

# AnyConnect VPN op FTD configureren met Cisco ISE als RADIUS-server met Windows Server 2012 Root CA

## Inhoud

[Inhoud](#)

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[Start CA-certificaat vanuit Windows Server uit](#)

[Installeer het Root CA-certificaat op de Windows/Mac-pc's van de medewerker](#)

[Genereert een CSR op FTD, laat CSR ondertekend door Windows Server Root CA en installeer dat ondertekende certificaat op FTD](#)

[ImageConnect + AnyConnect Profile Editor downloaden en een .xml-profiel maken](#)

[AnyConnect VPN op FTD configureren \(gebruik het Root CA-certificaat\)](#)

[Configureer de FTD NAT-regel om het VPN-verkeer van NAT vrij te stellen omdat deze toch wordt gedecrypteerd en om toegangscontroleregels/toegangscontroleregels te maken](#)

[Voeg FTD toe als Netwerkapparaat en stel beleid in op Cisco ISE \(gebruik RADIUS gedeeld geheim\)](#)

[Downloaden, installeren en aansluiten op de FTD met AnyConnect VPN-client op Windows/Mac PC's van werknemers](#)

[Verifiëren](#)

[FTD](#)

[Cisco ISE](#)

[AnyConnect VPN-client](#)

[Problemen oplossen](#)

[DNS](#)

[certificaatsterkte \(voor browser-compatibiliteit\)](#)

[Connectiviteit en firewallconfiguratie](#)

## Inhoud

## Inleiding

Dit document beschrijft hoe u AnyConnect VPN (Virtual Private Network) kunt configureren in een FTD (Firepower Threat Defense) firewall met Cisco ISE (Identity Services Engine) als RADIUS-server. We gebruiken een Windows Server 2012 als onze Root CA (certificaatautoriteit), zodat de communicatie via VPN wordt beveiligd met certificaten, d.w.z. dat de PC van de werknemer het

certificaat van de FTD vertrouwde omdat het FTD VPN-certificaat is ondertekend door onze Windows Server 2012 Root CA

## Voorwaarden

### Vereisten

U moet de volgende functies en functies in uw netwerk hebben:

- Firepower Management Center en Firepower Threat Defreat Firepower, ingezet met basisconnectiviteit
- Cisco ISE-applicatie en -uitvoering in uw netwerk
- Windows Server (met actieve map) is uitgevoerd en Windows/Mac PC van de werknemers is aangesloten bij het AD (Active Directory) domein

In ons voorbeeld hieronder, zullen de werknemers de AnyConnect Client op hun Windows/Mac PC openen en zullen zij zich veilig met de externe interface van de FTD verbinden via VPN met behulp van hun geloofsbrieven. De FTD zal hun gebruikersnaam en wachtwoord tegen Cisco ISE controleren (die met Windows Server Active Directory zal controleren om hun gebruikersnaam, wachtwoord en groep te controleren, d.w.z. alleen gebruikers in de AD Group 'Werknemers' zullen in VPN in het bedrijfsnetwerk kunnen belanden.

### Gebruikte componenten

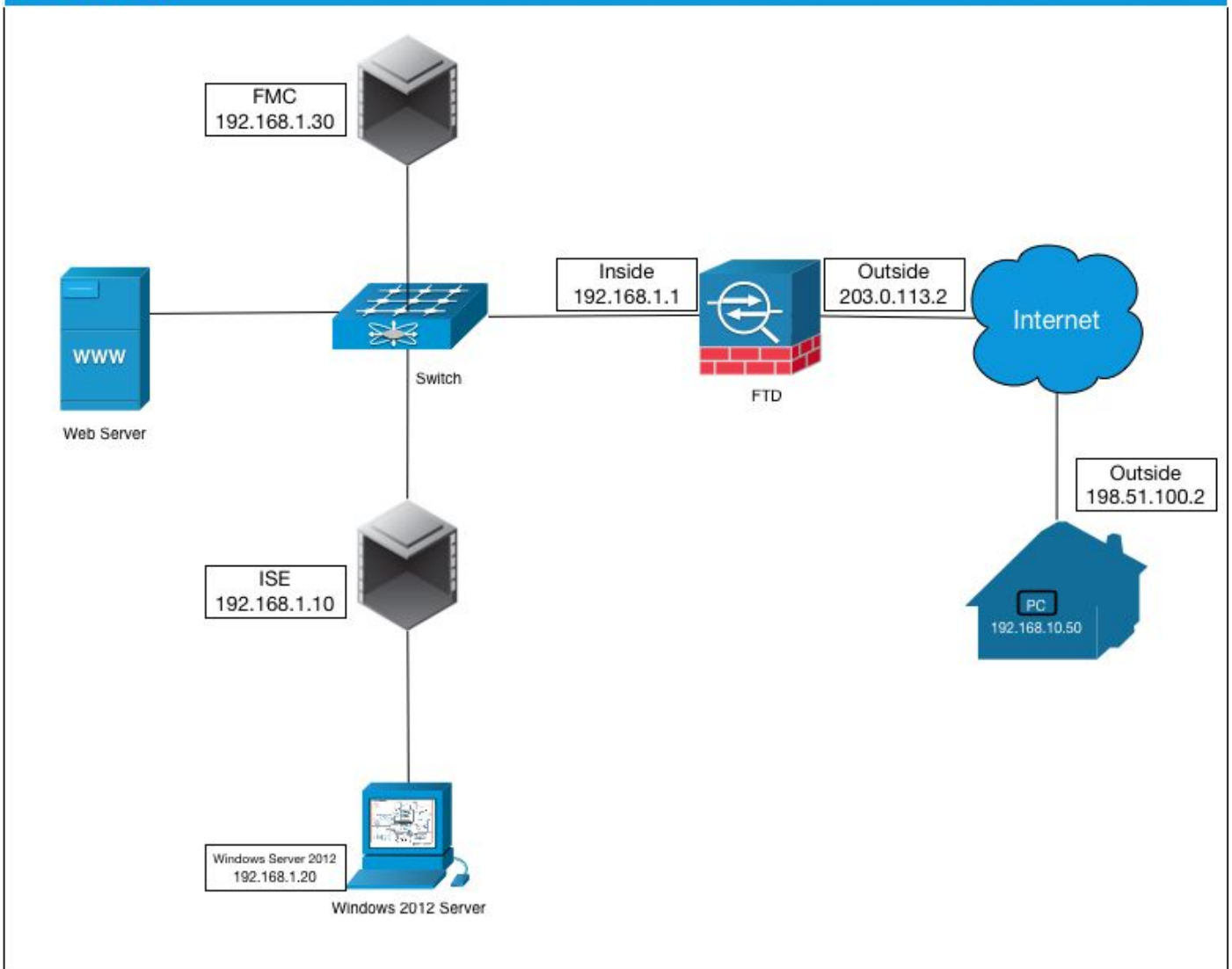
De informatie in dit document is gebaseerd op deze softwareversies:

- Firepower Management Center en Firepower Threat Defense, actief 6.2.3
- Cisco Identity Services Engine 2.4
- Cisco AnyConnect beveiligde mobiliteit-client met 4.6.030-49
- Windows Server 2012 R2 actieve Directory- en certificaatservices (dit is onze Root CA voor alle certificaten)
- Windows 7, Windows 10, Mac PC's

## Configureren

### Netwerkdigram

## Topology



In dit gebruiksgeslacht zal de Windows/Mac PC van de medewerker die de Any Connect VPN-client runt, verbinding maken met het externe openbare IP-adres van de FTD-firewall en Cisco ISE zal dynamisch beperkte of volledige toegang tot bepaalde interne of internetbronnen (configureerbaar) geven zodra ze via VPN zijn verbonden, afhankelijk van welke AD-groep ze lid zijn van de Active Directory

Apparaat	Hostname/FQDN	IP-adres:	Private IP-adres	AnyConnect IP-adres
Windows PC	-	198.51.100.2	10.0.0.1	192.168.10.50
FTD	ciscofp3.cisco.com	203.0.113.2	192.168.1.1	-
FMC	-	-	192.168.1.30	-
Cisco ISE	ciscoise.cisco.com	-	192.168.1.10	-
Windows Server 2012	ciscodc.cisco.com	-	192.168.1.20	-
Interne servers	-	-	192.168.1.x	-

## Configuratie

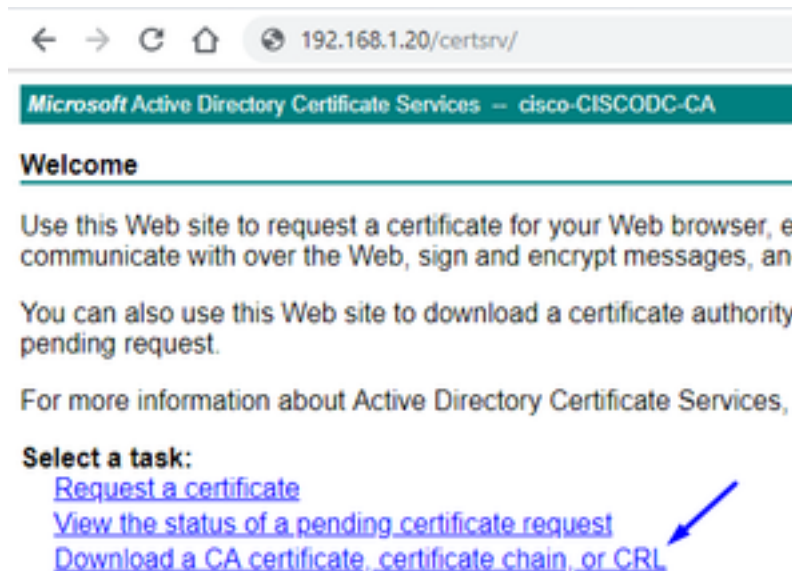
### Start CA-certificaat vanuit Windows Server uit

