

AnyConnect VPN-client op FTD configureren: haarspeld en NAT-vrijstelling

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Stap 1. Een SSL-certificaat importeren](#)

[Stap 2. Een RADIUS-server configureren](#)

[Stap 3. Een IP-groep maken](#)

[Stap 4. Een XML-profiel maken](#)

[Stap 5. AnyConnect XML-profiel uploaden](#)

[Stap 6. AnyConnect-afbeeldingen uploaden](#)

[Stap 7. Wizard Externe toegang VPN](#)

[NAT-vrijstelling en haarspeld](#)

[Stap 1. NAT-uitzonderingsconfiguratie](#)

[Stap 2. haarspeldconfiguratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u de Cisco Remote Access VPN-oplossing (AnyConnect) kunt configureren op Firepower Threat Defence (FTD), v6.3, beheerd door FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis externe toegang VPN, Secure Sockets Layer (SSL) en Internet Key Exchange versie 2 (IKEv2) kennis
- Basisverificatie, autorisatie en accounting (AAA) en RADIUS-kennis
- Basiskennis van het VCC
- Basiskennis van FTD

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco VCC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

Dit document beschrijft de procedure voor het configureren van Cisco Remote Access VPN-oplossing (AnyConnect) op Firepower Threat Defence (FTD), versie 6.3, beheerd door Firepower Management Center (FMC).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document is bedoeld voor de configuratie op FTD-apparaten. Als u naar het ASA-configuratievoorbeeld zoekt, raadpleegt u het document: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

Beperkingen:

Op dit moment worden deze functies niet ondersteund door FTD, maar nog wel door ASA-apparaten:

- Dubbele AAA-verificatie (beschikbaar op FTD versie 6.5)
- Dynamisch toegangsbeleid
- Hostscan
- ISE-houding
- RADIUS-CoA
- VPN-taakverdeling
- Lokale verificatie (beschikbaar op Firepower Device Manager 6.3). Cisco bug-id ([CSCvf92680](#))
- LDAP-kenmerkkaart (beschikbaar via FlexConfig, Cisco-bug-id [CSC64585](#))
- Aangepaste AnyConnect
- AnyConnect-scripts
- AnyConnect-lokalisatie
- VPN-services per app
- SCEP-proxy
- WSA-integratie
- SAML SSO (Cisco bug-id [CSCvq90789](#))
- Gelijktijdige IKEv2 dynamische cryptokaart voor RNA en L2L VPN
- AnyConnect-modules (NAM, Hostscan, AMP Enabler, SBL, Umbrella, webbeveiliging, enzovoort). DART is de enige module die standaard op deze versie is geïnstalleerd.
- TACACS, Kerberos (KCD-verificatie en RSA/SDI)
- Browser Proxy

Configureren

Om door de wizard Externe toegang VPN in het VCC te kunnen lopen, moeten de volgende stappen worden voltooid:

Stap 1. Een SSL-certificaat importeren

Certificaten zijn essentieel wanneer u AnyConnect configureert. Alleen op RSA gebaseerde certificaten worden ondersteund voor SSL en IPSec.

Elliptic Curve Digital Signature Algorithm (ECDSA)-certificaten worden ondersteund in IPSec, maar het is niet mogelijk om een nieuw AnyConnect-pakket of XML-profiel te implementeren wanneer op ECDSA gebaseerd certificaat wordt gebruikt.

Het kan worden gebruikt voor IPSec, maar u moet de AnyConnect-pakketten samen met het XML-profiel vooraf implementeren, alle XML-profielupdates moeten handmatig worden uitgevoerd op elke client (Cisco bug-id [CSCtx42595](#)).

Daarnaast moet het certificaat een Common Name (CN)-extensie met DNS-naam en/of IP-adres bevatten

