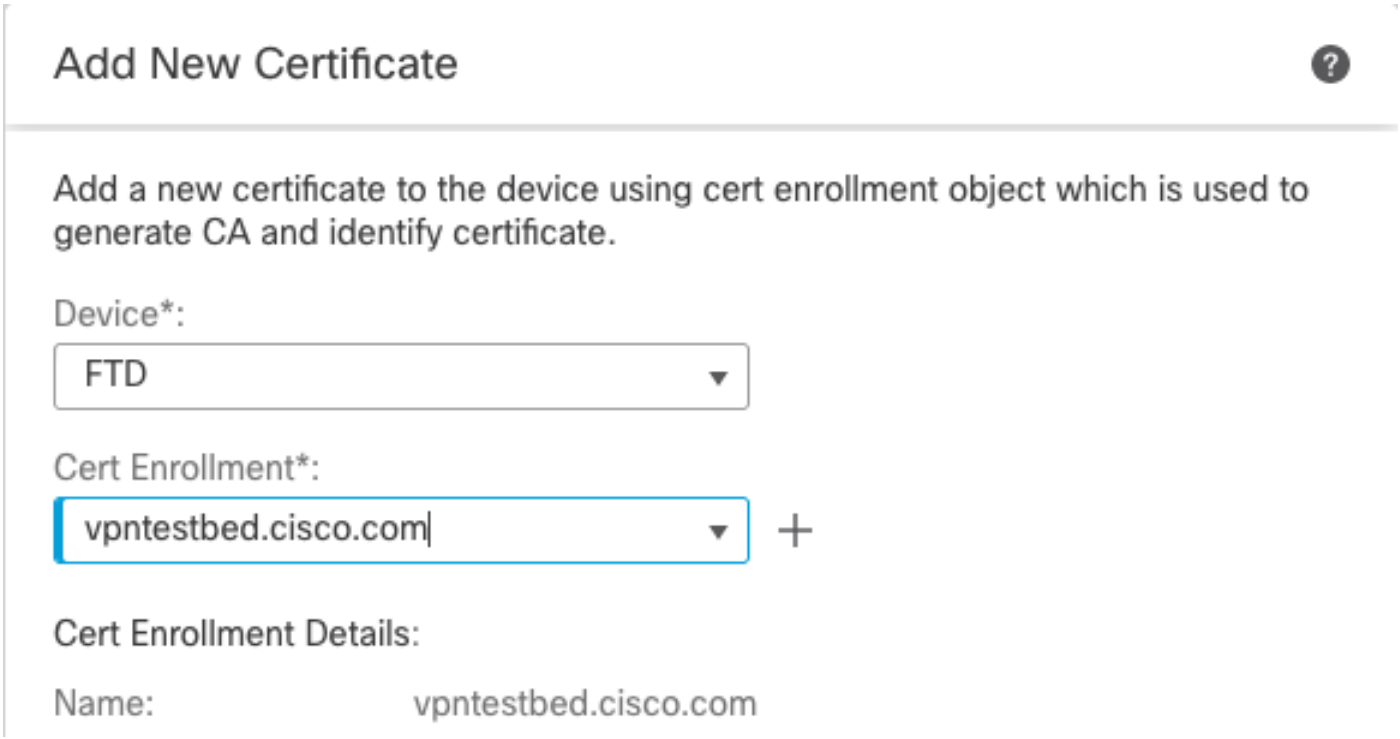
- Gehe zu Objects > **Object Management > PKI > Cert Enrollment** klicken Sie auf **Add Certificate Enrollment (Zertifikatregistrierung hinzufügen)**.



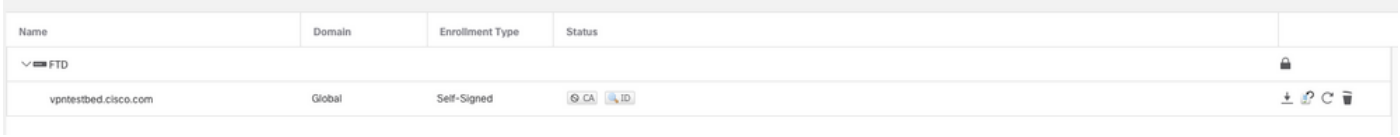
- Auswählen Enrollment Type und fügen Sie ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) ein (das Zertifikat, das zum Signieren des CSR verwendet wird).
- Wechseln Sie dann zur zweiten Registerkarte, und wählen Sie Custom FQDN und füllen Sie alle erforderlichen Felder aus, z. B.:



- Wählen Sie auf der dritten Registerkarte Key Type, wählen Sie Name und Größe. Für RSA sind mindestens 2048 Bit erforderlich.
- Klicken Sie auf Speichern und gehen Sie zu Devices > Certificates > Add > New Certificate.
- Wählen Sie Deviceund unter Cert Enrollment den soeben erstellten Vertrauenspunkt auswählen, klicken Sie auf Add:

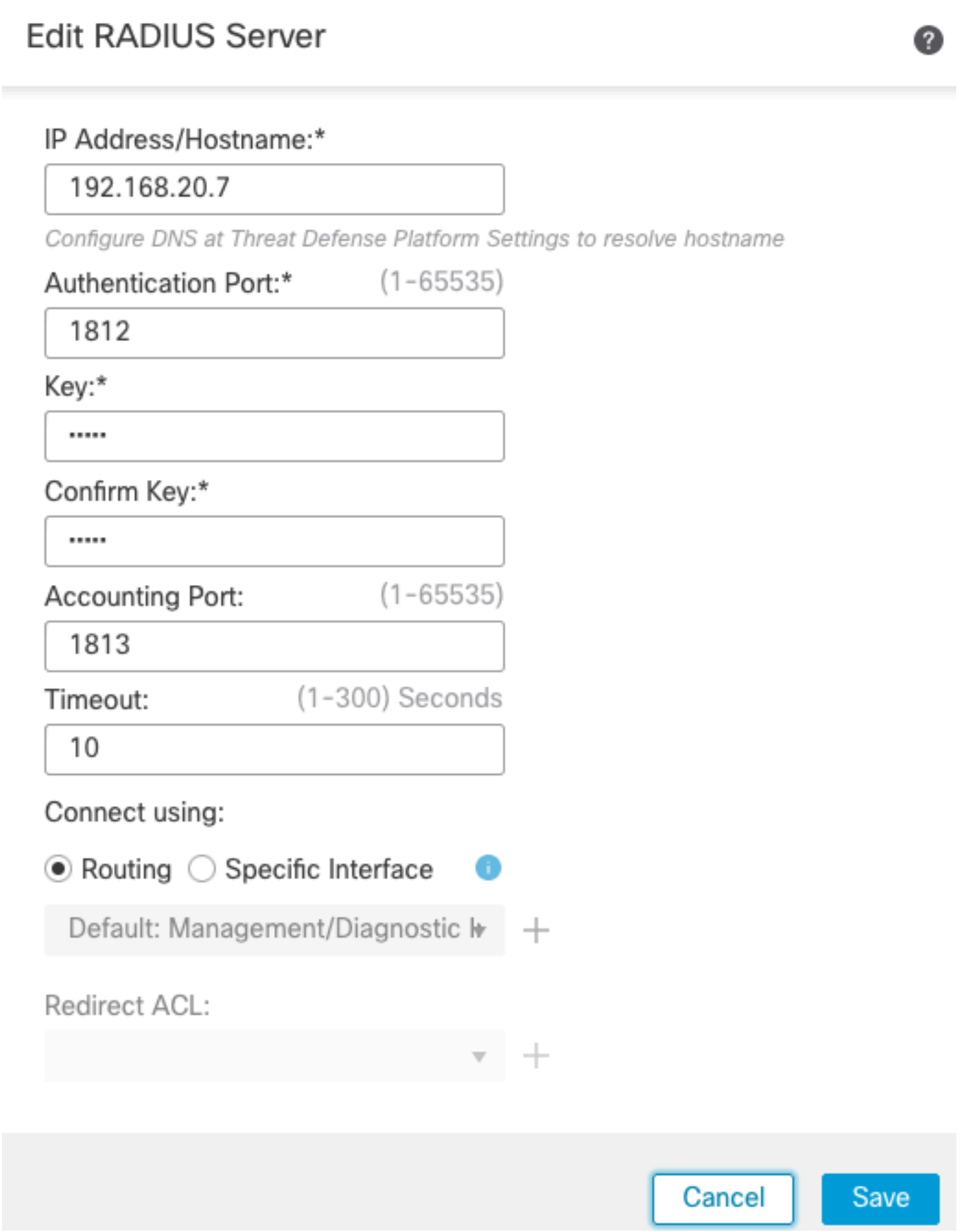


- Klicken Sie später neben dem Namen des Vertrauenspunkts auf Symbol, dann Yesund anschließend CSR auf CA kopieren und signieren. Das Zertifikat muss über dieselben Attribute wie ein normaler HTTPS-Server verfügen.
- Nachdem Sie das Zertifikat von CA im Base64-Format erhalten haben, wählen Sie es auf der Festplatte aus, und klicken Sie auf Import. Wenn dies erfolgreich ist, sehen Sie Folgendes:

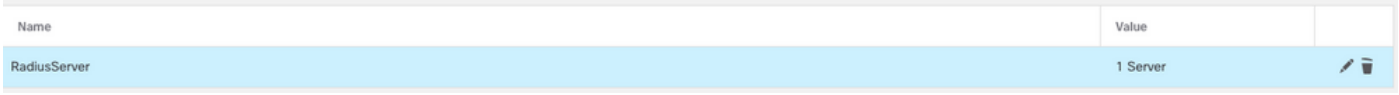


b) Konfigurieren des RADIUS-Servers

- Gehe zu **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Grou**p.
- Geben Sie den Namen ein, und fügen Sie die IP-Adresse zusammen mit dem geheimen Schlüssel hinzu. Klicken Sie auf Save:

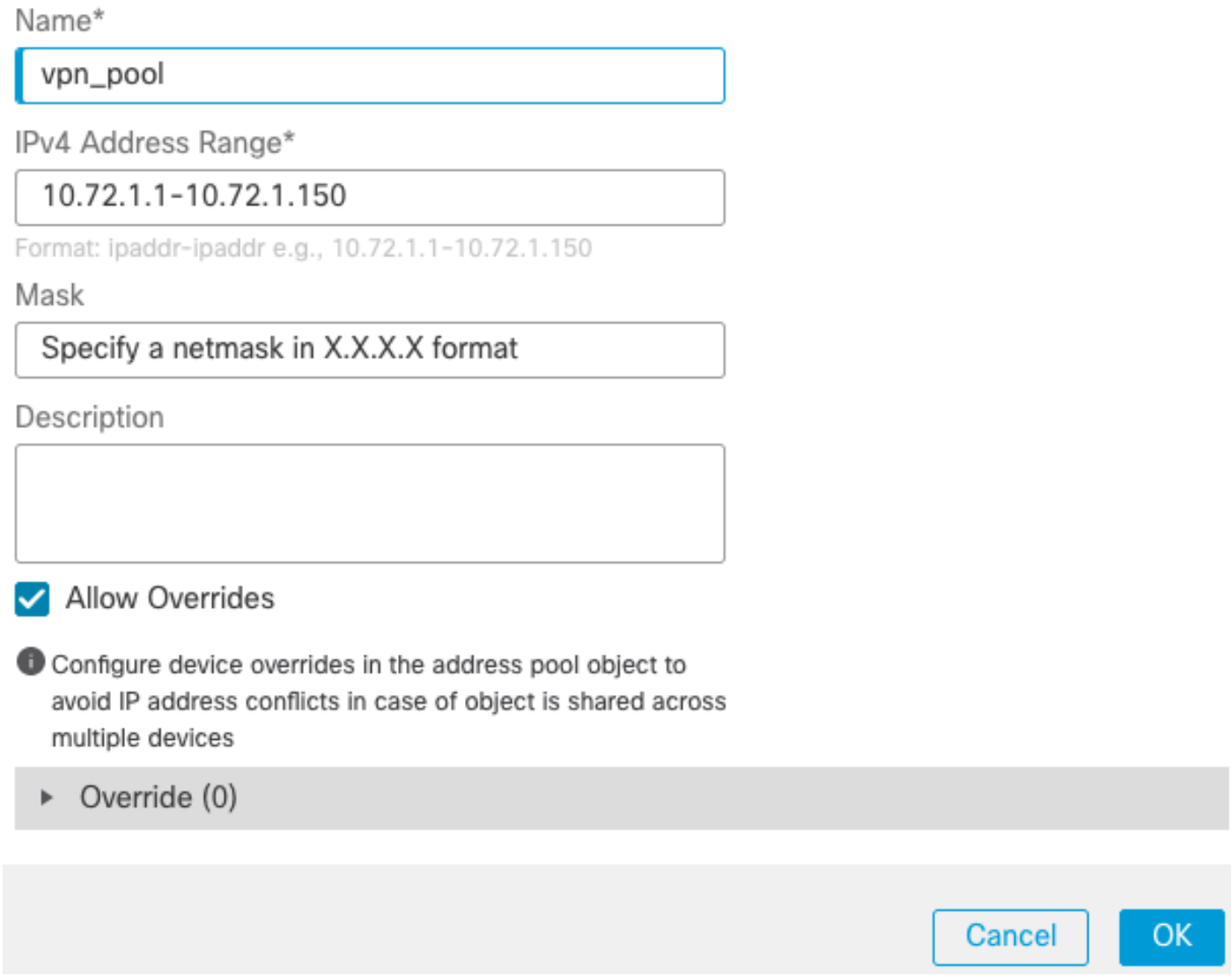


- Danach sehen Sie den Server auf der Liste:



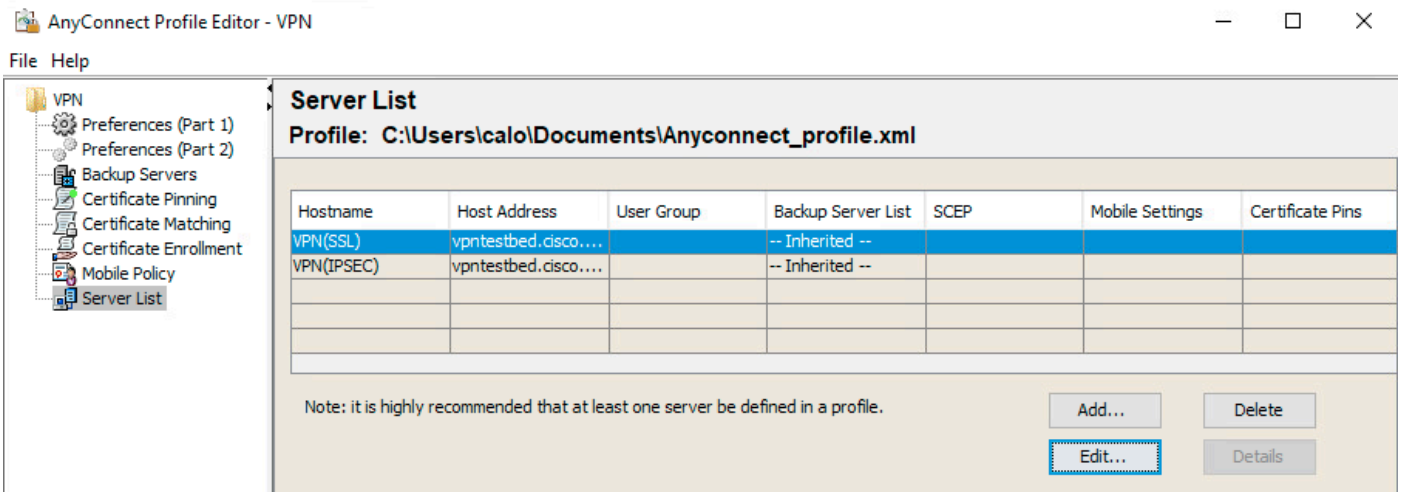
c) Erstellen eines Adresspools für VPN-Benutzer