In dit document gebruiken we Microsoft Windows Server 2012 als onze Root CA voor certificaten. De client-pc's vertrouwen op deze Root CA om veilig via VPN aan de FTD te verbinden (zie onderstaande stappen). Hierdoor wordt gewaarborgd dat zij via het internet een veilige verbinding

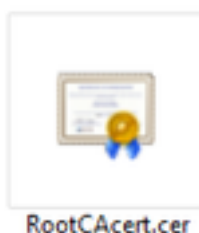
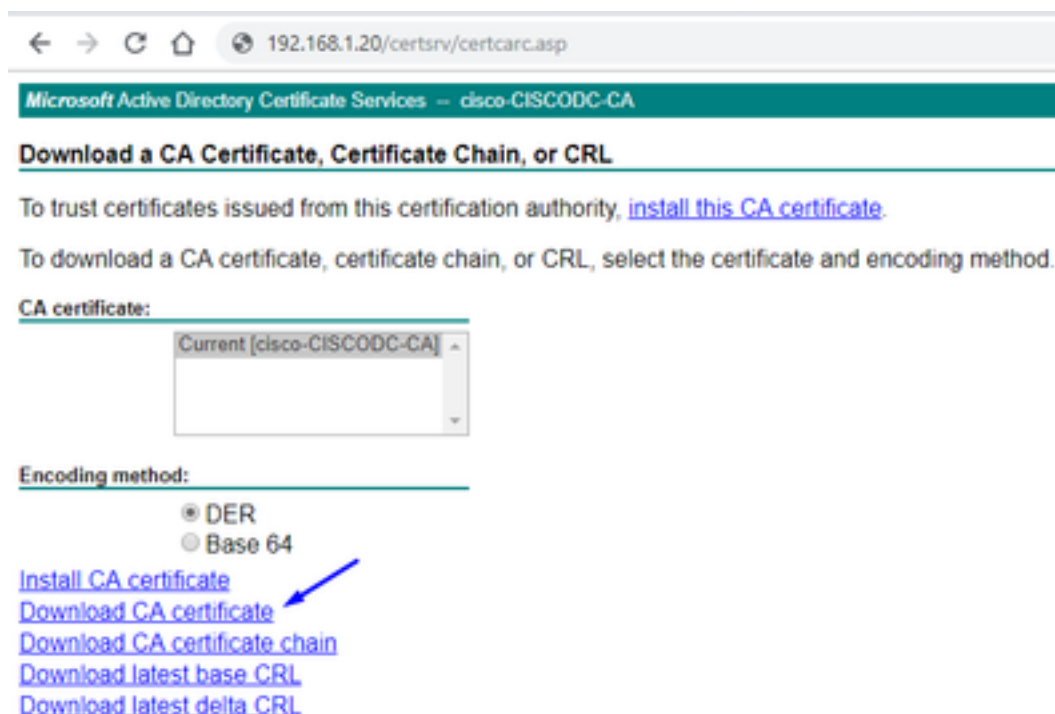
met de FTD kunnen maken en dat zij van thuis gebruik kunnen maken van interne middelen. Hun PC zal de verbinding in hun browser en AnyConnect Client vertrouwen.

Ga naar <http://192.168.1.20/certsrv> en volg de onderstaande stappen om uw Windows Server Root CA-certificaat te downloaden:

Klik op **CA-certificaat, certificeringsketen of CRL downloaden**



Klik op **Downloadcertificaat** en hernoem het naar 'RootCAcert3.cer'



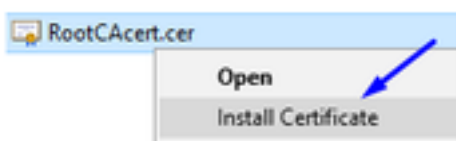
## Installeer het Root CA-certificaat op de Windows/Mac-pc's van de medewerker

**Methode 1:** Installeer het certificaat op alle PC's van de werknemer door het via het beleid van de Groep van de Server van Windows te drukken (ideaal voor om het even wat meer dan 10 VPN gebruikers):

[Hoe Windows Server te gebruiken om certificaten aan clientcomputers te distribueren met behulp van groepsbeleid](#)

**Methode 2:** Installeer het certificaat op alle PC's van de werknemer door het op elke PC afzonderlijk te installeren (ideaal om een VPN-gebruiker te testen):

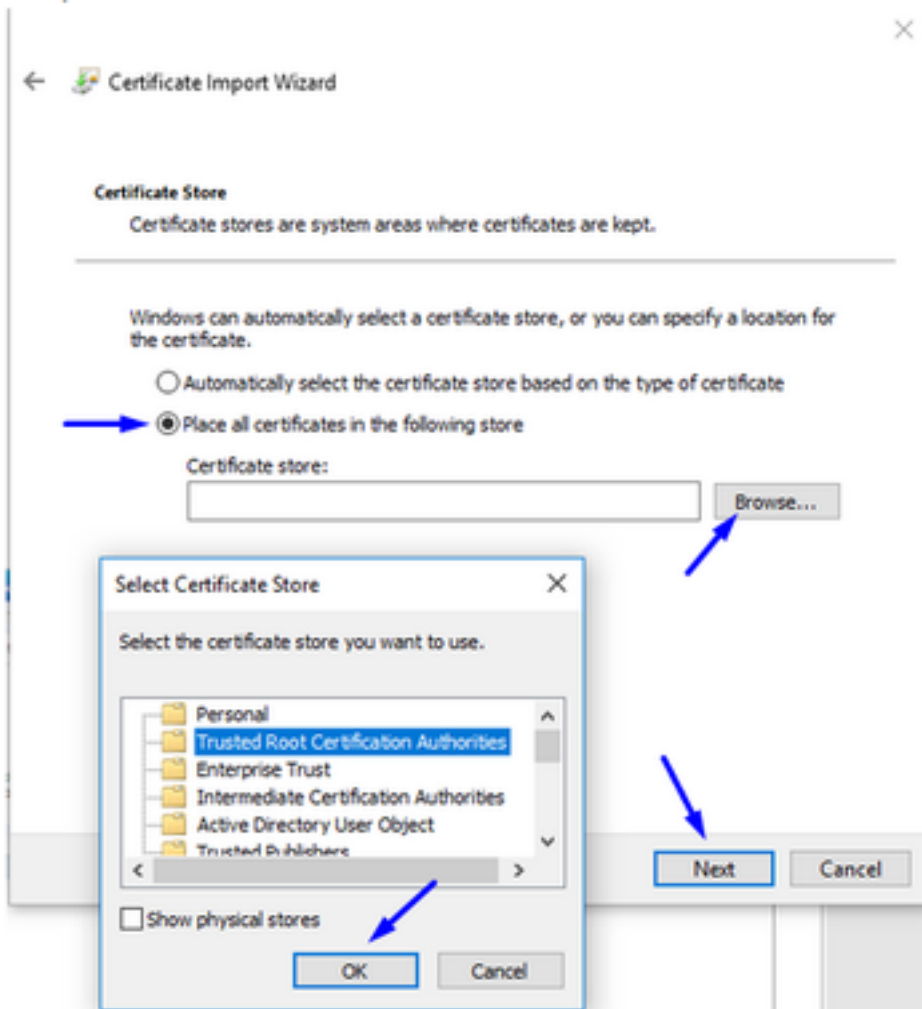
Klik met de rechtermuisknop op het certificaat op de Windows/Mac-pc van uw werknemers en klik op **Install Certificate**



Selecteer 'Huidige gebruiker'

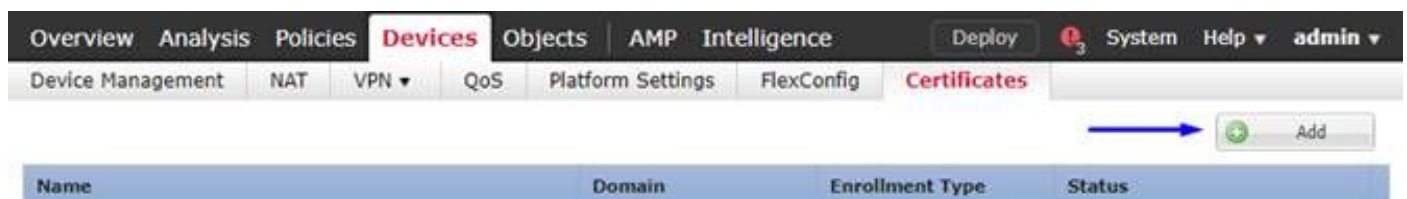


Selecteer **Plaats alle certificaten in de volgende winkel** en selecteer **Trusted Root Certified-certificeringsinstanties**, klik op **OK**, klik op **Volgende** en klik op **Voltoeien**



Genereert een CSR op FTD, laat CSR ondertekend door Windows Server Root CA en installeer dat ondertekende certificaat op FTD

Ga naar Objecten > Objectbeheer > PKI > Certinschrijving, klik op Add Cert Enrollment



Klik op de knop Toegang toevoegen

**Add New Certificate** ? X

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

Device\*: ciscofp3

Cert Enrollment\*: |

Add Cancel

Selecteer **Type inschrijving > Handmatig**

Zoals hieronder in de afbeelding wordt getoond, moeten we hier ons Root CA-certificaat plakken:

**Add Cert Enrollment** ? X

Name\*: FTDVPIIServerCert

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Certificate\*: Paste certificate here

Paste the Root CA Certificate in Base-64 text format here (we will do this in the step below)

Allow Overrides:

Save Cancel

Hier kunt u uw CA-certificaat downloaden, dit in tekstindeling bekijken en in het bovenstaande vak plakken:

Ga naar <http://192.168.1.20/certsrv>

Klik op **CA-certificaat, certificeringsketen of CRL downloaden**

← → ↻ 🏠 192.168.1.20/certsrv/

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

## Welcome

Use this Web site to request a certificate for your Web browser, e communicate with over the Web, sign and encrypt messages, an

You can also use this Web site to download a certificate authority pending request.

