

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

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Importieren eines SSL-Zertifikats](#)

[Schritt 2: Konfigurieren eines RADIUS-Servers](#)

[Schritt 3: IP-Pool erstellen](#)

[Schritt 4: XML-Profil erstellen](#)

[Schritt 5: Anyconnect XML-Profil hochladen](#)

[Schritt 6: AnyConnect-Images hochladen](#)

[Schritt 7: Remotezugriff-VPN-Assistent](#)

[NAT-Befreiung und Haarnadel](#)

[Schritt 1: NAT-Freistellungskonfiguration](#)

[Schritt 2: Haarnadelkonfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

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](#)).

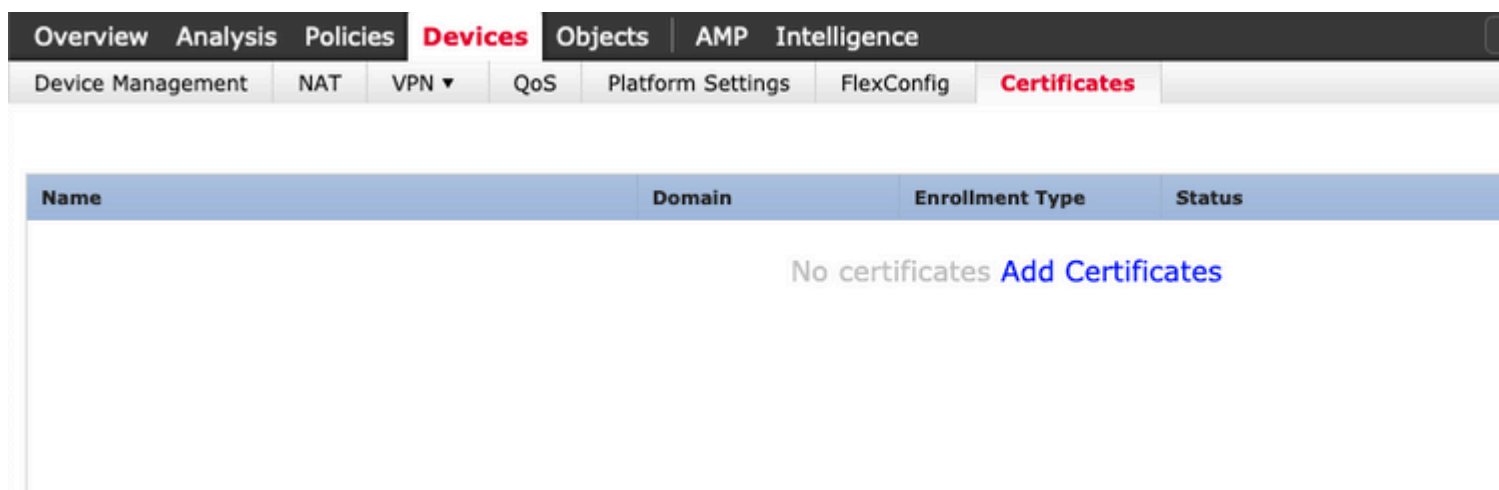
Darüber hinaus muss das Zertifikat eine Common Name (CN)-Erweiterung mit DNS-Name und/oder IP-Adresse enthalten, um Fehler aufgrund eines nicht vertrauenswürdigen Serverzertifikats in Webbrowsern zu vermeiden.

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.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Add Cert Enrollment

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

Enrollment URL:*

Challenge Password:

Confirm Password:

Retry Period: Minutes (Range 1-60)

Retry Count: (Range 0-100)

Fingerprint:

Allow Overrides

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

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: *

```
/3C4h07uzuRDyggwKEBaMdg4DI/z
4x3nk3tTUhyppmbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogkzou6
RqV66G9IE7Z2
xiVrSrJFqkrT795kMb8amBxhb4eXYXUjJmODTPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFskuzay27a48e/IJG2LgRDrA0Kt+jwb57DGSK4mfZsZqhFdQP
LhBNFbyBVb9
dOJUlkmD5vzQDR5qSo+HINEm3E8/q20wrtIzP4MpAabyhr+hEpeP
VMYhIVBOT8h
H8eMJSQjGhhHkuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDv
mwNgy5mTP9cHh
9Or3RIWRzEa11HE3mHO4Rj6DOngufjx+TZRYczownSKLL7LcW1
D8ZcLYmfalDC
W2CZuBR0yVDxvCq4f04ISEIBFOWFSd5rAD/bvk2n6xrJI1SLqABMJ
uslu9KTGH1
bIVKEYACKVYETw==
-----END CERTIFICATE-----
```

Allow Overrides

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.