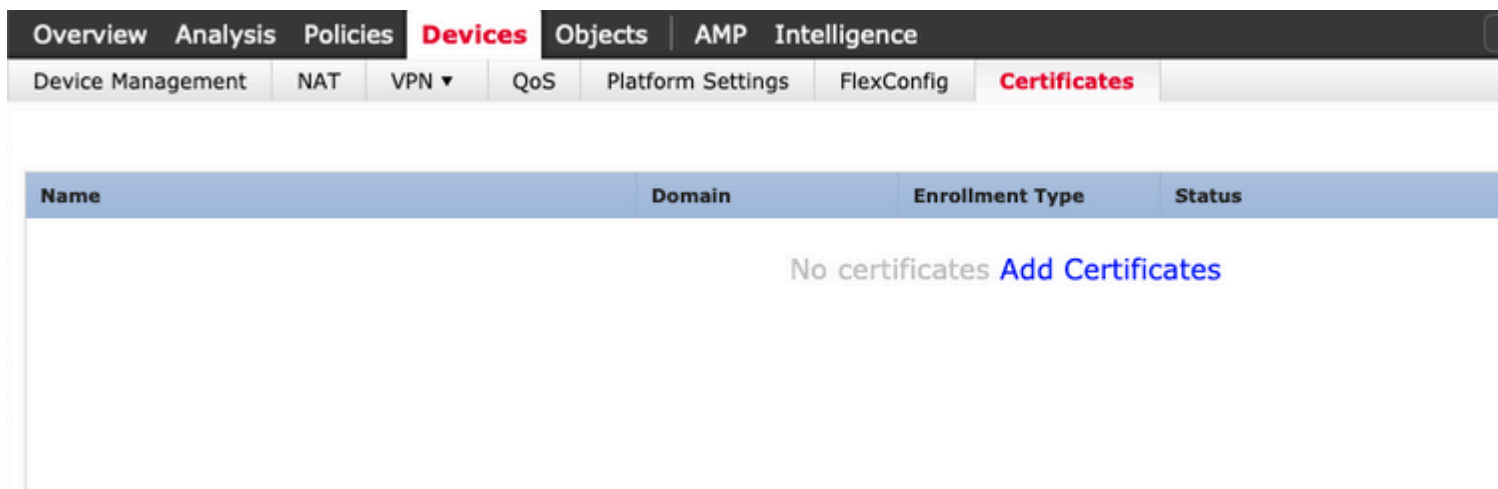
om fouten in het "Onbetrouwbare servercertificaat" in webbrowsers te voorkomen.

Opmerking: op FTD-apparatuur is het certificaat van de certificeringsinstantie (CA) vereist voordat het verzoek tot ondertekening van het certificaat (CSR) wordt gegenereerd.

- Als de CSR wordt gegenereerd in een externe server (zoals Windows Server of OpenSSL), is de **handmatige inschrijvingsmethode** bedoeld om te mislukken, omdat FTD handmatige toeteninschrijving niet ondersteunt.
- Er moet een andere methode worden gebruikt, zoals PKCS12.

Om een certificaat voor het FTD-apparaat te verkrijgen met de handmatige inschrijvingsmethode, moet een CSR worden gegenereerd, ondertekend met een CA en vervolgens het identiteitscertificaat importeren.

1. Navigeren naar **Apparaten > Certificaten** en selecteer **Toevoegen** zoals in de afbeelding.



2. Selecteer het **apparaat** en voeg een nieuw object **Cert Enrollment toe** zoals in de afbeelding.

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. Selecteer handmatig **Inschrijftype** en plak het CA-certificaat (het certificaat dat bedoeld is om de CSR te ondertekenen).

Add Cert Enrollment ? X

Name* Anyconnect-certificate

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Certificate: *

```

/3C4h07uzuRDyggwKEBaMdg4DI/z
4x3nk3tTUhyppmbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogkzou6
RqV66G9IE7Z2
xiVrSrJFqhrT795kMb8amBxhb4eXYXUgJmODTPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFskuzay27a48e/IJG2LgRDrA0Kt+jwb57DGSK4mfZsZqhFdQP
LhBNFbyBVb9
dOJukmd5vzQDR5qSo+HINEm3E8/q20wrtIzP4MpAabyhr+hEpeP
VMYhIVBOT8h
H8eMJSQGHhHkuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDv
mwNgy5mTP9chla
9Or3RIWRzEa11HE3mHO4Rj6DOnmgujfx+TZRYczownSKLL7LcW1
D8ZcLYmfaIdC
W2CZuBR0yVDxvCq4f04ISEIBFOWFSd5rAD/bvk2n6xrJI1SLqABMJJ
uslu9KTGH1
bIVKEYACKVYETw==
-----END CERTIFICATE-----

```

Allow Overrides

Save Cancel

4. Selecteer het tabblad **Certificaatparameters** en selecteer "Aangepaste FQDN" voor het veld **Inclusief FQDN** en vul de certificaatgegevens in zoals in de afbeelding.

Add Cert Enrollment ? X

Name* Anyconnect-certificate

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN: Use Device Hostname as FQDN

Include Device's IP Address:

Common Name (CN): vpn.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): MX

State (ST): Mexico

Country Code (C): MX

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

5. Selecteer het tabblad **Sleutel** en selecteer het type toets. U kunt naam en grootte kiezen. Voor RSA is 2048 bytes een minimumvereiste.

6. Selecteer Opslaan, bevestig het **apparaat** en selecteer onder **Volledige inschrijving** het trustpoint dat zojuist is gemaakt, selecteer **Toevoegen** om het certificaat te implementeren.