- Gehe zu **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Legen Sie den Namen und den Bereich, Maske ist nicht erforderlich:



d) XML-Profil erstellen

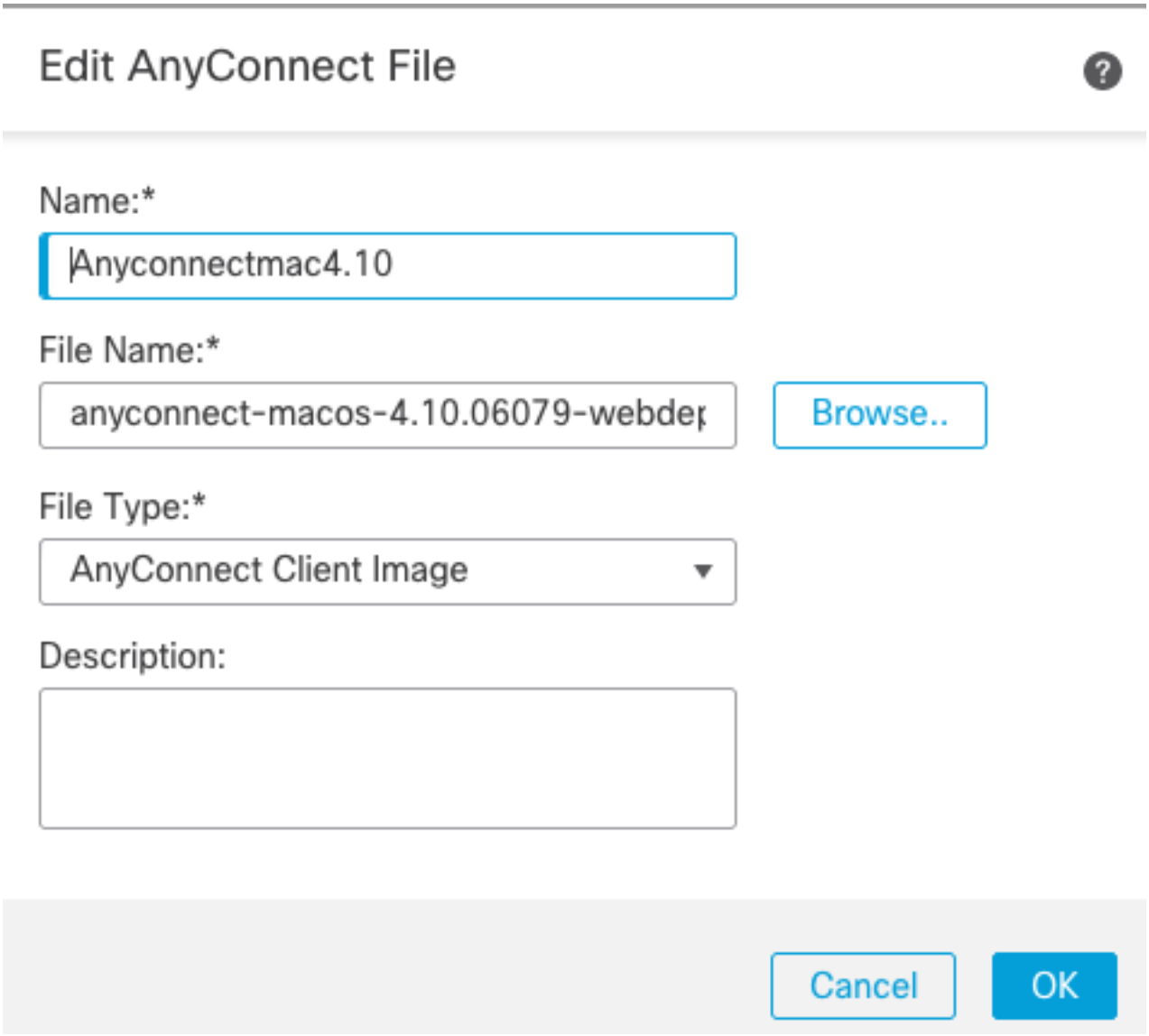
- Laden Sie den Profil-Editor von der Cisco Website herunter, und öffnen Sie ihn.
- Gehe zu Server List > Add...
- Geben Sie den Anzeigenamen und den FQDN ein. Einträge werden in der Serverliste angezeigt:



- Klicken Sie auf OKund **File** > **Save as...**

e) AnyConnect-Images hochladen

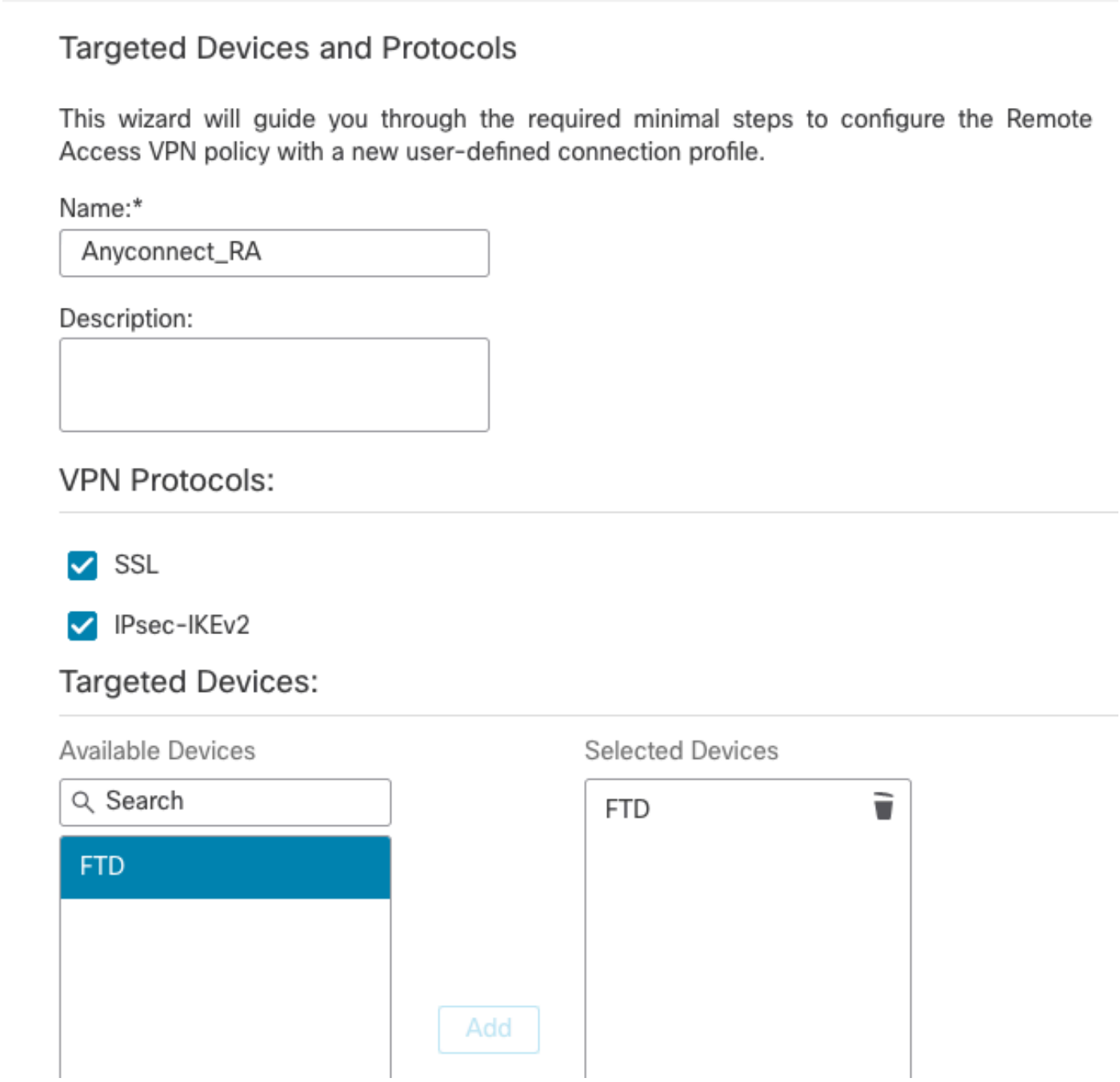
- Laden Sie Paketbilder von der Cisco Website herunter.
- Gehe zu Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- Geben Sie den Namen ein, und wählen Sie die PKG-Datei auf der Festplatte aus. Klicken Sie auf Save:



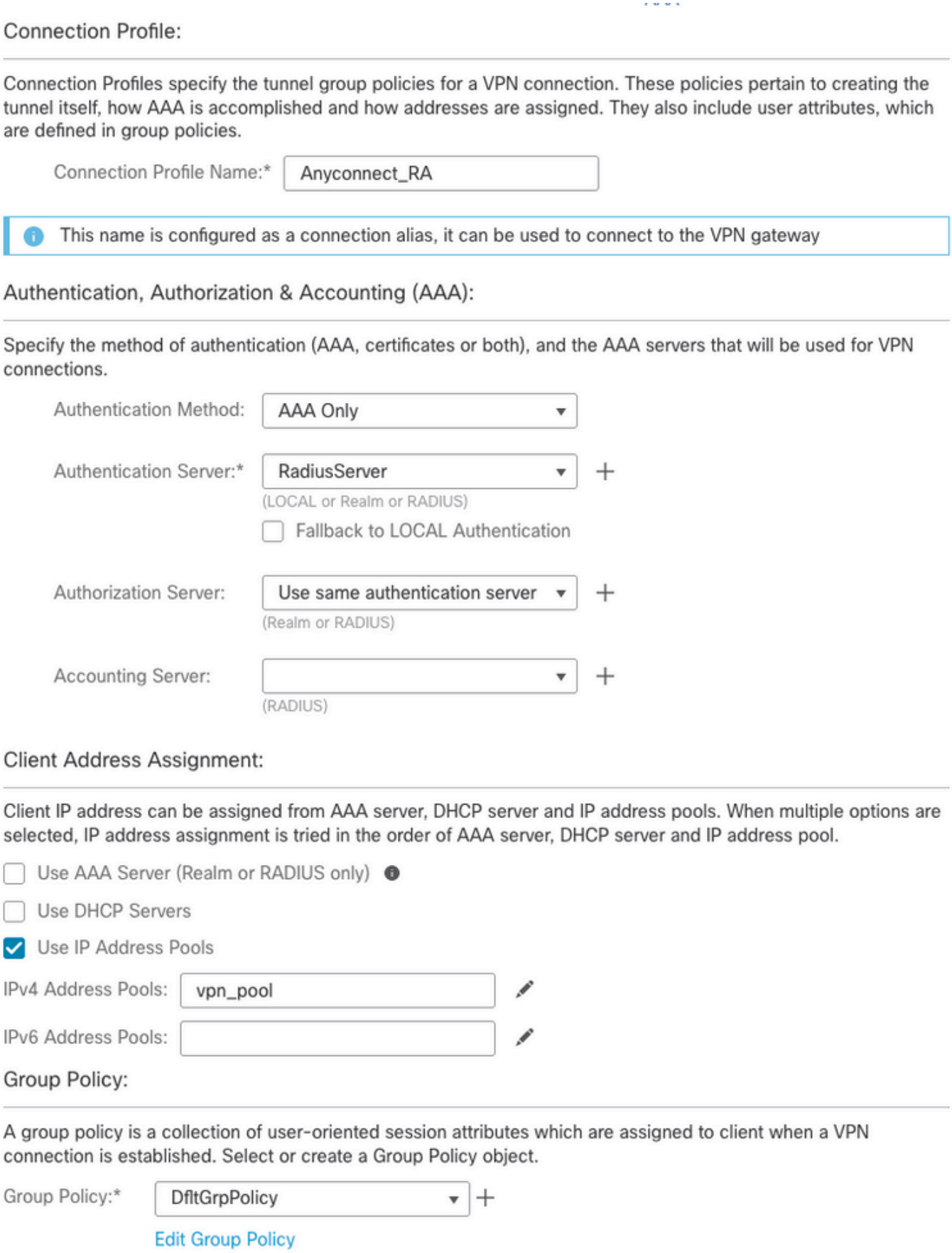
- Fügen Sie weitere Pakete entsprechend Ihrer Anforderungen hinzu.

2. Assistent für den Remotezugriff

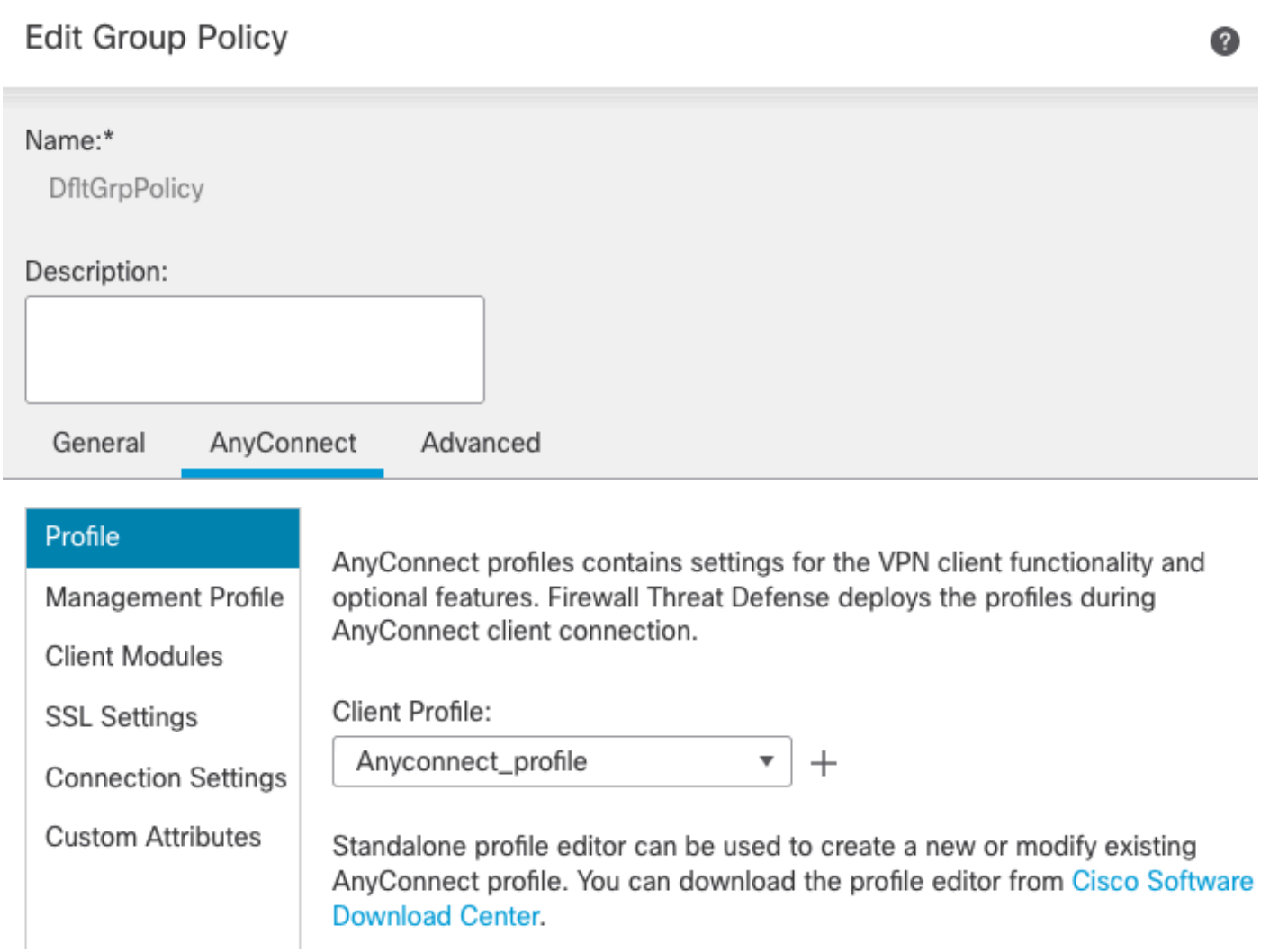
- Gehe zu Devices > VPN > Remote Access > Add a new configuration.
- Nennen Sie das Profil, und wählen Sie ein FTD-Gerät:



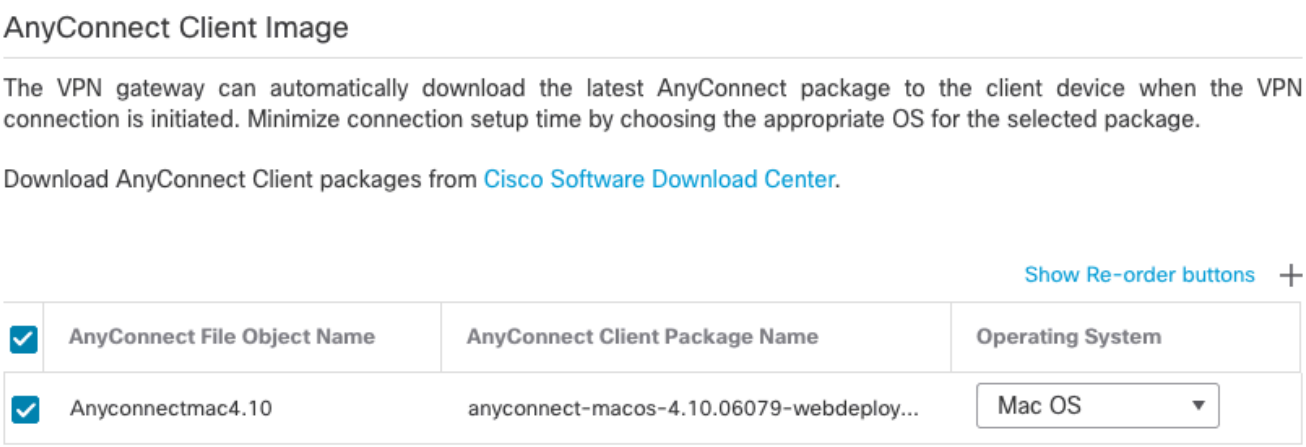
- Geben Sie im Schritt Verbindungsprofil Folgendes ein: **Connection Profile Name**, wählen Sie **Authentication Server** und Address Pools die Sie zuvor erstellt haben:



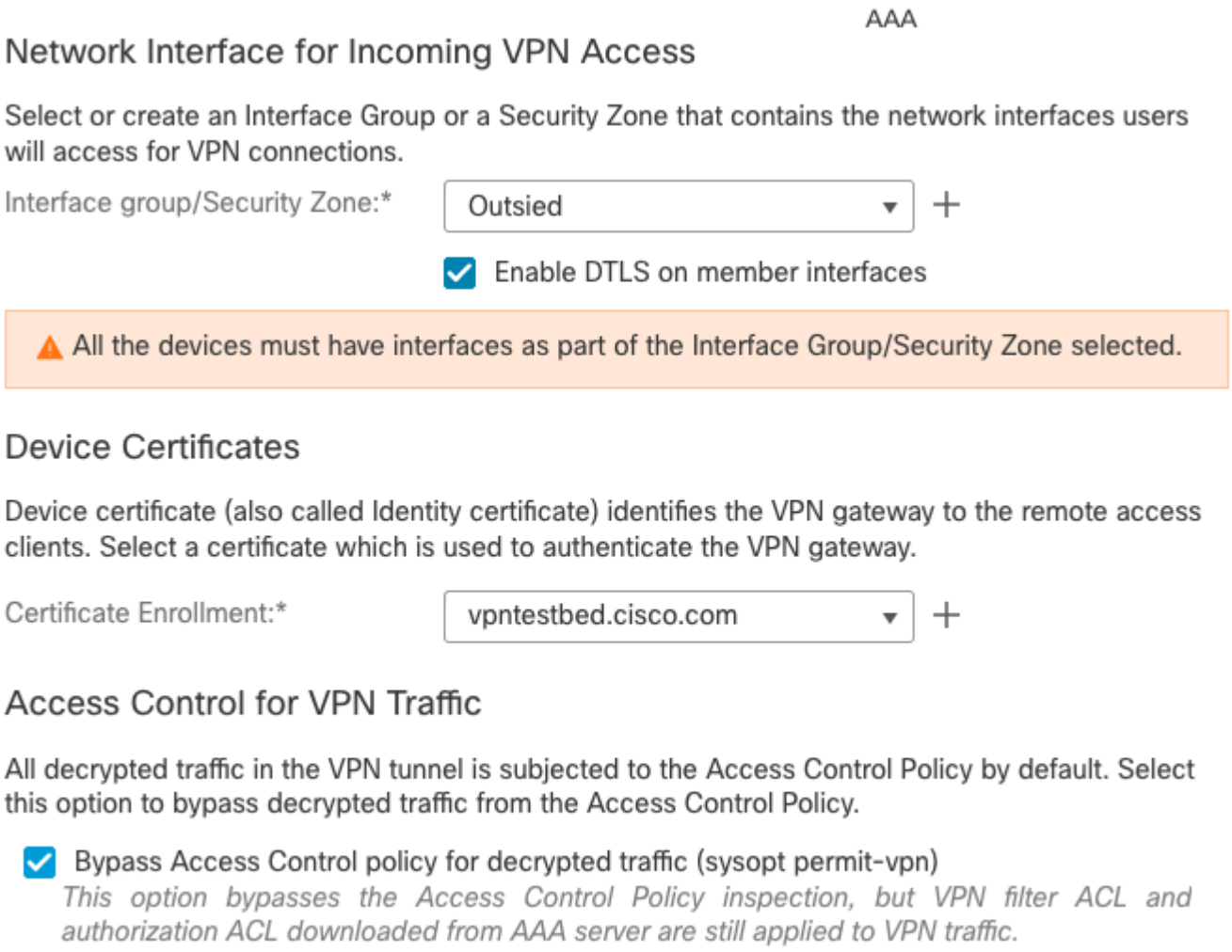
- Klicken Sie **Edit Group Policy** und wählen Sie auf der Registerkarte AnyConnect Client Profile, und klicken Sie dann auf Save:



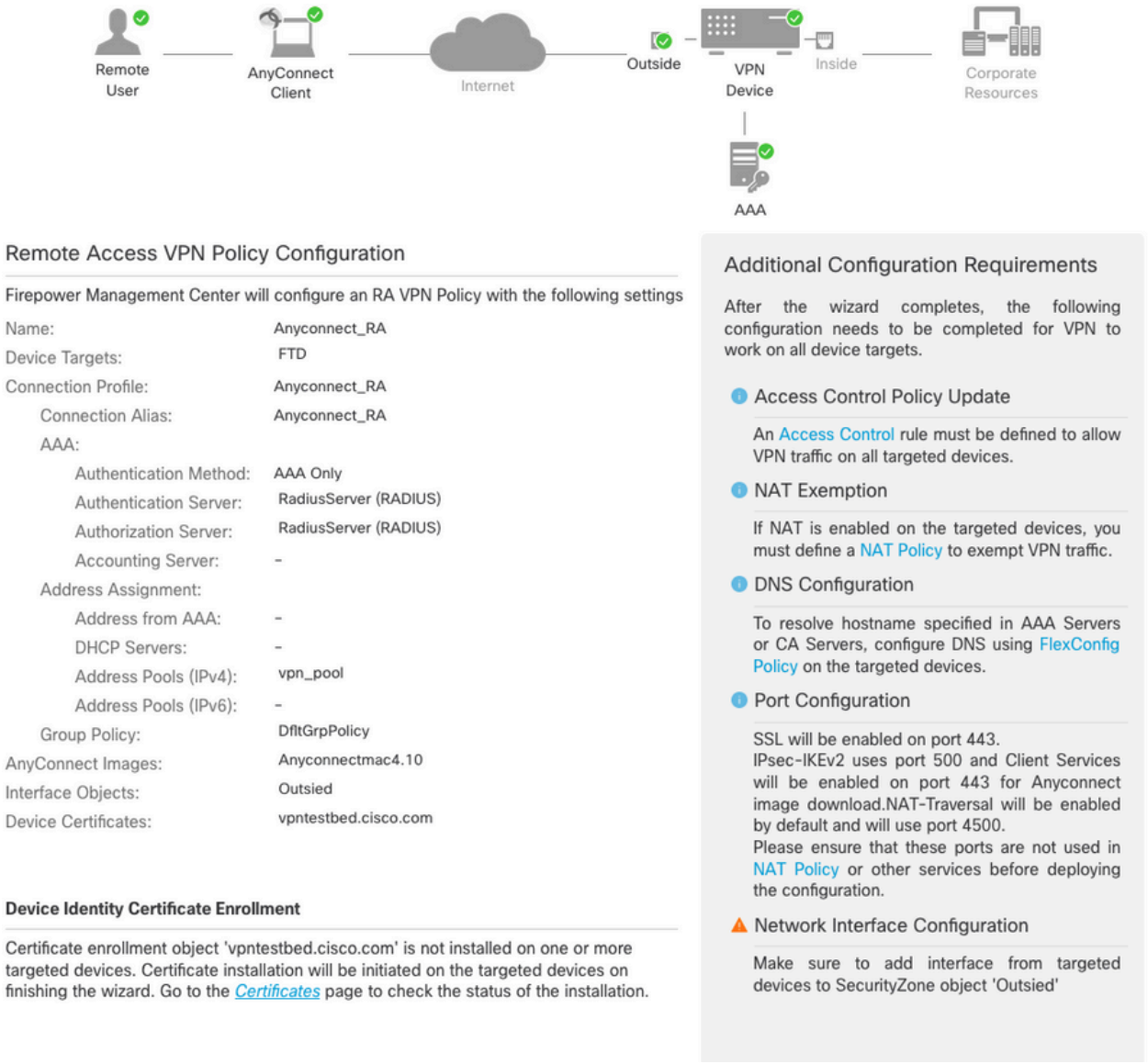
- Wählen Sie auf der nächsten Seite AnyConnect-Bilder aus, und klicken Sie auf Next.



- Wählen Sie auf dem nächsten Bildschirm **Network Interface and Device Certificates**:



- Wenn alles richtig konfiguriert ist, können Sie auf Finish und dann Deploy:



- Dadurch wird die gesamte Konfiguration zusammen mit Zertifikaten und AnyConnect-Paketen in die FTD-Appliance kopiert.

Verbindung

Um eine Verbindung zu FTD herzustellen, müssen Sie einen Browser öffnen, indem Sie den DNS-Namen oder die IP-Adresse eingeben, die auf die externe Schnittstelle verweist. Anschließend melden Sie sich mit den Anmeldeinformationen an, die im RADIUS-Server gespeichert sind, und führen die Anweisungen auf dem Bildschirm aus. Nach der Installation von AnyConnect müssen Sie dieselbe Adresse in das AnyConnect-Fenster eingeben und auf Connect.

Einschränkungen

Derzeit nicht unterstützt auf FTD, aber verfügbar auf ASA:

- Die Schnittstellenauswahl auf dem RADIUS-Server wird von Firepower Threat Defense6.2.3 oder früheren Versionen nicht unterstützt. Die Schnittstellenoption wird bei der Bereitstellung ignoriert.
- Ein RADIUS-Server mit aktivierter dynamischer Autorisierung erfordert Firepower Threat

Defense6.3 oder höher, damit die dynamische Autorisierung funktioniert.
- FTDposture VPN unterstützt keine Gruppenrichtlinienänderungen durch dynamische Autorisierung oder RADIUS-Autorisierungsänderung (CoA).
- AnyConnect-Anpassung (Erweiterung: Cisco Bug-ID CSCvq87631)
- AnyConnect-Skripte
- AnyConnect-Lokalisierung
- WSA-Integration
- Gleichzeitige dynamische IKEv2-Kryptografiezuordnung für RA und L2L VPN (Erweiterung: Cisco Bug-ID CSCvr52047)
- AnyConnect-Module (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security usw.) - DART ist standardmäßig installiert (Verbesserungen für AMP Enabler und Umbrella: Cisco Bug-ID CSCvs03562 und Cisco Bug-ID CSCvs06642).
- TACACS, Kerberos (KCD-Authentifizierung und RSA SDI)
- Browser-Proxy