Add Cert Enrollment

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

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.

The screenshot shows a dialog box titled "Add New Certificate" with a close button (X) and a help button (?). The main text reads: "Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate." Below this, there are two dropdown menus: "Device*" set to "FTD-Virtual" and "Cert Enrollment*" set to "Anyconnect-certificate" with a green plus icon to its right. Under the heading "Cert Enrollment Details:", there are three fields: "Name:" with the value "Anyconnect-certificate", "Enrollment Type:" with the value "Manual", and "SCEP URL:" with the value "NA". At the bottom right, there are two buttons: "Add" and "Cancel".

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

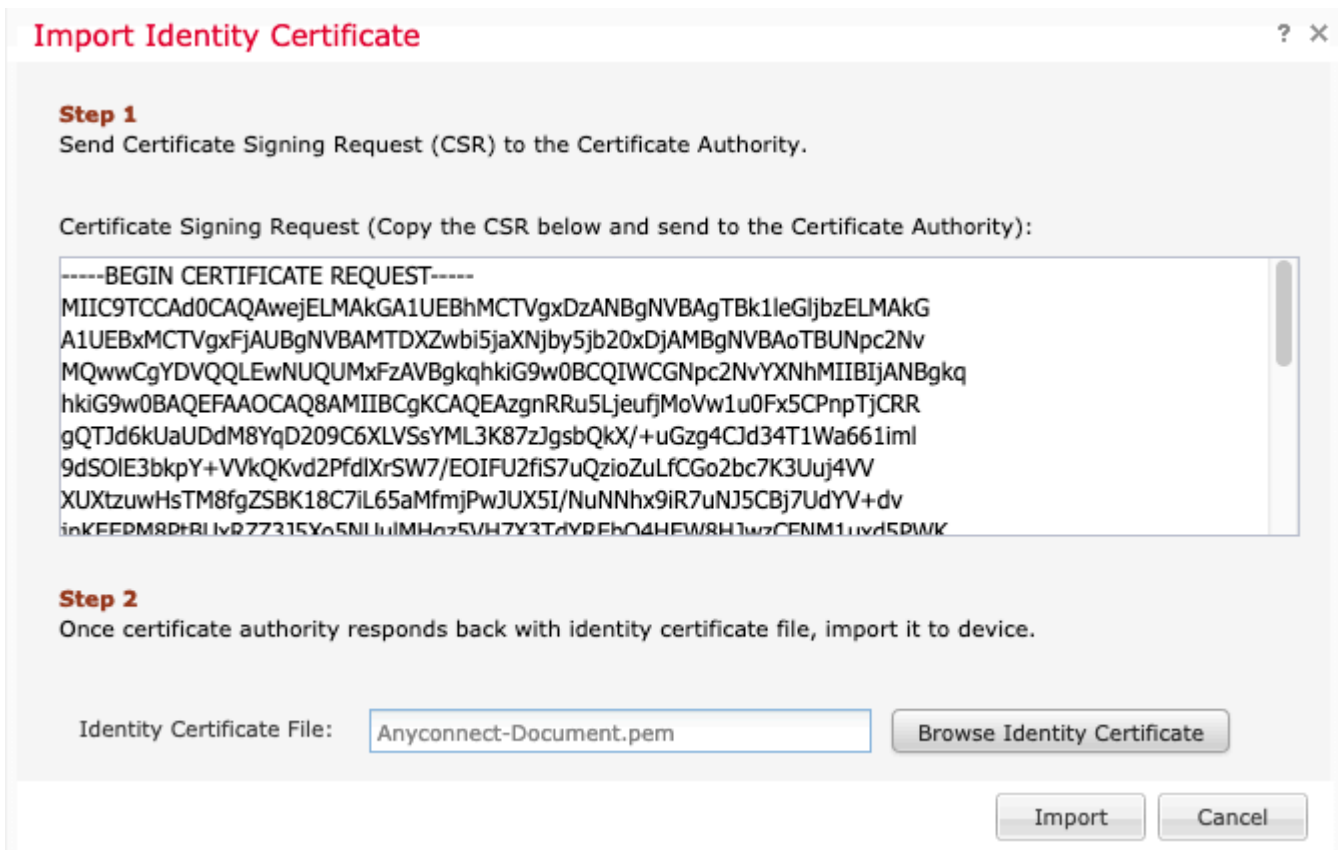
The screenshot shows the "Certificates" tab in a network management interface. The top navigation bar includes "Overview", "Analysis", "Policies", "Devices" (selected), "Objects", "AMP", and "Intelligence". Below this, there are sub-tabs: "Device Management", "NAT", "VPN", "QoS", "Platform Settings", "FlexConfig", and "Certificates" (selected). A table displays certificate information:

Name	Domain	Enrollment Type	Status
FTD-Virtual			
Anyconnect-certificate	Global	Manual	CA ID Identity cer

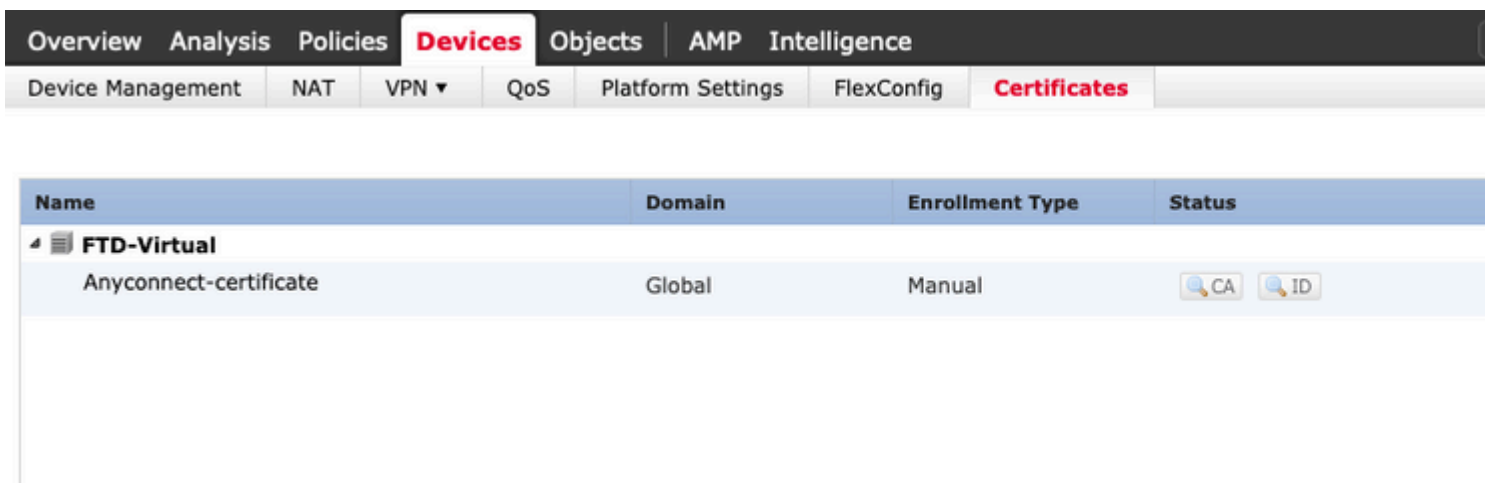
A warning dialog box is overlaid on the table, asking: "Warning: This operation will generate Certificate Signing Request do you want to continue?". It has "Yes" and "No" buttons.

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.