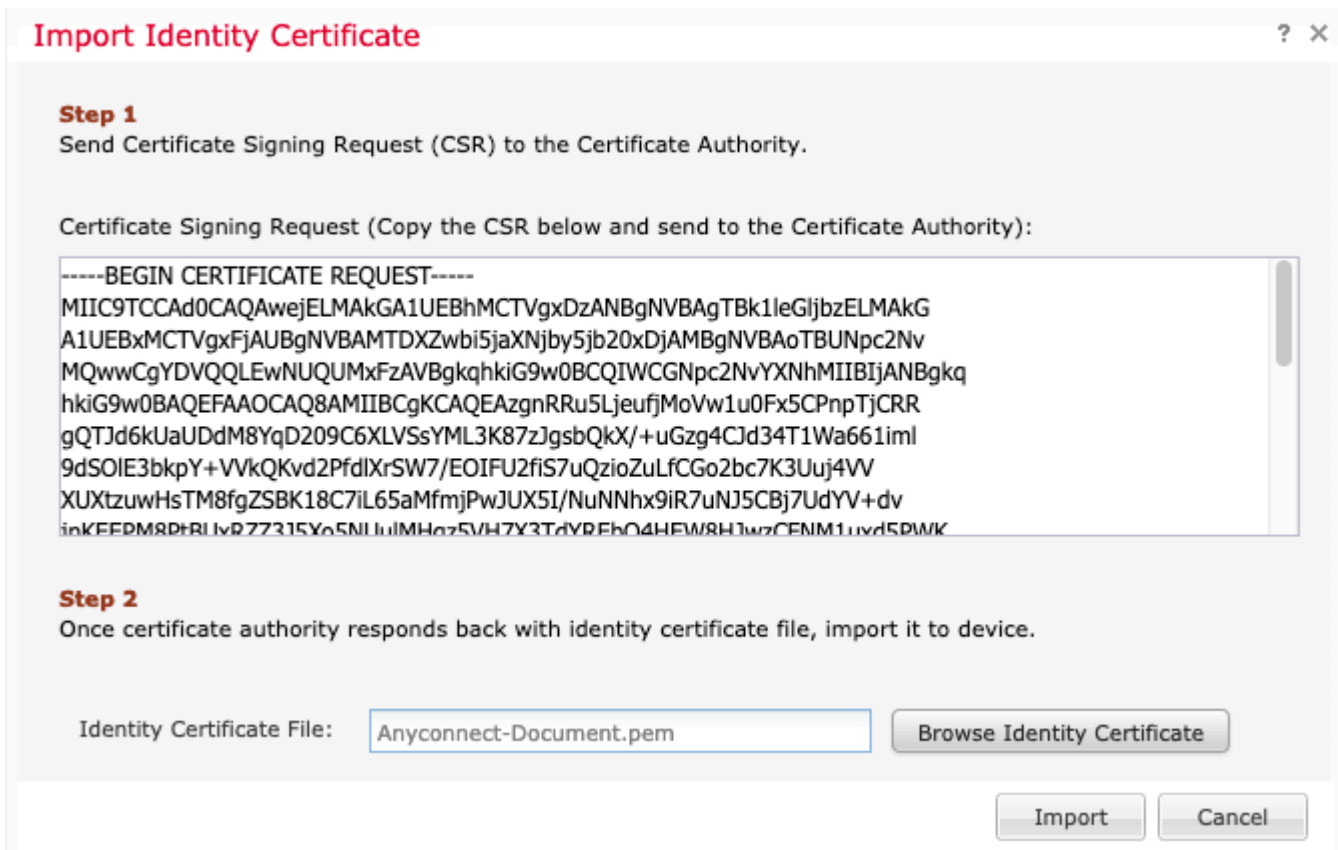
The screenshot shows a dialog box titled "Add New Certificate" with a close button (X) and a help button (?). The text inside reads: "Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate." Below this, there are two dropdown menus: "Device*" set to "FTD-Virtual" and "Cert Enrollment*" set to "Anyconnect-certificate" with a 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. Selecteer in de kolom **Status** het **ID**-pictogram en selecteer **Ja** om de MVO te genereren zoals in de afbeelding.