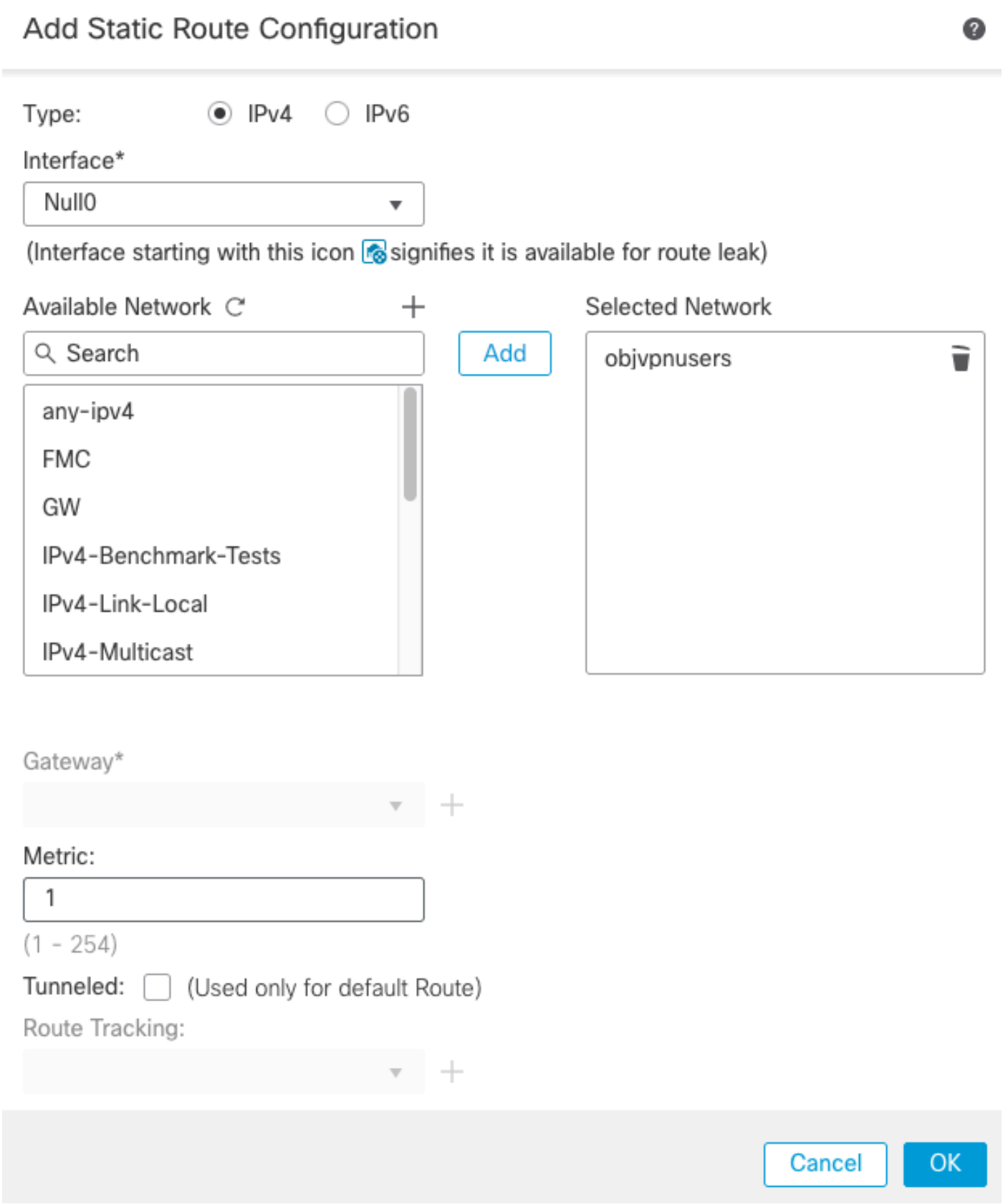
Sicherheitsüberlegungen

Standardmäßig wird das sysopt connection permit-vpnist deaktiviert. Das bedeutet, dass Sie den Datenverkehr, der aus dem Adresspool an einer externen Schnittstelle stammt, über die Zugriffskontrollrichtlinie zulassen müssen. Obwohl die Vorfilter- oder Zugriffskontrollregel hinzugefügt wird, um nur VPN-Datenverkehr zuzulassen, wird dieser irrtümlicherweise zugelassen, wenn der Klartextdatenverkehr den Regelkriterien entspricht.

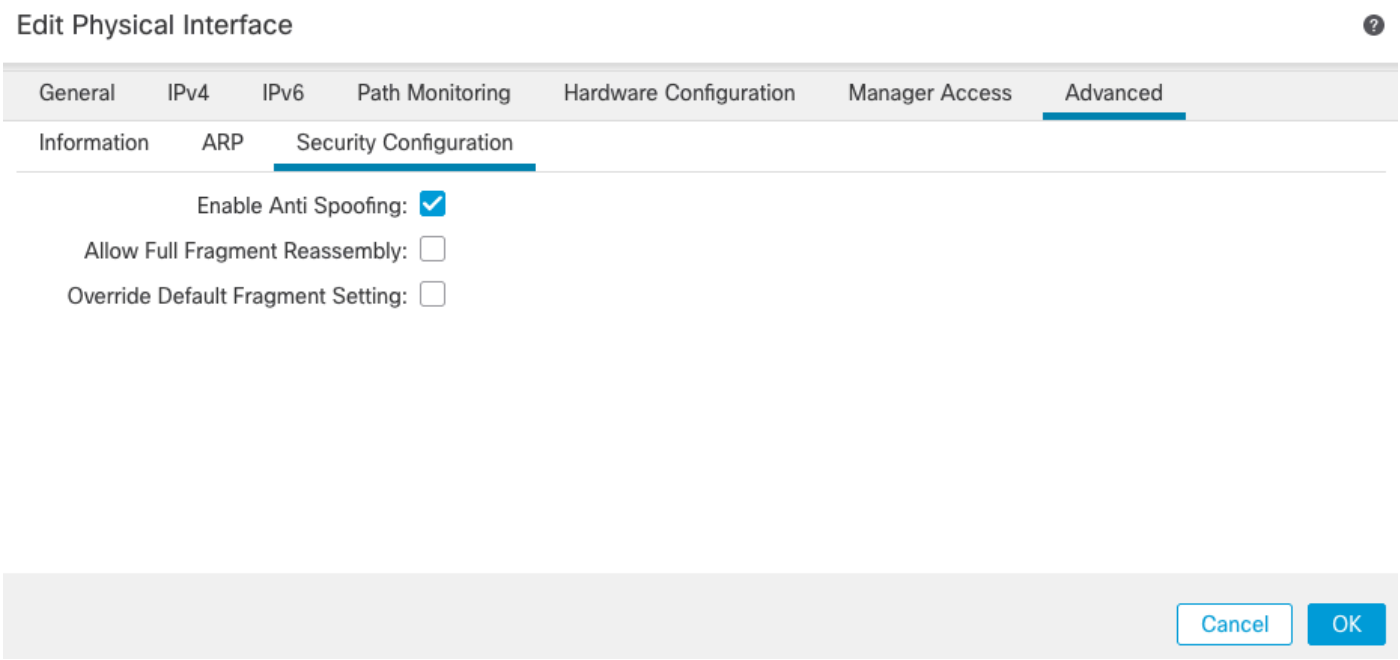
Für dieses Problem gibt es zwei Ansätze. Die empfohlene Option für das TAC besteht zum einen darin, Anti-Spoofing (auf ASA wurde es als Unicast Reverse Path Forwarding - uRPF bezeichnet) für eine externe Schnittstelle zu aktivieren, und zum anderen darin, sysopt connection permit-vpn um Snort Inspection vollständig zu umgehen. Die erste Option ermöglicht eine normale Überprüfung des Datenverkehrs von und zu VPN-Benutzern.

a) uRPF aktivieren

- Erstellen Sie eine Null-Route für das Netzwerk, das für RAS-Benutzer verwendet wird, wie in Abschnitt C definiert. Gehen Sie zu Devices > Device Management > Edit > Routing > Static Route und wählen Add route



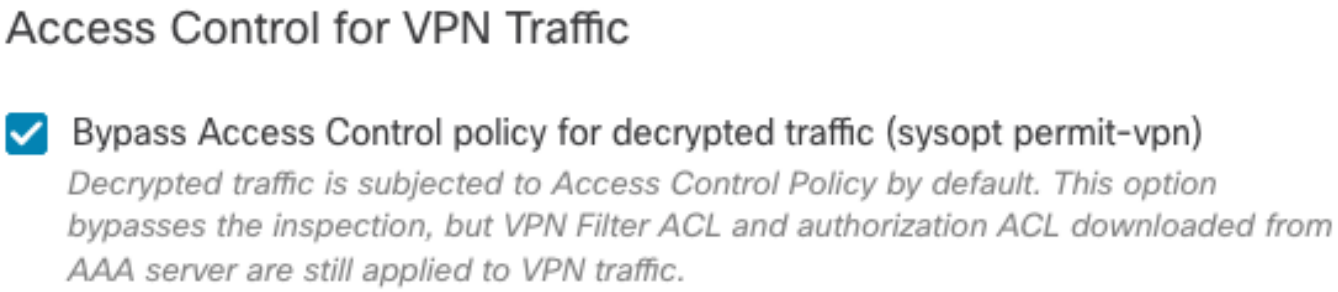
- Aktivieren Sie anschließend uRPF an der Schnittstelle, an der die VPN-Verbindungen enden. Navigieren Sie zu **Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing**.