Add RADIUS Server Group

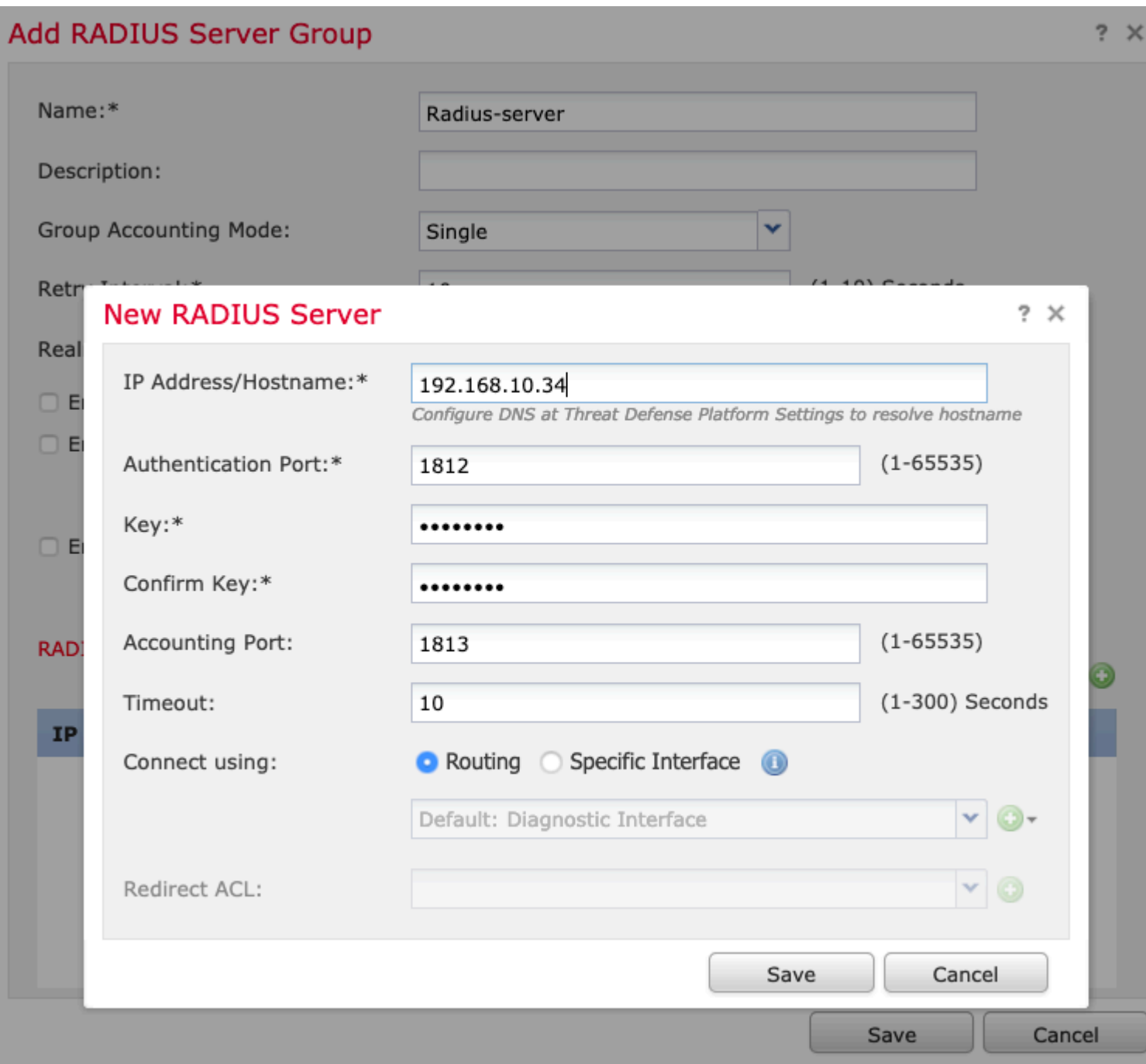


Name:*	<input type="text" value="Radius-server"/>
Description:	<input type="text"/>
Group Accounting Mode:	<input type="text" value="Single"/>
Retry Interval:*	<input type="text" value="10"/> (1-10) Seconds
Realms:	<input type="text"/>
<input type="checkbox"/> Enable authorize only	
<input type="checkbox"/> Enable interim account update	
Interval:*	<input type="text" value="24"/> (1-120) hours
<input type="checkbox"/> Enable dynamic authorization	
Port:*	<input type="text" value="1700"/> (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname
No records to display

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.

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

192.168.10.34



Save

Cancel

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.

Add IPv4 Pool

Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

ⓘ Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

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.

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Hostname	Host Address	User Group	Backup Server List	SCEP

Note: it is highly recommended that at least one server be defined in a profil

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.

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) Corporate - FTD (SSL)

FQDN or IP Address User Group

vpn.cisco.com / ssl

Group URL

Connection Information

Primary Protocol SSL

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address

Add

Move Up

Move Down

Delete

OK Cancel

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

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobil
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --		

Note: it is highly recommended that at least one server be defined in a profile.