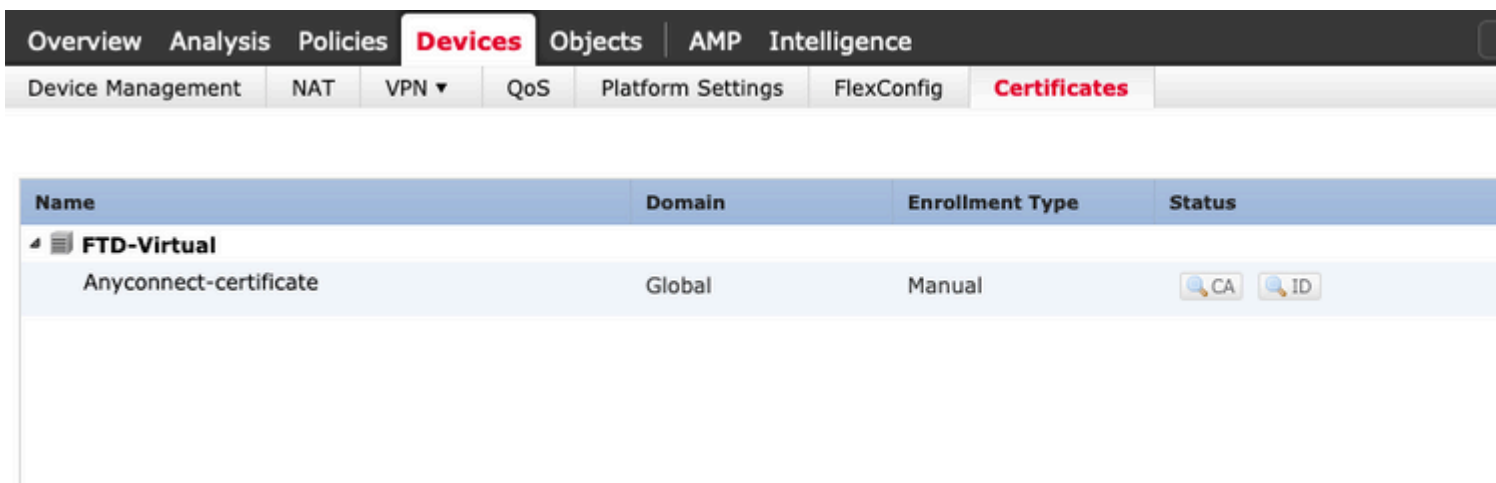
The screenshot shows the "Certificates" tab in a network management interface. The table has columns for "Name", "Domain", "Enrollment Type", and "Status". A row is highlighted for "Anyconnect-certificate" under the "FTD-Virtual" device, with "Global" as the domain and "Manual" as the enrollment type. In the "Status" column, there are three icons: a magnifying glass over "CA", a yellow triangle with "ID", and a yellow triangle with "Identity cer". A "Warning" dialog box is overlaid on the table, containing a question mark icon and the text: "This operation will generate Certificate Signing Request do you want to continue?". There are "Yes" and "No" buttons at the bottom of the dialog.

8. Kopieer CSR en onderteken het met uw gewenste CA (bijvoorbeeld GoDaddy of DigiCert).

9. Zodra het identiteitscertificaat van de CA (die in het base64-formaat moet zijn) is ontvangen, selecteert u **Identiteitscertificaat doorbladeren** en plaatst u het certificaat in de lokale computer. Selecteer **Importeren**.



10. Na invoer kunnen zowel CA- als ID-certificaatgegevens worden weergegeven.



Stap 2. Een RADIUS-server configureren

Op door het VCC beheerde FTD-apparaten wordt de lokale gebruikersdatabse niet ondersteund. Er moet een andere verificatiemethode worden gebruikt, zoals RADIUS of LDAP.

1. Navigeer naar **objecten > Objectbeheer > RADIUS-servergroep > RADIUS-servergroep toevoegen** zoals in de afbeelding wordt weergegeven.

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

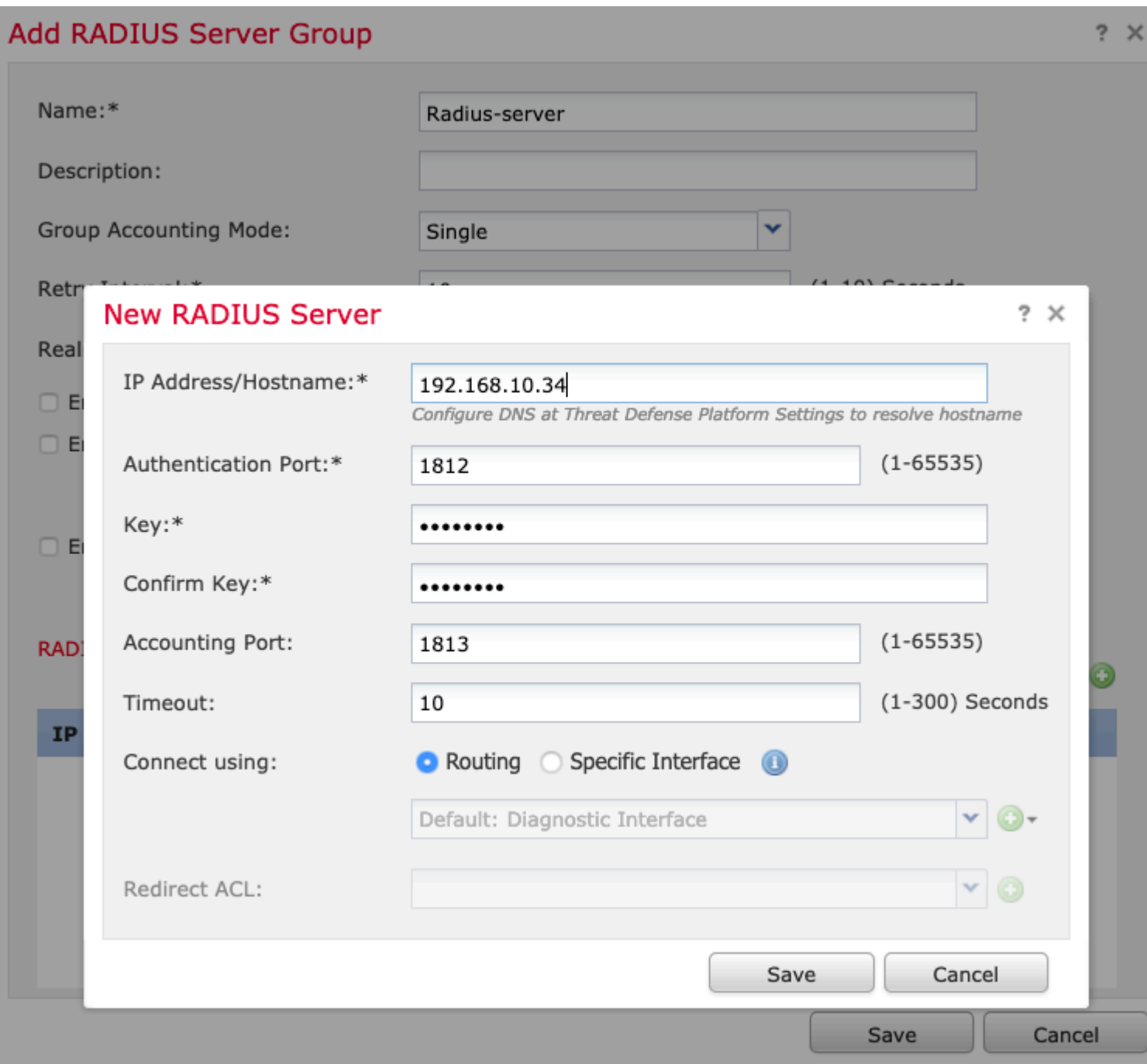
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname
No records to display