For more information about Active Directory Certificate Services,

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Klik op **Base 64-toets** > Klik op **Download CA**

← → ↻ 🏠 192.168.1.20/certsrv/certcarc.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

## Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.


CA certificate:

Current [cisco-CISCODC-CA]

Encoding method:

- DER
- Base 64

- [Install CA certificate](#)
- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)



RootCAcertBase64.cer

Open het bestand RootCAcertBase64.cer in Kladblok

Kopieer en plak de .cer inhoud (Root CA certificaat) van Windows AD Server hier:



## Add Cert Enrollment



Name: \*

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: \*

```
QgizA0KCRWEA88INZPIHQWCWTDVK0PBRQD8JGDMR6GR10UEW
EB/wQFMAMBAf8wHQYD
VR00BBYEF0lpC7y9musCkmDJaKVus9bJUoMIMBAGCSsGAQQBg
jcVAQQDAgEBMCMG
CSsGAQQBgjcVAgQWBBQXIqPq2/dCT41fyYZHPxKhGEYNnzANBg
kqhkiG9w0BAQsF
AAOCAQEAOTa5S8Zw7RfarjTGm7HHJHZsA2p9CHdsvB/I35nYeqc
OnxyeTWFN7by6
C43uyBFTWtpU3LlJr1mCgEo72qJErJOoU/Y4y7ADAKJF8RtUIb4H
Zq13XNW7Tu9X
DbZCTeYL7INbzZxPyfcuZWIBk5I8uHRvqq2YkBdx6YUYJocNTshH
WwZIXYvQPwwc
yjHrFjm0/YIQIJMhyIVULXXxWGP7diLIEQ67aHsdz+UZq9JofvYa
heHBjzbzIF
zvN2WWFXQs3mFMUxkrjEyzNlDws6vrm6ZhqvOupzmeC6YqByK
QIEAggjevemL7Zd
8DufTZQ4E4VQ9Kp4hrSdzuHSggDTuw==
-----END CERTIFICATE-----
```

Allow Overrides:

Klik op tabblad **certificaatparameters** >> type informatie over het certificaat

Opmerking:

Aangepast FQDN-veld moet de FQDN van uw FTD zijn

Het veld Gemeenschappelijke naam moet de FQDN van uw FTD zijn

## Add Cert Enrollment



Name:\*

Description:

CA Information Certificate Parameters Key Revocation

Include FQDN:

Custom 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:

Save Cancel

Tip: U kunt de FQDN van uw FTD krijgen door de volgende opdracht van de FTD CLI te typen:

```
> show network
===== [ System Information ] =====
Hostname : ciscofp3.cisco.com
Domains : cisco
DNS Servers : 192.168.1.20
Management port : 8305
IPv4 Default route
Gateway : 192.168.1.1

===== [ br1 ] =====
State : Enabled
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 00:0C:29:4F:AC:71
----- [ IPv4 ] -----
Configuration : Manual
Address : 192.168.1.2
Netmask : 255.255.255.0
```

Klik op het tabblad **Key** en type een **sleutelnaam**

**Add Cert Enrollment** ? X

Name: \*

Description:

CA Information Certificate Parameters **Key** Revocation

Key Type:  RSA  ECDSA

Key Name: \*

Key Size:

**Advanced Settings**

Ignore IPsec Key Usage  
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides:

Save Cancel

Klik op **Opslaan**

Selecteer uw FTNServerCert die we net boven gemaakt hebben en klik op **Toevoegen**

**Add New Certificate** ? X

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

Device\*:

Cert Enrollment\*:

**Cert Enrollment Details:**

Name: FTDVPNServerCert

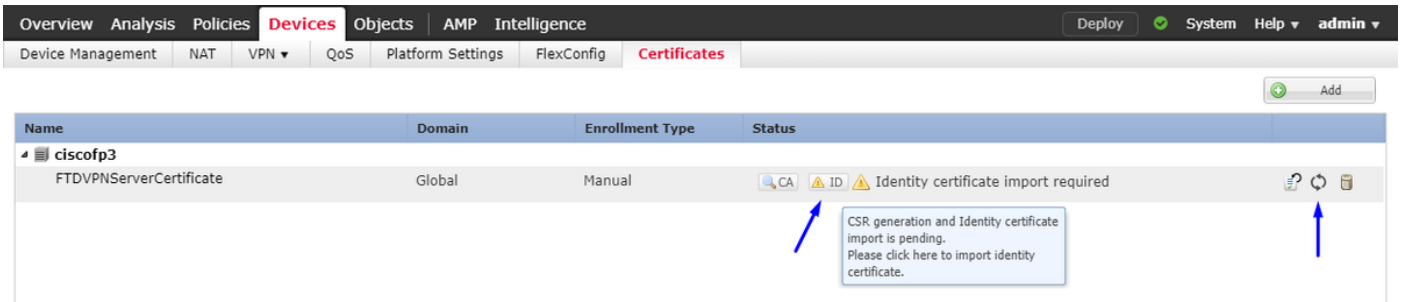
Enrollment Type: Manual

SCEP URL: NA

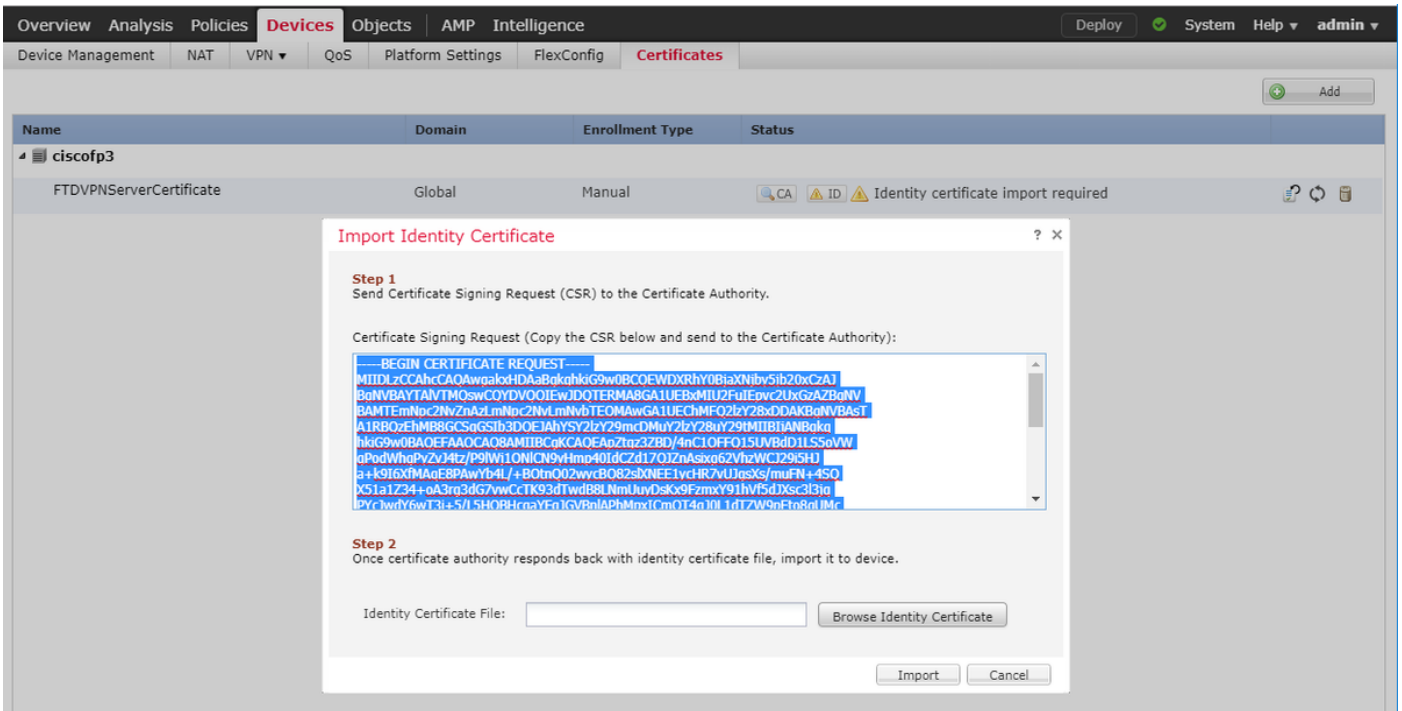
Add Cancel

Tip: Wacht ongeveer 10-30 seconden voor de FMC + FTD om het certificaat Root CA te controleren en te installeren (klik op het pictogram Vernieuwen als dit niet wordt weergegeven)