Add... Edit...

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.

Add AnyConnect File

? X

Name:*	<input type="text" value="Corporate-profile(SSL)"/>
File Name:*	<input type="text" value="FTD-corp-ssl.xml"/> <input type="button" value="Browse.."/>
File Type:*	<input type="text" value="AnyConnect Client Profile"/> ▾
Description:	<input type="text"/>

Schritt 6: AnyConnect-Images hochladen

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

AnyConnect Headend Deployment Package (Mac OS)	26-Jun-2019	51.22 MB	↓
anyconnect-macos-4.7.04056-webdeploy-k9.pkg			

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**.

Add AnyConnect File ? X

Name:*

File Name:*

File Type:* ▼

Description:

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.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:* TAC

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices

Search

FTD-Virtual

Selected Devices

FTD-Virtual

Add

Before You Start

Before you start, configuration elements to complete Remote Access VPN.

Authentication Server

Configure [Realm](#) or to authenticate VPN.

AnyConnect Client

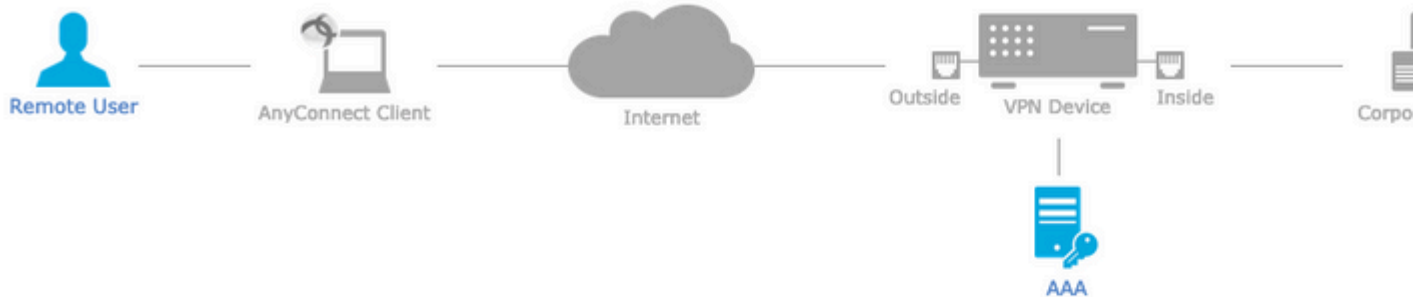
Make sure you have for VPN Client download the relevant Cisco client during the wizard.

Device Interface

Interfaces should be targeted [devices](#) so as a security zone enable VPN access.

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.

Remote Access VPN Policy Wizard



Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: ▼
 Authentication Server:* ▼ + (Realm or RADIUS)
 Authorization Server: ▼ + (RADIUS)
 Accounting Server: ▼ + (RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools
 IPv4 Address Pools: ✎
 IPv6 Address Pools: ✎

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. or create a Group Policy object.

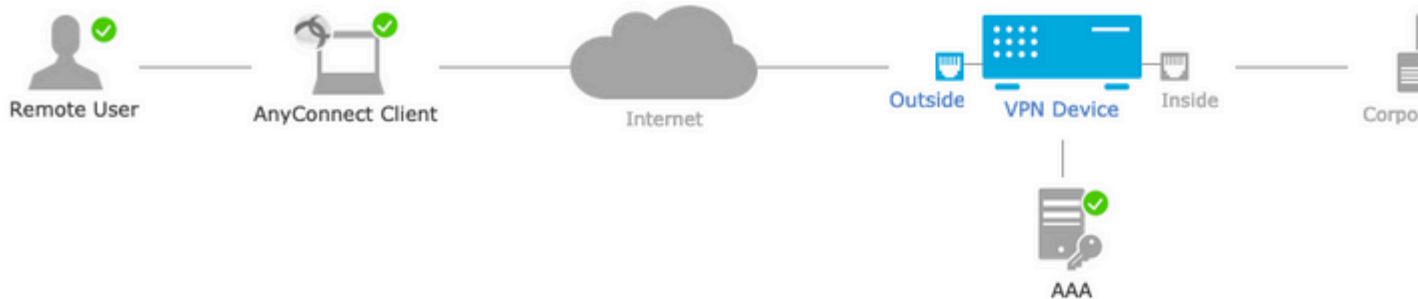
Group Policy:* ▼ +
[Edit Group Policy](#)

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.