2. Wijs een naam toe aan de **Radius Server Group** en voeg het IP-adres van de Radius-server toe, samen met een gedeeld geheim (het gedeelde geheim is vereist om het FTD te koppelen met de Radius-server). Selecteer **Opslaan** zodra dit formulier is ingevuld zoals in de afbeelding.



3. De RADIUS-serverinformatie is nu beschikbaar in de lijst Radius Server zoals in de afbeelding.

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

Stap 3. Een IP-groep maken

1. Navigeer naar **objecten > Objectbeheer > Adrespools > IPv4-pools toevoegen**.
2. Wijs de naam en het bereik van IP-adressen toe. Het veld **Masker** is niet vereist, maar kan worden gespecificeerd zoals in de afbeelding.

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

Stap 4. Een XML-profiel maken

1. Download de **Profile Editor** tool van Cisco.com en voer de applicatie uit.
2. Navigeer in de toepassing Profile Editor naar **Server List** en selecteer **Add** zoals in de afbeelding.

The screenshot shows the Profile Editor interface. On the left is a navigation menu with the following items: VPN, Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Pinning, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List. The main area is titled "Server List" and contains a table with the following columns: Hostname, Host Address, User Group, Backup Server List, and SCEP. The table is currently empty. Below the table, there is a note: "Note: it is highly recommended that at least one server be defined in a profil".

3. Wijs een **weergavenaam, volledig gekwalificeerde domeinnaam (FQDN) of IP-adres toe** en selecteer **OK** zoals in de afbeelding.

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. De ingang is nu zichtbaar in het menu **Serverlijst**:

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. Navigeren naar **Bestand > Opslaan als**.

Opmerking: Sla het profiel op met een gemakkelijk herkenbare naam met de extensie **.xml**.

Stap 5. AnyConnect XML-profiel uploaden

1. Ga in het VCC naar Objecten > **Objectbeheer** > **VPN** > **AnyConnect File** > **Add AnyConnect File**.
2. Wijs een **naam** aan het object toe en klik op **Bladeren**, zoek het clientprofiel in uw lokale systeem en selecteer **Opslaan**.

Waarschuwing: Zorg ervoor dat u het **AnyConnect-clientprofiel** selecteert als het bestandstype.

Add AnyConnect File

Name:* Corporate-profile(SSL)

File Name:* FTD-corp-ssl.xml

File Type:* AnyConnect Client Profile

Description:

Stap 6. AnyConnect-afbeeldingen uploaden

1. Download de afbeeldingen van webimplementation (**.pkg**) van de downloadwebpagina van Cisco.

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

2. Navigeer naar objecten > **Objectbeheer** > **VPN** > **AnyConnect File** > **AnyConnect File**.
3. Wijs een naam toe aan het AnyConnect-pakketbestand en selecteer het bestand **.pkg** uit uw lokale systeem nadat het is geselecteerd.
4. Selecteer **Opslaan**.

Add AnyConnect File ? X

Name:*

File Name:*

File Type:* ▼

Description:

Opmerking: extra pakketten kunnen worden geüpload op basis van uw vereisten (Windows, Mac, Linux).

Stap 7. Wizard Externe toegang VPN

Gebaseerd op de vorige stappen kan de Wizard Externe toegang dienovereenkomstig worden gevolgd.

1. Navigeer naar **Apparaten > VPN > Externe toegang**.
2. Wijs de naam van het beleid voor externe toegang toe en selecteer een FTD-apparaat uit de lijst met **beschikbare apparaten**.