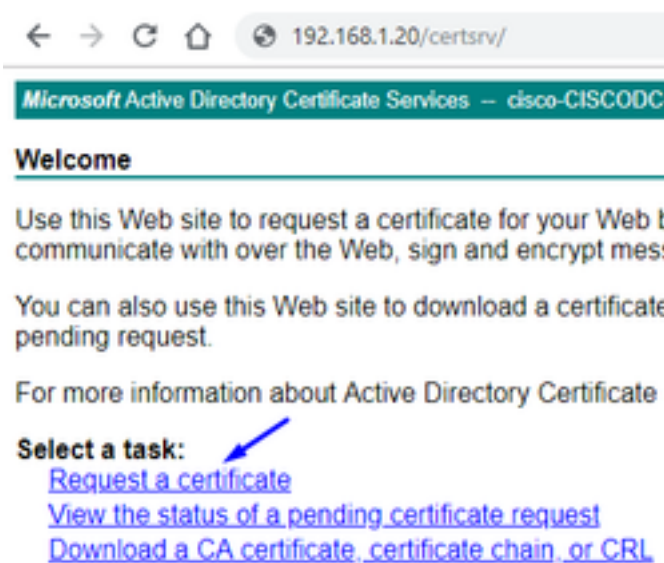
Klik op de knop ID:



Kopieer en plak deze CSR en breng het naar uw Windows Server Root CA:



Ga naar <http://192.168.1.20/certsrv>



Klik op geavanceerde certificaataanvraag

← → ↻ 🏠 192.168.1.20/certsrv/certrqus.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

### Request a Certificate

Select the certificate type:  
[User Certificate](#)

Or, submit an [advanced certificate request](#).

Plakt uw CSR-aanvraag (certificaataanvraag) in het onderstaande veld en selecteer **Webserver** als de certificaatsjabloon

← → ↻ 🏠 192.168.1.20/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
DbZCTeYL71NbZxPvfCuZWl8k5l8uHRvqq2Yk8.
yiHrFim0/YlIQIjImhyIVULXXxwGP7dillEQ67.
zvN2wMFXQs3mFMUxkrjEyzNlDws6vrm6Zhaiv0
8DuFTZQ4E4VQ9Kp4hrSdzuh5ggDTuw==
-----END CERTIFICATE-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >


Klik op **Inzenden**

Klik op **Base 64 Encoded** knop en klik op **Download certificaat**

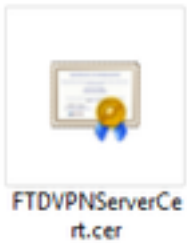
### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)



Klik op **Bladeren identiteitsbewijs** en selecteer het certificaat dat we zojuist hebben gedownload