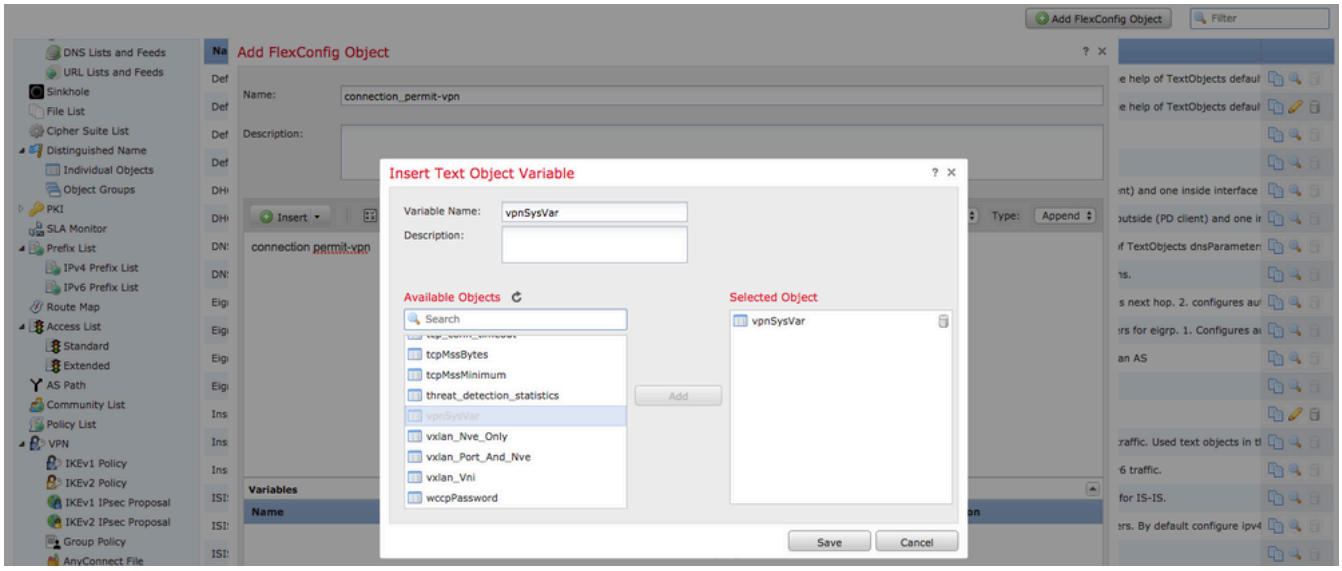
Wenn ein Benutzer verbunden ist, wird die 32-Bit-Route für diesen Benutzer in der Routing-Tabelle installiert. Löschen Sie den Textverkehr, der von den anderen, nicht verwendeten IP-Adressen aus dem Pool stammt, und wird vom RFP fallen gelassen. Um eine Beschreibung von **Anti-Spoofing**Weitere Informationen finden Sie unter [Sicherheitskonfigurationsparameter für Firepower Threat Defense festlegen.]

b) Aktivieren Sysopt connection permit-vpn Option

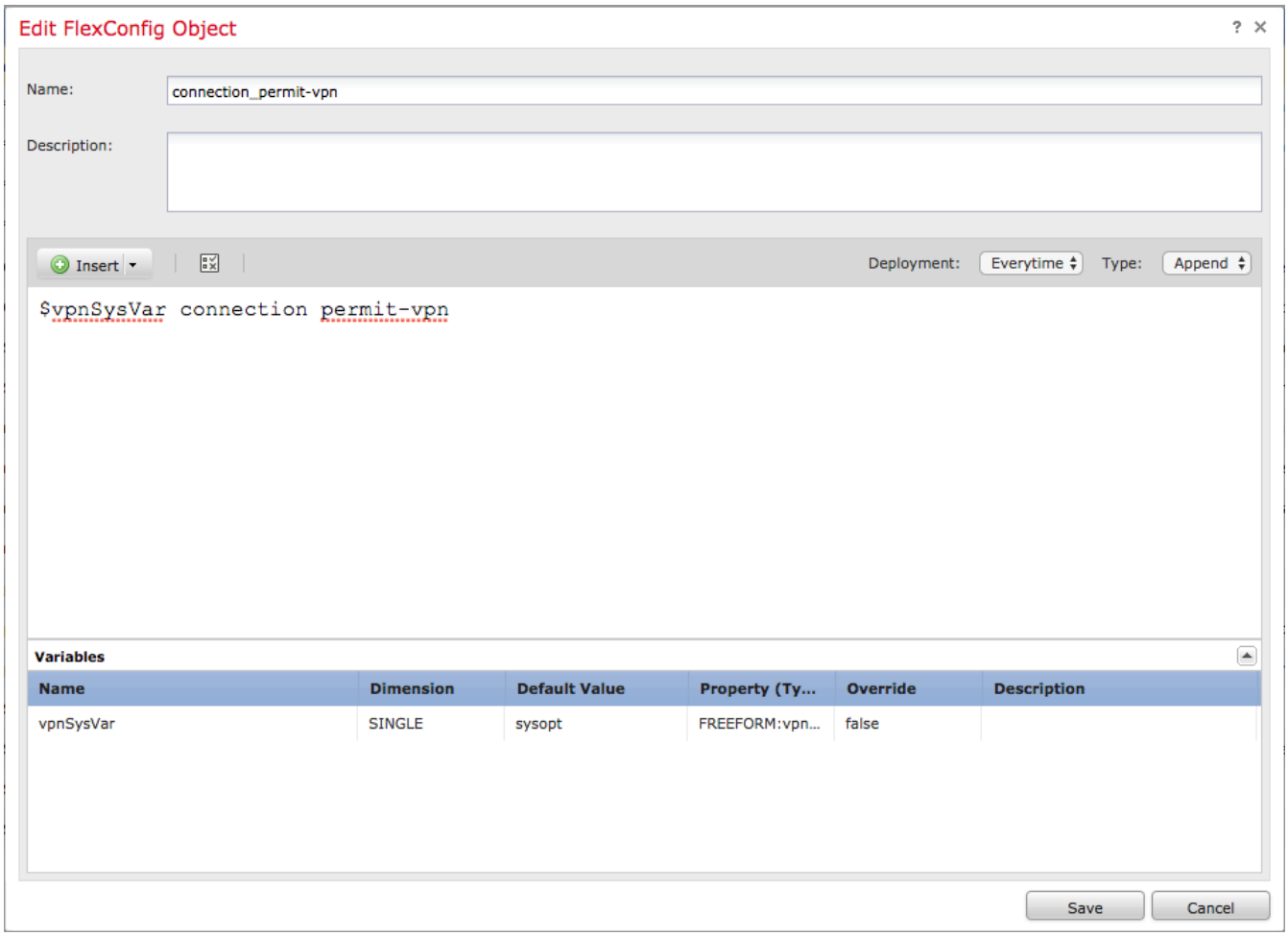
- Wenn Sie Version 6.2.3 oder höher haben, gibt es eine Option, dies mit dem Assistenten oder unter Devices > VPN > Remote Access > VPN Profile > Access Interfaces**.**



- Versionen vor 6.2.3 finden Sie unter Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- Erstellen Sie eine Textobjektvariable, z. B.: vpnSysVar ein einzelner Eintrag mit Wert sysopt.
- Gehe zu Objects**> Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.**
- Erstellen Sie FlexConfig Objekt mit CLI connection permit-vpn.
- Fügen Sie die Textobjektvariable in das Feld FlexConfig Objekt in der Kommandozeile mit **$vpnSysVar connection permit-vpn**. Klicken Sie auf Save:



- Anwenden des FlexConfigObjekt als **Append** und die Bereitstellung auswählen, Everytime:



- Gehe zu**Devices > FlexConfig** und die aktuelle Richtlinie bearbeiten oder eine neue mit New Policy -Taste.
- Nur erstellte hinzufügen FlexConfig,Klicken Sie auf Save.
- Bereitstellung der Konfiguration für die Bereitstellung**sysopt connection permit-vpn**-Befehls auf dem Gerät.

Danach können Sie jedoch nicht mehr die Zugriffskontrollrichtlinie verwenden, um den Datenverkehr der Benutzer zu überprüfen. Sie können weiterhin VPN-Filter oder herunterladbare ACL verwenden, um den Benutzerdatenverkehr zu filtern.

Wenn Sie Paketverluste mit Snort von den VPN-Benutzern sehen, wenden Sie sich an das TAC und verweisen Sie auf die Cisco Bug-ID CSCvg91399.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

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.