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.

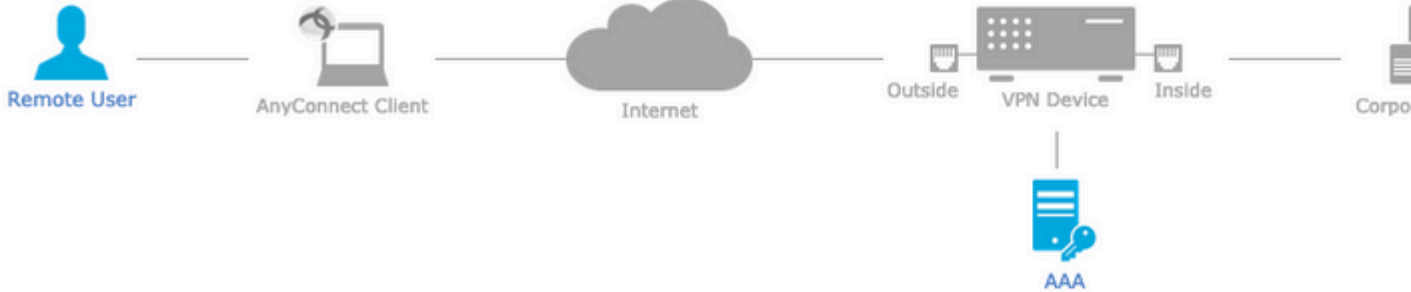
Device Interface

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

3. Wijs de **naam** van het **verbindingprofiel toe** (de naam van het verbindingprofiel is de naam van de tunnelgroep), selecteer de **verificatieserver** en **adresgroepen** zoals in de afbeelding.

Remote Access VPN Policy Wizard

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



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) i
 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](#)

Back

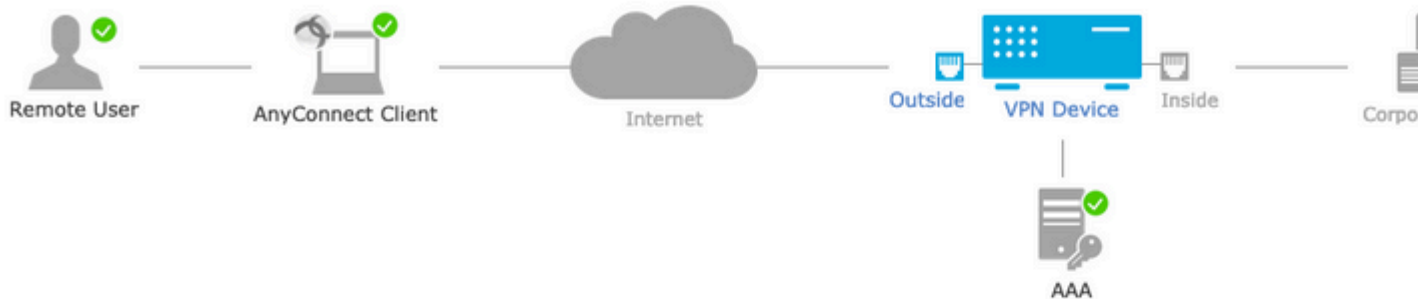
Next

4. Selecteer het +-symbool om **Groepsbeleid** te maken.

in dit scenario is de FTD zo geconfigureerd dat hij geen VPN-verkeer inspecteert, wordt de optie Toegangsbeheer (ACS) omzeild.

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. Selecteer **Voltoeien** en **wijzig** de wijzigingen:

Alle configuratie met betrekking tot VPN, SSL-certificaten en AnyConnect-pakketten wordt via FMC

is een voorkeursvertaalmethode die wordt gebruikt om te voorkomen dat verkeer naar het internet wordt geleid als het is bedoeld om via een VPN-tunnel te stromen (Externe toegang of Site-to-Site).

Dit is nodig wanneer het verkeer van uw interne netwerk bedoeld is om over de tunnels te stromen zonder enige vertaling.