**Import Identity Certificate**

**Step 1**  
Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDLzCCAhcCAQAwgAkxHDAaBkqhkiG9w0BCEQWDXRhy0BjaXNjbv5ib20xCzAJ  
BgNVBAYTAiVTMQswCQYDQ0EwJ0QTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNV  
BAMTEmNpY2NpZmNpY2NpY2NpY2NpY2NpY2NpY2NpY2NpY2NpY2NpY2NpY2Np  
A1RBOzEhMB8GCSaGSIb3DQEJAhYSY2lyZ29mcDMuY2lyZ28uY29tMTIiBjANBgkq  
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApz3ZBD/4nClOFFO15UVBd1LS5oVW  
gPodWhgPvZv4tz/P9lW10NICN9vHmp40idCZd17OJZnAsix62VhzWCJ29i5HJ  
a+k9i6xfMaqE8PAwYb4L/+BOTnQ02wvcBQ82sIXNEE1vcHR7vUJgsXs/muFN+4SQ  
XS1a1234+ga3rg3dG7wvCctK93dTwdB8LNMUuvOsk9FzmxY91hvF5d2Xsc3l3iq  
Pyc1wdY6wT3i+5/l5HOBHcnaYFn1GVbnlAphMnx1CmOT4n10L1d7W9nFto8nlIMc
```

**Step 2**  
Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

FTD VPN Server Certificate (ondertekend door Windows Server Root CA) is geïnstalleerd.

Name	Domain	Enrollment Type	Status
FTDVPNServerCertificate	Global	Manual	

ImageConnect + AnyConnect Profile Editor downloaden en een .xml-profiel maken

[Cisco AnyConnect Profile Editor](#) downloaden en installeren

Profile Editor (Windows)  
tools-anyconnect-win-4.6.03049-profileeditor-k9.msi  
20-SEP-2018 7.74 MB

Profiel editor van AnyConnect openen

Klik op **Server List** > Klik op **Add...**

Typ een **Display Name** en de **FQDN** van de externe interface-IP van uw FTD. U dient items in de serverlijst te zien



AnyConnect Profile Editor - VPN

File Help

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 List	SCEP	Mobile Settings	Certificate Pins

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

Add... Delete  
Edit... Details

### Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required)

FQDN or IP Address  / User Group

Group URL

Connection Information

Primary Protocol

ASA gateway

Auth Method During IKE Negotiation

IKE Identity (IOS gateway only)

Backup Servers

Host Address	Action
<input type="text"/>	Add
	Move Up
	Move Down
	Delete

OK Cancel

AnyConnect Profile Editor - VPN

File Help

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 List	SCEP	Mobile Settings	Certificate Pins
discofp3.cisco.com	discofp3.cisco.com		-- Inherited --			

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

Add... Delete  
Edit... Details

Klik op OK en Bestand > Opslaan als...

VPNprofile.xml

Download [hier](#) Windows- en Mac.pkg-afbeeldingen

AnyConnect Headend Deployment Package (Windows) 	20-SEP-2018	41.34 MB
anyconnect-win-4.6.03049-webdeploy-k9.pkg		
AnyConnect Headend Deployment Package (Mac OS) 	20-SEP-2018	41.13 MB
anyconnect-macos-4.6.03049-webdeploy-k9.pkg		

Ga naar **objecten > Objectbeheer > VPN > AnyConnect-bestand > klik op AnyConnect-bestand toevoegen**

**Edit AnyConnect File** ? x

Name:*	<input type="text" value="AnyConnect_Windows_4.6.03049"/>
File Name:*	<input type="text" value="anyconnect-win-4.6.03049-webdeploy-k9.pk"/> <input type="button" value="Browse.."/>
File Type:*	<input type="text" value="AnyConnect Client Image"/> ▾
Description:	<input type="text" value="Cisco AnyConnect Image for Windows PCs"/>

**Add AnyConnect File** ? x

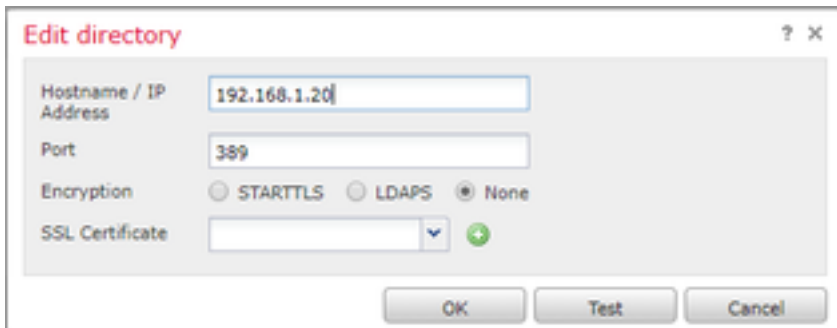
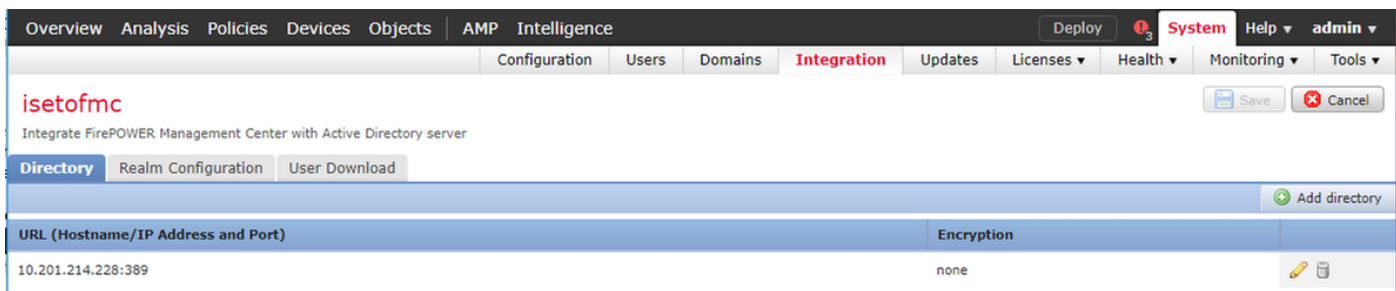
Name:*	<input type="text" value="AnyConnect_Mac_4.6.03049"/>
File Name:*	<input type="text" value="anyconnect-macos-4.6.03049-webdeploy-k9"/> <input type="button" value="Browse.."/>
File Type:*	<input type="text" value="AnyConnect Client Image"/> ▾
Description:	<input type="text" value="Cisco &lt;del&gt;AnyConnect&lt;/del&gt; Image for Mac PCs"/>

**AnyConnect VPN op FTD configureren (gebruik het Root CA-certificaat)**

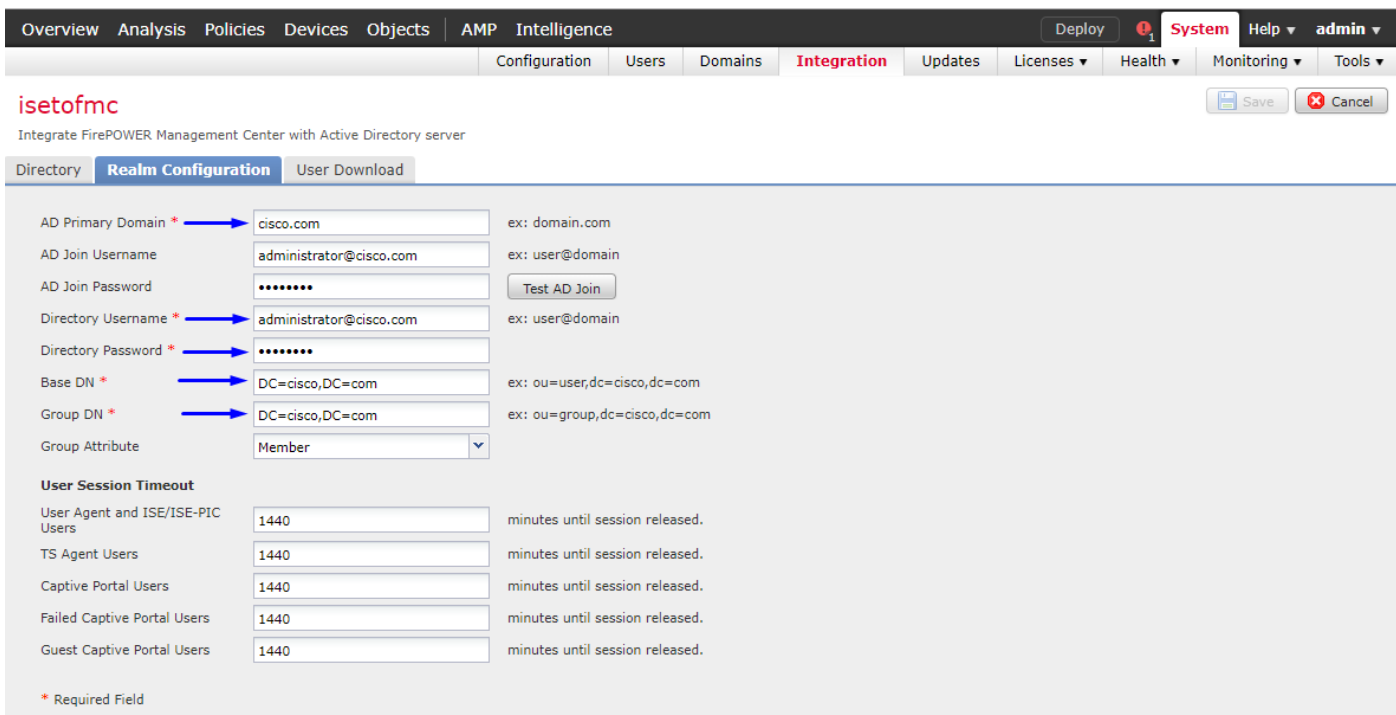
Aanmelden bij het **FirePOWER Management Center**

Klik op **Systeem > Integratie > Realms > Klik op Nieuw venster > klik Map > klik op Map toevoegen > Klik op Map toevoegen**





Klik op het tabblad Configuratie **Realm** - configureer hier de informatie van uw domeincontroller



Opmerking: In het bovenstaande voorbeeld wordt een AD-gebruikersnaam met 'Domain Admin'-rechten in de Windows AD-server gebruikt. Als u een gebruiker wilt configureren met specifiekere, minimale bevoegdheden voor het FMC om zich bij uw Active Directory Domain aan te sluiten voor uw configuratie van het programma, kunt u de stappen [hier](#) zien

Klik op het tabblad **User Download** - zorgt ervoor dat User Download slaagt

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

isetofmc  
Integrate FirePOWER Management Center with Active Directory server

Directory Realm Configuration **User Download**

Download users and groups  
Begin automatic download at 8 PM America/New York Repeat Every 24 Hours  
Download Now

Available Groups

- Enterprise Admins
- Hyper-V Administrators
- Group Policy Creator Owners
- Guri-group2
- Cloneable Domain Controllers
- Distributed COM Users
- Allowed RODC Password Replication Group
- Cryptographic Operators
- Server Operators
- Remote Desktop Users
- WinRMRemoteWMIUsers\_
- Users
- Administrators