Remote Access VPN Policy Wizard

1 Policy Assignment > 2 Connection Profile > 3 AnyConnect > **4 Access & Certificate** > 5



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back

Next

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

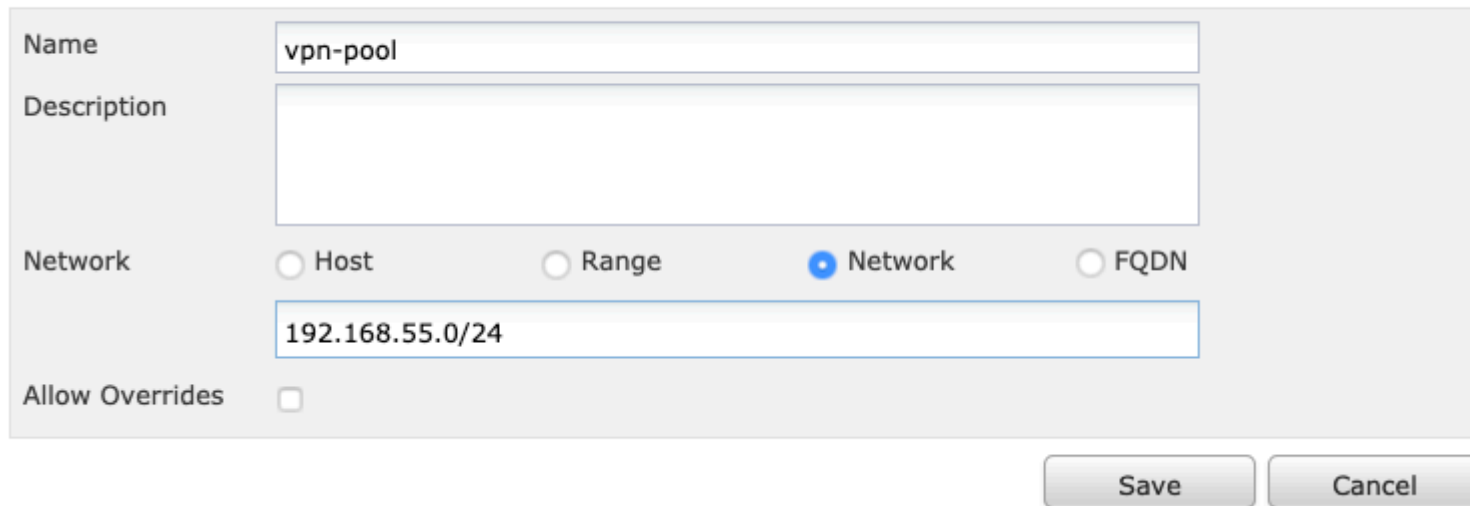
Sämtliche VPN-, SSL-Zertifikate und AnyConnect-Pakete betreffende Konfigurationen werden per P

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.

New Network Object



Name: vpn-pool

Description:

Network: Host Range Network FQDN

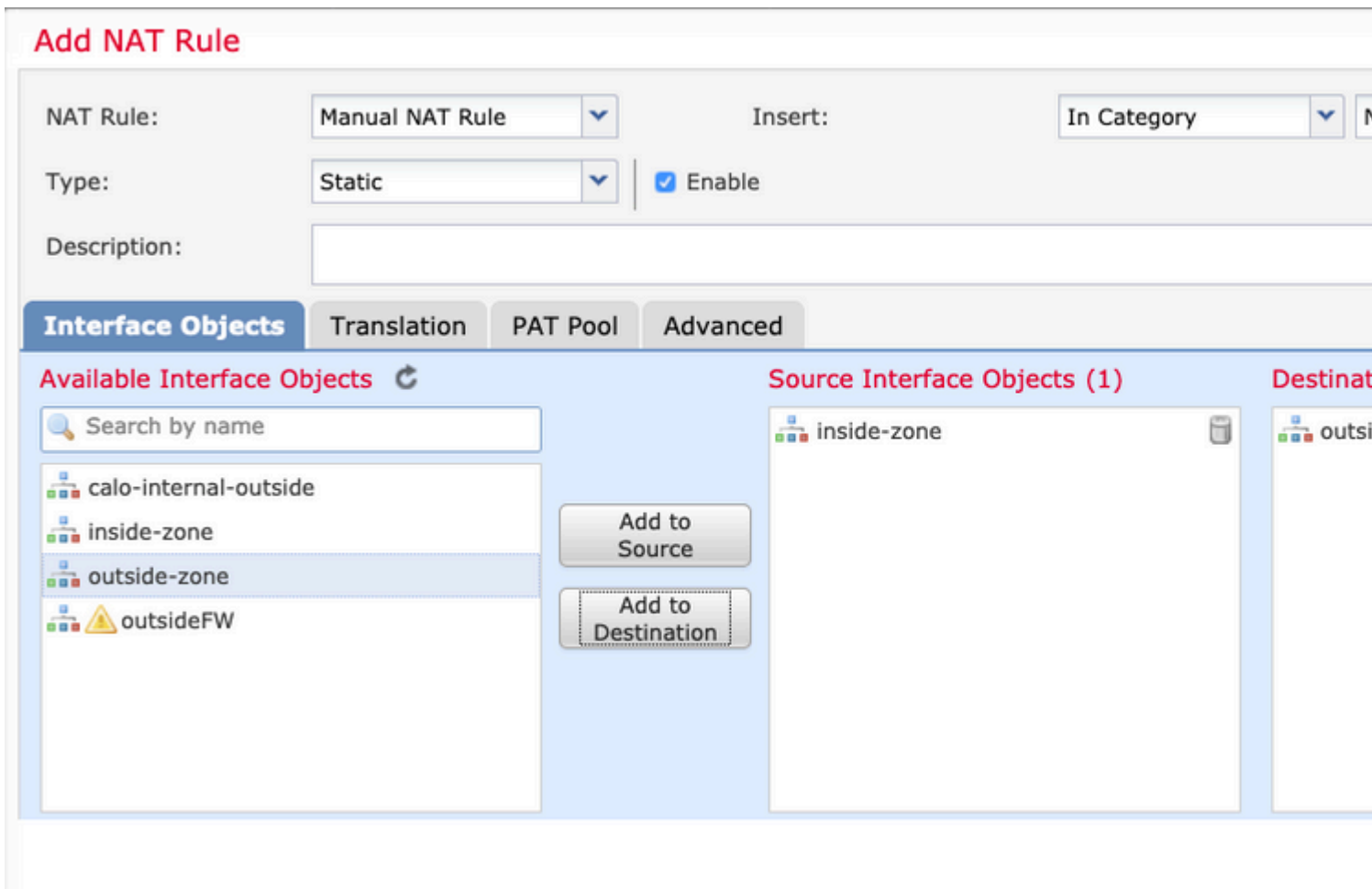
192.168.55.0/24

Allow Overrides:

Save Cancel

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.

Add NAT Rule

NAT Rule:

Manual NAT Rule

Insert:

In Category

Type:

Static

Enable

Description:

Interface Objects

Translation

PAT Pool

Advanced

Original Packet

Original Source:*

FTDv-Inside-SUPERNE

Original Destination:

Address

vpn-pool

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source:

Address

FTDv-Inside-SUPERNE

Translated Destination:

vpn-pool

Translated Source Port:

Translated Destination Port:

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.

Edit NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination Interface
- Unidirectional

5. Dies ist das Ergebnis der NAT-Ausnahmekonfiguration.

1 Static inside-zone outside-zone FTDv-Inside-SUPERNE vpn-pool FTDv-Inside-SUPERNE vpn-pool

Die im vorherigen Abschnitt verwendeten Objekte sind die unten beschriebenen.