1. Navigeer naar **Objecten > Netwerk > Netwerk toevoegen > Object toevoegen** zoals in de afbeelding.

New Network Object

Name

Description

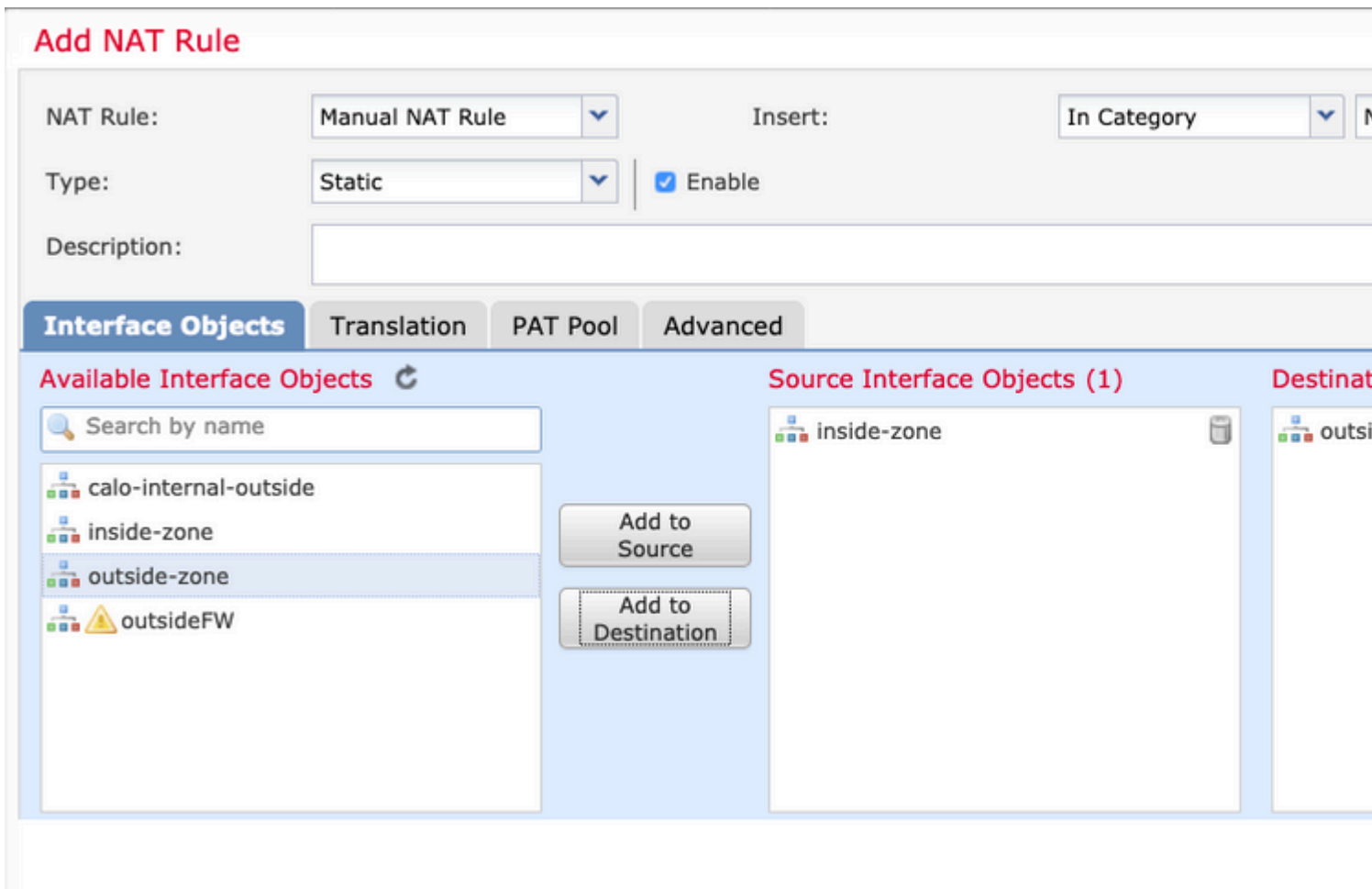
Network Host Range Network FQDN

Allow Overrides

Save Cancel

2. Navigeer naar **apparaat > NAT**, selecteer het NAT-beleid dat door het apparaat in kwestie wordt gebruikt en maak een nieuwe instructie.

Opmerking: de verkeersstroom gaat van binnen naar buiten.



3. Selecteer de interne bronnen achter de FTD (**oorspronkelijke bron** en **vertaalde bron**) en de bestemming als de lokale ip-pool voor de AnyConnect-gebruikers (**oorspronkelijke bestemming** en **vertaalde bestemming**) zoals in de afbeelding.

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:

Translated Destination:

Translated Source Port:

Translated Destination Port:

4. Zorg ervoor dat de opties (zoals in de afbeelding) van elkaar worden gewisseld, zodat "**no-proxy-arp**" en "**route-lookup**" in de NAT-regel zijn ingeschakeld, en selecteer **OK** zoals in de afbeelding.

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. Dit is het resultaat van de NAT-vrijstellingsconfiguratie.



De in de vorige sectie gebruikte objecten worden hieronder beschreven.