- Windows Authorization Access Group
- Enterprise Read-only Domain Controllers
- Domain Admins
- Domain Users
- Pre-Windows 2000 Compatible Access
- Cert Publishers

Groups to Include (0) Groups to Exclude (0)

LDAP Download  
Download users/groups from isetofmc  
LDAP download successful: 51 groups, 25 users download

Klik op Apparaten > VPN > Externe toegang > klik op Add

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

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

Add

Name	Status	Last Modified
No configuration available <a href="#">Add a new configuration</a>		

Typ een naam, beschrijving en klik op Add om het FTD-apparaat te selecteren dat u AnyConnect VPN wilt configureren op

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

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: FTDAnyConnectVPN  
Description: AnyConnect VPN configuration for this FTD

VPN Protocols:  SSL  IPsec-IKEv2

Targeted Devices: Available Devices Selected Devices

10.201.214.134

Add

**Before You Start**  
Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

**Authentication Server**  
Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

**AnyConnect Client Package**  
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

**Device Interface**  
Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

Klik op Add voor de verificatieserver en kies RADIUS-servergroep - dit is uw Cisco Identity

## Services Engine PSN (Policy Services Node)

The screenshot shows the 'Remote Access VPN Policy Wizard' in the Cisco ISE GUI. The wizard is on the 'Access & Certificate' step. A diagram at the top illustrates the network flow: Remote User -> AnyConnect Client -> Internet -> VPN Device (Outside/Inside) -> Corporate Resources. Below the diagram, the 'Connection Profile' section is configured with 'FTDAnyConnectVPN' as the name. The 'Authentication, Authorization & Accounting (AAA)' section is set to 'AAA Only' with 'Use same authentication server' selected. A blue arrow points to the 'Realms or RADIUS' dropdown menu, which is currently set to 'Realms'. The 'Client Address Assignment' section has 'Use IP Address Pools' checked. The 'Group Policy' is set to 'DfltGrpPolicy'.

Typ een **naam** voor de RADIUS-server  
Selecteer het hierboven ingestelde antwoord  
Klik op **Toevoegen**

### Add RADIUS Server Group

The 'Add RADIUS Server Group' dialog box is shown with the following configuration:

- Name: CiscoISE
- Description: Cisco ISE (Joined to Windows AD Server)
- Group Accounting Mode: Single
- Retry Interval: 10 (1-10) Seconds
- Realms: isetofmc
- Enable authorize only
- Enable interim account update  
Interval: 24 (1-120) hours
- Enable dynamic authorization  
Port: 1700 (1024-65535)

Below the configuration fields, there is a section for 'RADIUS Servers (Maximum 16 servers)'. A blue arrow points to a green plus icon (+) used to add a new server. The table below is currently empty, displaying 'No records to display'.

IP Address/Hostname
No records to display

Typ de volgende informatie voor uw Cisco ISE-knooppunt:  
**IP-adres/hostnaam:** IP-adres van Cisco ISE PSN (Policy Service Node) - dit is waar

verificatieverzoeken worden gedaan

Sleutel: Cisco 123

**Bevestig sleutel:** Cisco 123

**Voorzichtig:** Het bovenstaande is uw RADIUS gedeelde geheime toets - we zullen deze toets in een latere stap gebruiken

**Edit RADIUS Server** ? X

IP Address/Hostname:\*   
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:\*  (1-65535)

Key:\*

Confirm Key:\*

Accounting Port:  (1-65535)

Timeout:  (1-300) Seconds

Connect using:  Routing  Specific Interface ⓘ

Redirect ACL:

Opmerking: Wanneer de eindgebruiker probeert via AnyConnect VPN verbinding te maken met de FTD, wordt de gebruikersnaam + wachtwoord die hij typt, verzonden als een verificatieaanvraag bij deze FTD. De FTD zal dat verzoek naar het Cisco ISE PSN-knooppunt voor verificatie doorsturen (Cisco ISE zal dan Windows Active Directory voor die gebruikersnaam en wachtwoord controleren en toegangscontrole/netwerktoegang afdwingen, afhankelijk van de voorwaarde die we momenteel in Cisco ISE hebben ingesteld)

## Add RADIUS Server Group

Name: CiscoISE

Description: Cisco ISE (joined to Windows AD server)

Group Accounting Mode: Single

Retry Interval: 10 (1-10) Seconds

Realms: isetofmd

Enable authorize only

Enable interim account update

Interval: 24 (1-120) hours

Enable dynamic authorization

Port: 1700 (1024-65535)

**RADIUS Servers** (Maximum 16 servers)

IP Address/Hostname
192.168.1.10

Save Cancel

Klik op Opslaan  
Klik op Bewerken voor IPv4-adresgroep

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN Remote Access QoS Platform Settings FlexConfig Certificates

Deploy System Help admin

### Remote Access VPN Policy Wizard

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

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

Connection Profile Name: FTDAAnyConnectVPN  
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: AAA Only