Name

Description

Network Host Range Network

Allow Overrides

Name	<input type="text" value="vpn-pool"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/>
	<input type="text" value="192.168.55.0/24"/>
Allow Overrides	<input type="checkbox"/>

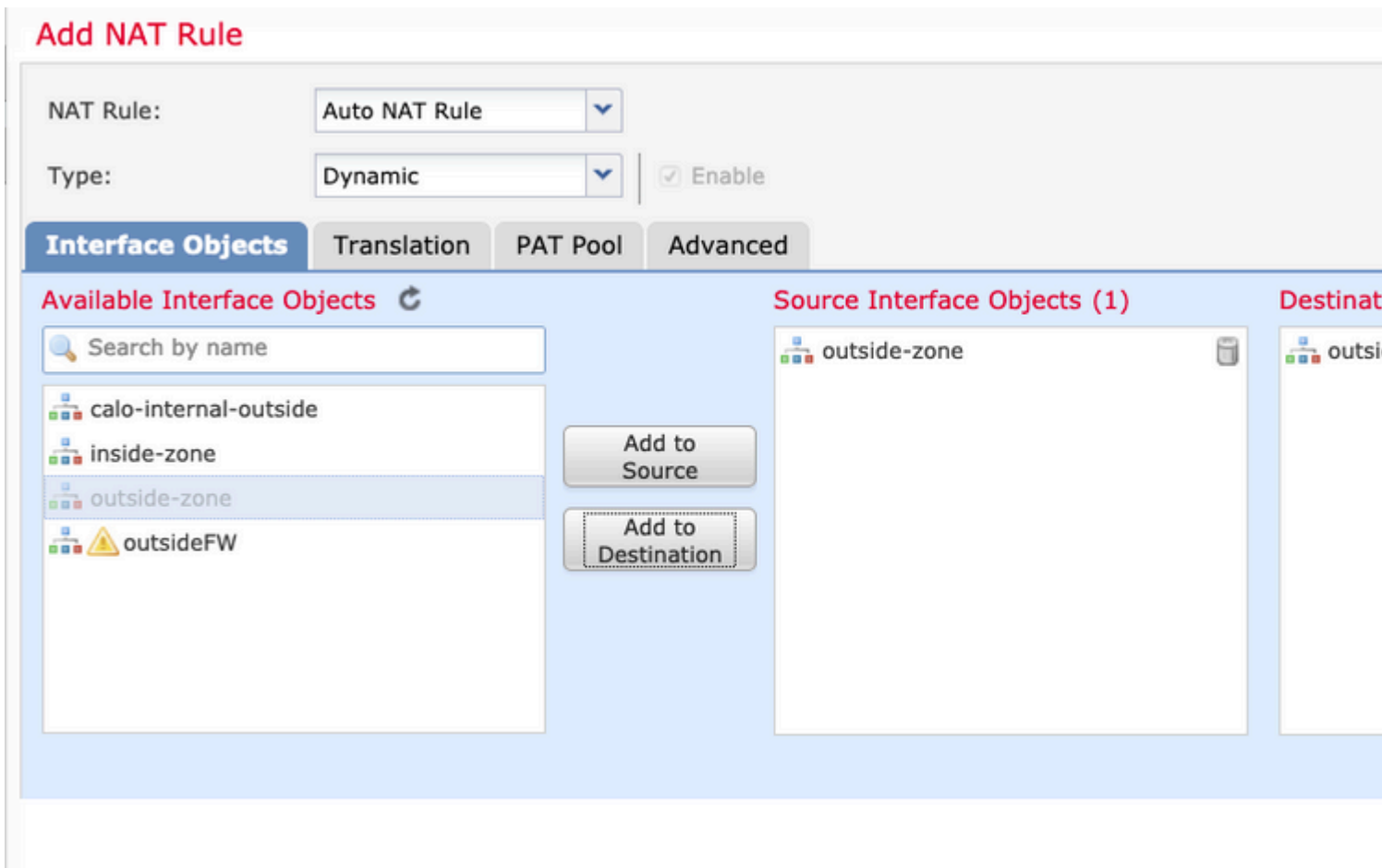
Schritt 2: Haarnadelkonfiguration

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.

Add NAT Rule

NAT Rule: ▼

Type: ▼ Enable

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* ▼ +

Original Port: ▼

Translated Packet

Translated Source: ▼ i The va Object

Translated Port:

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

Rules									
Filter by Device Filter Rules									
#	Direction	Type	Source Interface Obj...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destination
▼ NAT Rules Before									
1	↔	Static	inside-zone	outside-zone	FTDv-Inside-SUPERNE	vpn-pool		FTDv-Inside-SUPERNE	vpn-pool
▼ Auto NAT Rules									
#	→	Dyna...	outside-zone	outside-zone	vpn-pool			Interface	
▼ NAT Rules After									

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.