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"/>

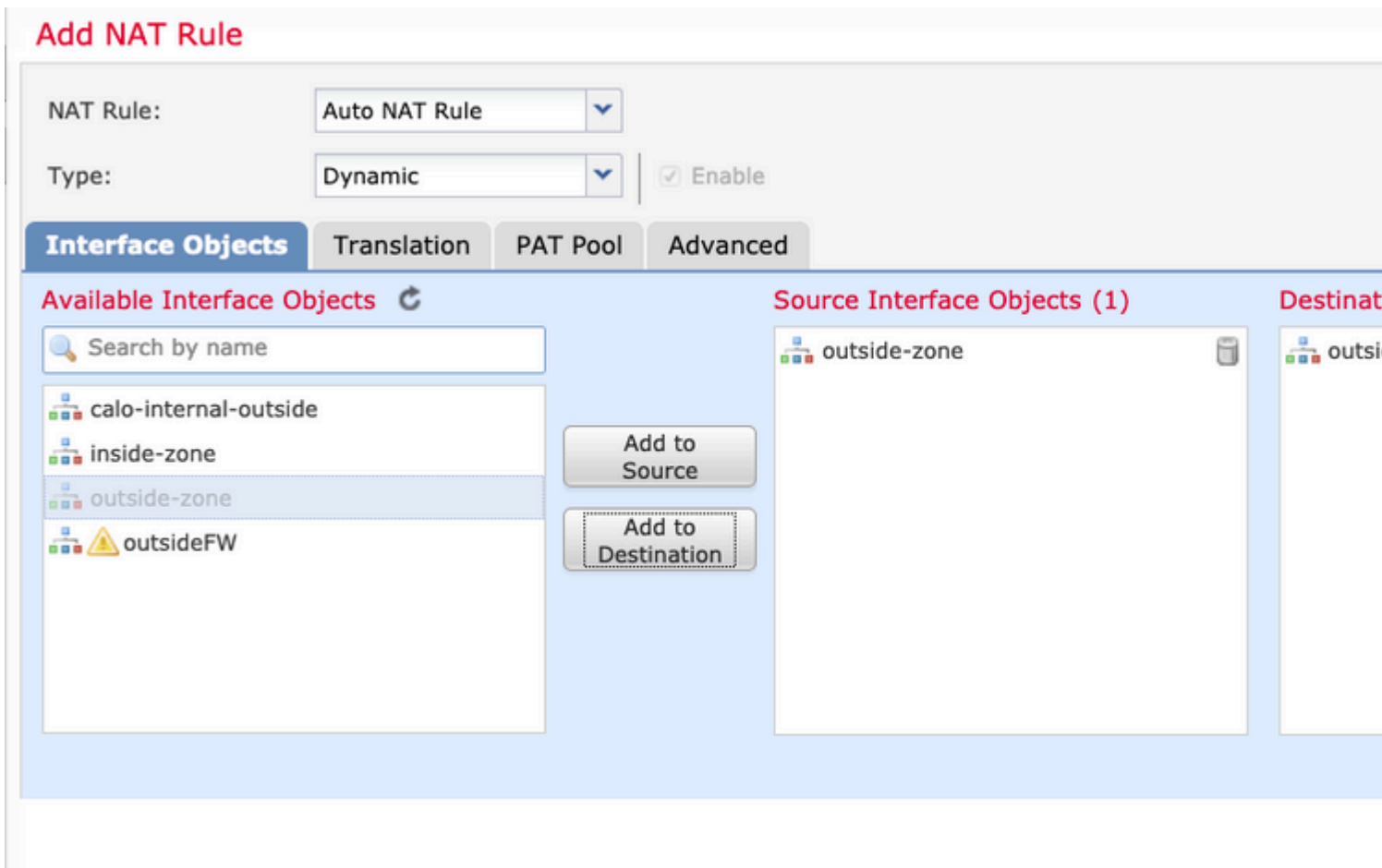
Stap 2. haarspeldconfiguratie

Ook bekend als **U-turn**, dit is een vertaalmethode die het verkeer toelaat om over dezelfde interface te stromen als het verkeer ontvangen wordt.

Bijvoorbeeld, wanneer AnyConnect wordt geconfigureerd met een **Full-tunnel** split-tunnelbeleid, worden de interne bronnen benaderd volgens het NAT-vrijstellingsbeleid. Als het AnyConnect-clientverkeer bedoeld is om een externe site op internet te bereiken, is de haarspeld NAT (of U-turn) verantwoordelijk voor het routeren van het verkeer van buiten naar buiten.

Een VPN pool object moet gemaakt worden voor de NAT configuratie.

1. Maak een nieuwe NAT-verklaring, selecteer **Auto NAT-regel** in het veld **NAT-regel** en selecteer **Dynamisch** als **NAT-type**.
2. Selecteer dezelfde interface voor de **bron-** en **doelinterfaceobjecten** (buiten):



3. Selecteer op het tabblad Vertaling als **Oorspronkelijke bron** het VPN-pool object en selecteer **Doelinterface IP** als **Vertaalde bron**, selecteer **OK** zoals in de afbeelding.

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. Dit is de samenvatting van de NAT-configuratie zoals in de afbeelding.

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. Klik op **Opslaan** en de wijzigingen **implementeren**.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Voer deze opdrachten uit in de FTD-opdrachtregel.

- **sh crypto ca-certificaten**
- **tonen in werking stellen-configuratie ip lokale pool**
- **tonen in werking stellen-configuratiwebvpn**
- **tonen in werking stelt-Config tunnel-groep**

- **tonen in werking stelt-configuratiegroepsbeleid**
- **Toon in werking stelt -in werking stellen-configuratiesl**
- **toon in werking stelt -in werking stellen-Config NAT**

Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuratie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.