Authentication Server: CiscoISE (Realm or RADIUS)

Authorization Server: Use same authentication 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: [Edit]

IPv6 Address Pools: [Edit]

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

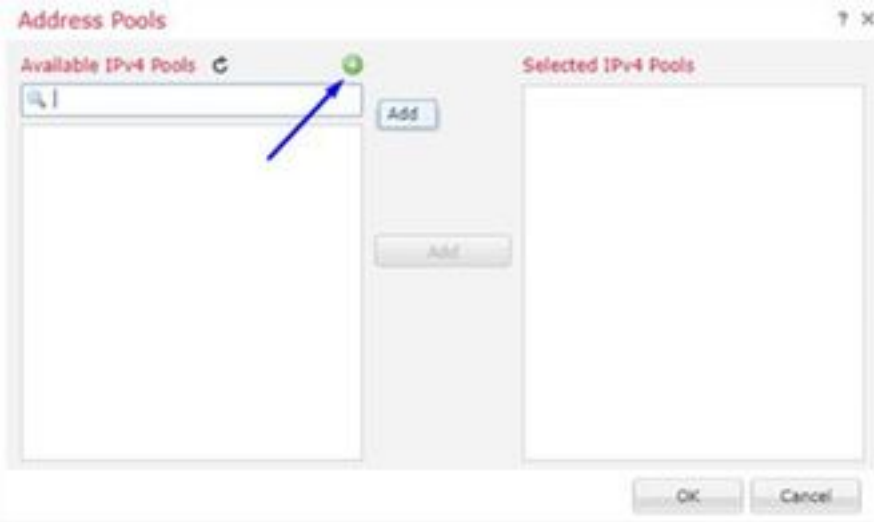
Group Policy: DfGpPolicy (Edit Group Policy)

Back Next Cancel

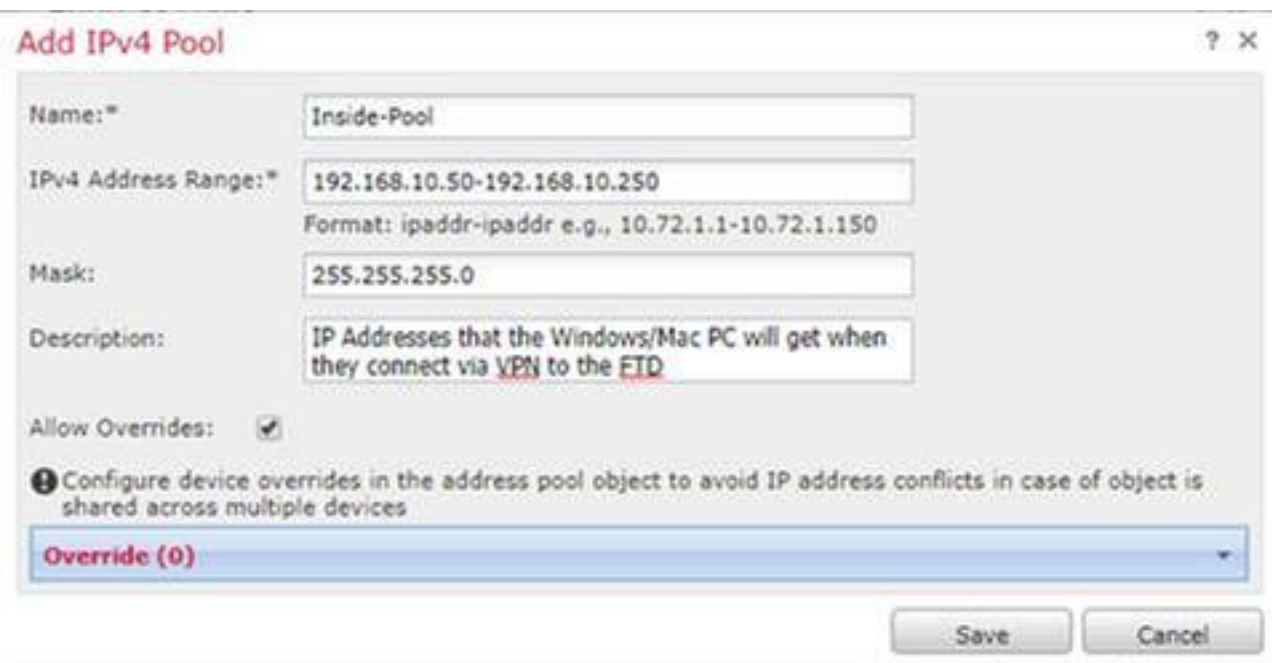
Last login on Wednesday, 2018-10-10 at 10:30:14 AM from 10.152.21.157

How-To Cisco

Klik op Toevoegen

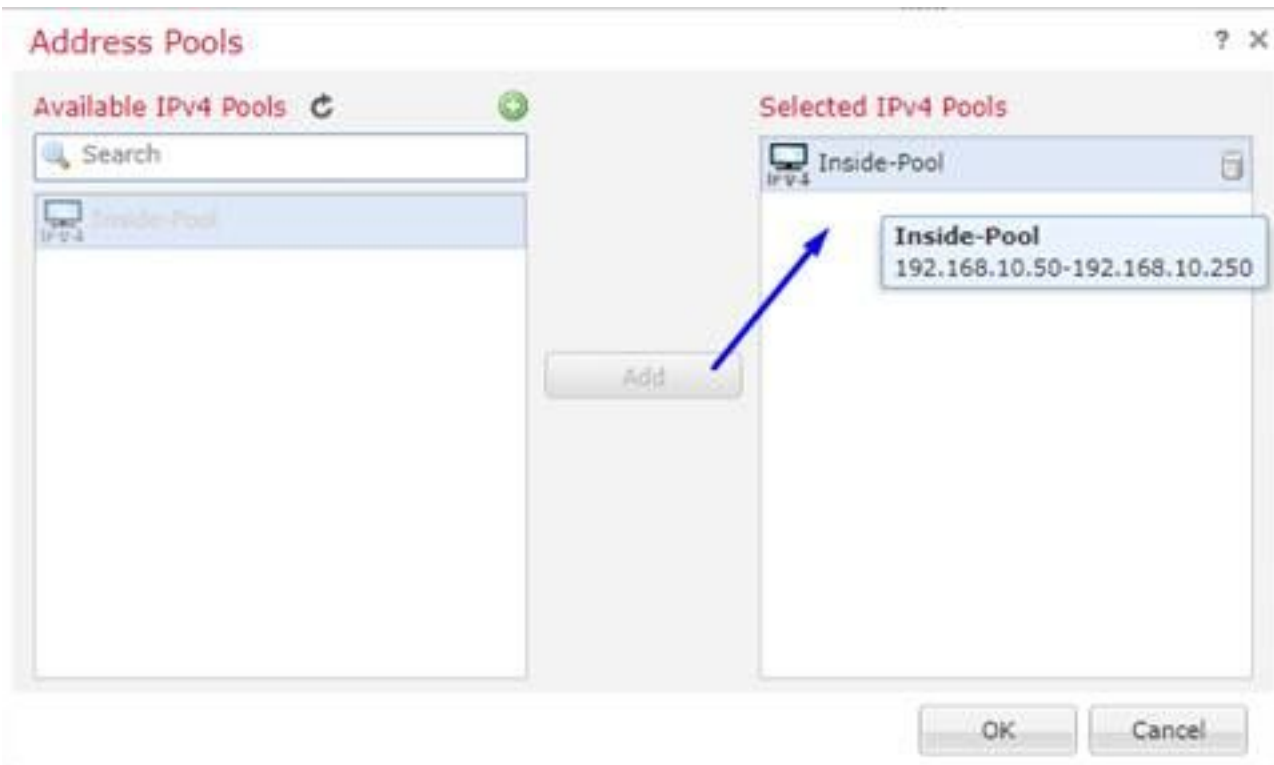


Typ een naam, IPv4-adresbereik en subnetmasker

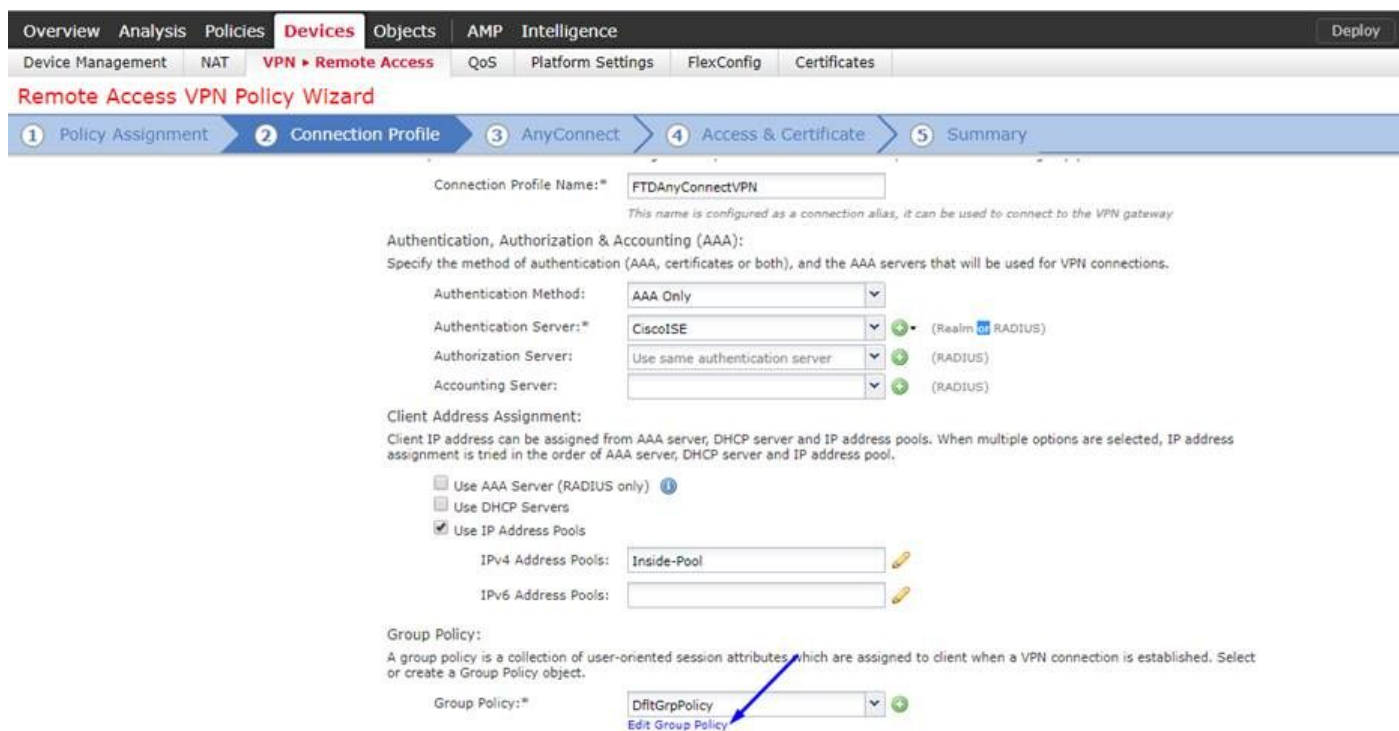


Selecteer uw IP-adresgroep en klik op OK





Klik op groepsbeleid bewerken



Klik op AnyConnect tabblad > profielen > klik op Add

## Edit Group Policy

? X

Name:\* DfitGrpPolicy

Description:

General **AnyConnect** Advanced

Profiles

SSL Settings

Connection Settings

AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Client Profile:

Standalone profile editor can be used to create a new or modify existing Anyconnect profile. You can download the profile editor from Cisco Software Download Center.

Typ een naam en klik op **Bladeren..** en selecteer het bestand VPNProfile.xml in stap 4 hierboven

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

Edit Group Policy

Name:\* DfitGrpPolicy

Description:

General **AnyConnect** Advanced

Profiles

SSL Settings

Connection Settings

AnyConnect XML Profile

Name:\* AnyConnect\_XML\_Profile

File Name:\* VPNprofile.xml

File Type:\* AnyConnect Client Profile

Description:\* XML profile we created using Profile Editor earlier

Save Cancel

Save Cancel

Back Next Cancel

Klik op **Opslaan** en klik op **Volgende**

Selecteer vanuit stap 4 hierboven de selectiekaarten voor uw AnyConnect Windows/Mac-bestand



Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

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

**AnyConnect Client Image**  
The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyConnect_Mac_4.6.03049	anyconnect-macos-4.6.03049-webdeploy-k9...	Mac OS
<input checked="" type="checkbox"/>	AnyConnect_Windows_4.6.03049	anyconnect-win-4.6.03049-webdeploy-k9.pkg	Windows

Back Next Cancel

Klik op **Volgende**

Selecteer **Interface Group/Security Zone** als buiten

Selecteer **certificaatschrijving** als uw certificaat dat we in stap 3 hierboven hebben gemaakt

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

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

**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 Cancel

Bekijk uw configuratie en klik op **Volgende**

**Remote Access VPN Policy Configuration**

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: FTDAnyConnectVPN

Device Targets: 10.201.214.134

Connection Profile: FTDAnyConnectVPN

Connection Alias: FTDAnyConnectVPN

AAA:

- Authentication Method: AAA Only
- Authentication Server: CiscoISE
- Authorization Server: CiscoISE
- Accounting Server: CiscoISE

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): Inside-Pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images: AnyConnect\_Windows\_4.6.03049

Interface Objects: Outside

Device Certificates: FTDVPNServerCert

**Additional Configuration Requirements**

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**  
An *Access Control* rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**  
If NAT is enabled on the targeted devices, you must define a *NAT rule* to exempt VPN traffic.
- DNS Configuration**  
To resolve hostname specified in AAA Servers or ICA Servers, configure DNS using *FlexConfig Policy* on the targeted devices.
- Network Interface Configuration**  
Make sure to add interface from targeted devices to SecurityZone object 'Outside'.

**Device Identity Certificate Enrollment**

Certificate enrollment object 'FTDVPNServerCert' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Configureer de FTD NAT-regel om het VPN-verkeer van NAT vrij te stellen omdat deze toch wordt gedecrypteerd en om toegangscontroleregels/toegangscontroleregels te maken

Maak een statische NAT-regel om er zeker van te zijn dat het VPN-verkeer geen NAT'd krijgt (FTD decrypteert de AnyConnect-pakketten wanneer ze naar de buiteninterface komen, dus het is alsof die PC al achter de interne interface zit en ze al een privé IP-adres hebben - we moeten nog een NAT-vrijstellingsregel (No-NAT) voor dat VPN-verkeer configureren:

Ga naar **objecten** > klik op **Netwerk toevoegen** > klik op **Objecten toevoegen**

**Edit Network Objects** ? X

Name: inside-subnet

Description:

Network: 192.168.1.0/24  
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

Save Cancel

### Edit Network Objects

Name:

Description:

Network:

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

Save Cancel

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Example\_Company\_NAT\_Policy

Rules

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet		Translated Packet		Options
					Original Sources	Original Destinations	Translated Sources	Translated Destinations	
▼ NAT Rules Before									
1		Static	Inside	Outside	inside-subnet	outside-subnet-anyconnect-pool	inside-subnet	outside-subnet-anyconnect-pool	Dns: false route-lookup no-proxy-arp
▼ Auto NAT Rules									
#		Dynamic	Inside	Outside	inside-subnet		Interface		Dns: false
▼ NAT Rules After									

Daarnaast moet u het gegevensverkeer toestaan om na de inloop van de gebruiker VPN te stromen. Hiervoor hebt u twee keuzes:

- Regels toestaan of ontkennen om VPN-gebruikers toe te staan of te ontkennen om toegang te krijgen tot bepaalde bronnen
- 'Bypass Access Control Policy voor gedecrypteerd verkeer' - dit maakt iedereen die met succes verbinding kan maken met de FTD via VPN toegang tot ACL's en maakt toegang tot alles achter de FTD zonder regels in toegangsbeleid toe te staan of te ontkennen

**Bypass Access Control Policy voor gedecrypteerd verkeer onder: Apparaten > VPN > Externe toegang > VPN-profiel > Toegangsinterfaces:**

#### Access Control for VPN Traffic

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

Opmerking: Als u deze optie niet uitschakelt, moet u naar **beleid > Toegangsbeleid** gaan en regels creëren voor VPN-gebruikers die toegang kunnen krijgen tot dingen achter of dmz

Klik op Instellen rechtsboven op FirePOWER Management Center

Voeg FTD toe als Netwerkapparaat en stel beleid in op Cisco ISE (gebruik RADIUS gedeeld geheim)

Aanmelden bij Cisco Identity Services Engine en klik op **Beheer > Netwerkapparaten > klik op Add**

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

### Network Devices

Name	Profile Name	Location	Type	Description
<input type="checkbox"/> ASAv2	Cisco	All Locations	Cisco Devices	asa lab
<input type="checkbox"/> CatalystSwitch	Cisco	All Locations	All Device Types	Catalyst 3850 Switch
<input type="checkbox"/> CiscoWLC	Cisco	All Locations	All Device Types	Cisco 3504 WLC
<input type="checkbox"/> CiscoWLC2	Cisco	All Locations	All Device Types	WLC at desk

Typ een naam, type het IP-adres van uw FTD en type uw RADIUS gedeelde geheim uit de bovenstaande stappen

Voorzichtig: Dit moet het interface/ip-adres zijn waarop de FTD uw Cisco ISE (RADIUS-server) kan bereiken, d.w.z. de FTD-interface die uw Cisco ISE via FTD kan bereiken

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

### Network Devices List > FTDVPN

#### Network Devices

\* Name

Description

IP Address \* IP:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

\* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

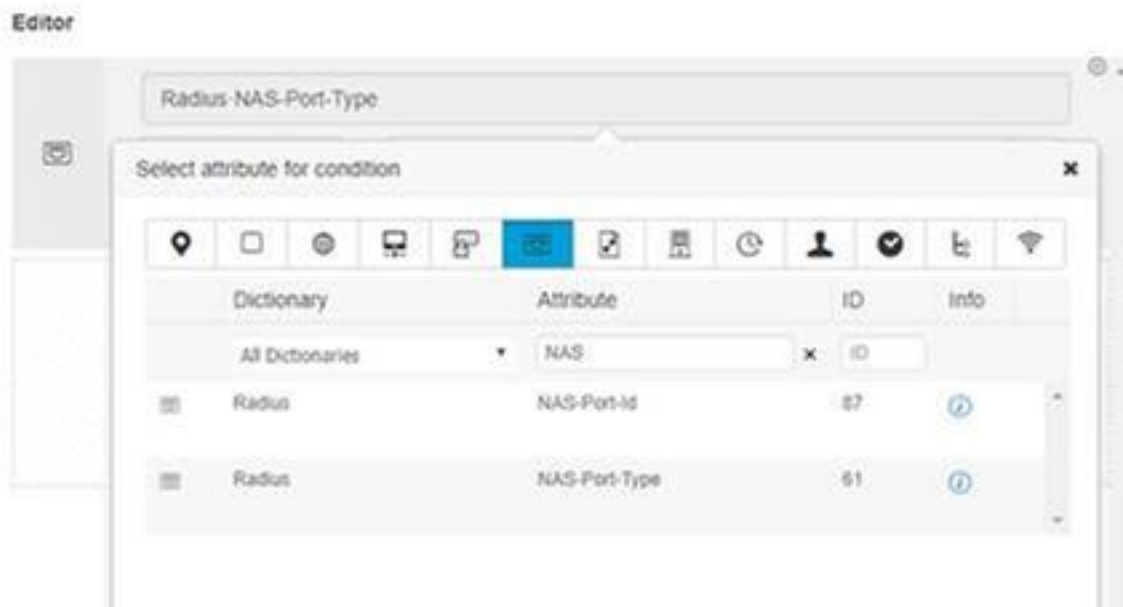
Klik op **Policy > Policy Set > creëren PolicySet** voor alle verificatieverzoeken van het volgende type:

### **RADIUS-NAS-poorts EQUALS virtueel**

Dit betekent dat als een RADIUS-aanvraag die in ISE komt en er op VPN-verbindingen uitziet, deze Policy Suite wordt ingedrukt

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	QuestSSID		Airspace Airspace-Wan-Id EQUALS 1	Default Network Access	181	+	⚙️ ▶️
✔	EmployeeSSID		Airspace Airspace-Wan-Id EQUALS 2	Default Network Access	606	+	⚙️ ▶️
✔	VPN Users		Radius NAS-Port-Type EQUALS Virtual	Default Network Access		+	⚙️ ▶️
✔	Default	Default policy set		Default Network Access	1360	+	⚙️ ▶️

Hier kunt u die voorwaarde in Cisco ISE vinden:



Bewerken van de hierboven gemaakte **beleidsset**

Voeg een regel boven de standaardblokregel toe om mensen het machtigingsprofiel van de "Toegang" te geven slechts als zij in de Actieve Groep van de Map "Werknemers" zijn:

Policy Sets → VPN Users

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	VPN Users		Radius NAS-Port-Type EQUALS Virtual	Default Network Access	52

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1X	Wireless_802.1X	All_User_ID_Stores	0	Options
✔	Default		All_User_ID_Stores	29	Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✔	Default		DenyAccess	Select from list	2	Options

Hieronder ziet uw wet er na voltooiing uit

Policy Sets → VPN Users

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	VPN Users		Radius NAS-Port-Type EQUALS Virtual	Default Network Access	88

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1X	Wireless_802.1X	All_User_ID_Stores	0	Options
✔	Default		All_User_ID_Stores	48	Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✔	Allow FTD VPN connections if AD Group VPNusers	ciscocd: ExternalGroups EQUALS cisco.com/Users/Employees	PermiAccess	Select from list	22	Options
✔	Default		DenyAccess	Select from list	2	Options

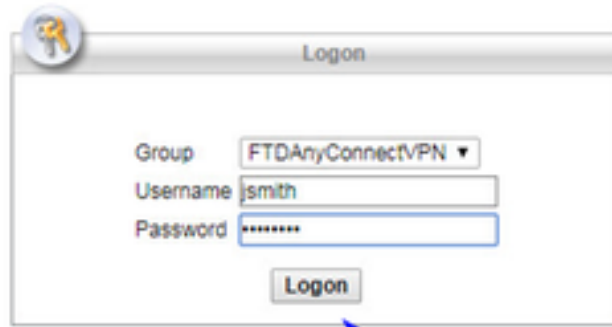
Downloaden, installeren en aansluiten op de FTD met AnyConnect VPN-client op Windows/Mac PC's van werknemers

Open uw browser op de Windows/Mac PC van de medewerker en ga naar het externe adres van uw FTD in uw browser

← → ↻ <https://cisconfp3.cisco.com>

Typ uw gebruikersnaam en wachtwoord voor de actieve map



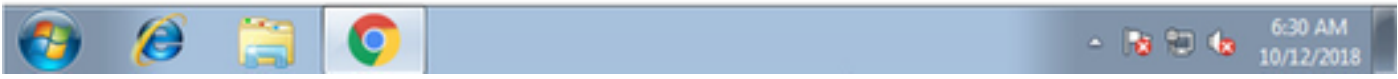


Logon

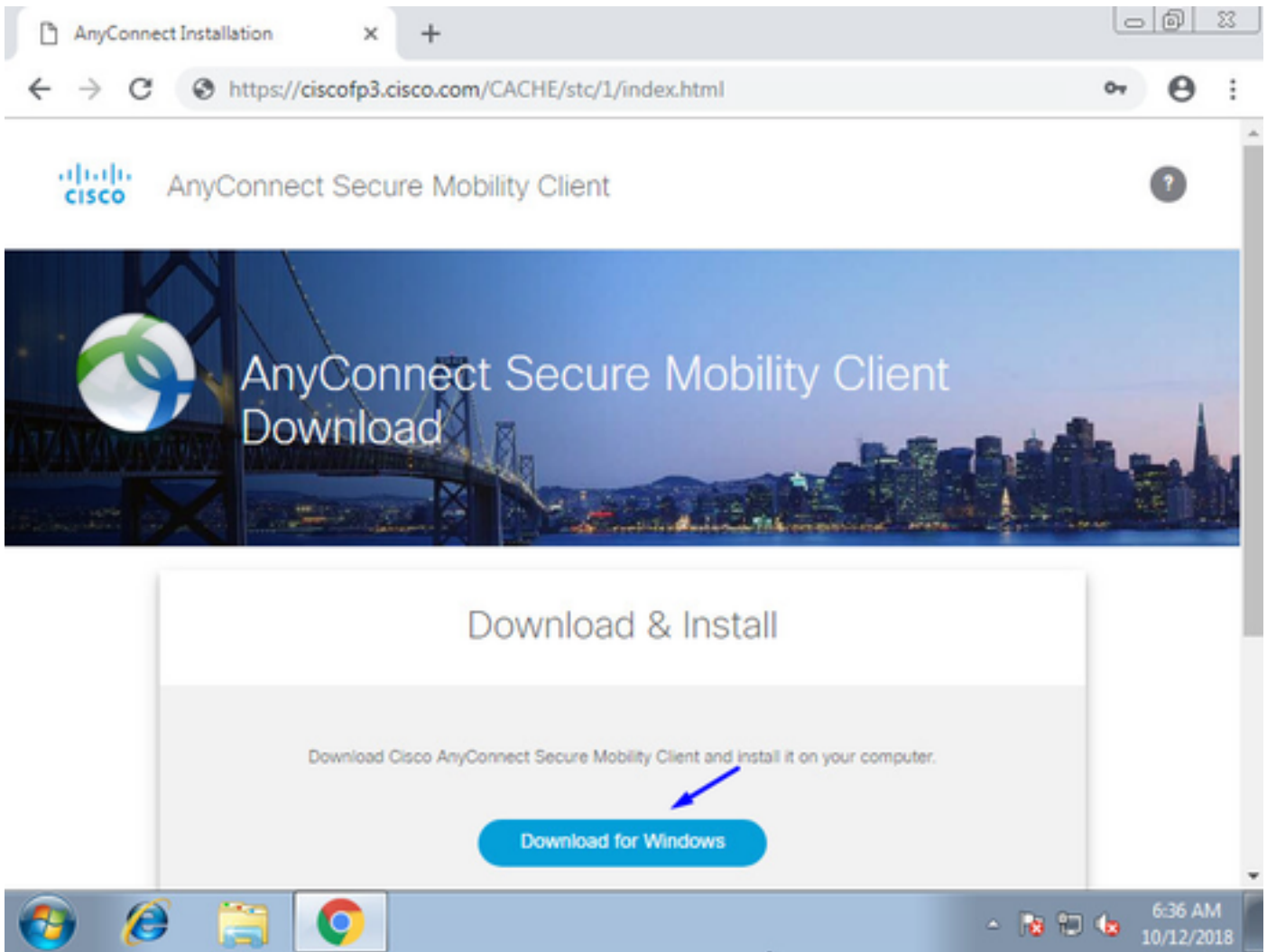
Group

Username

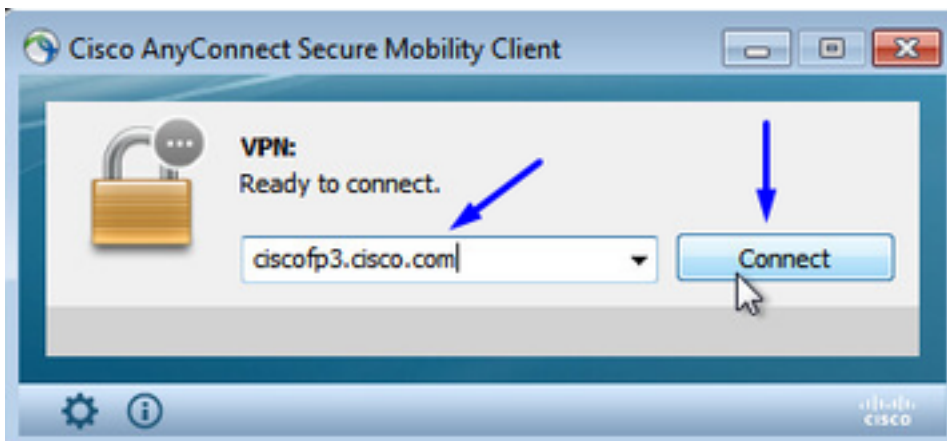
Password



Klik op **Download**



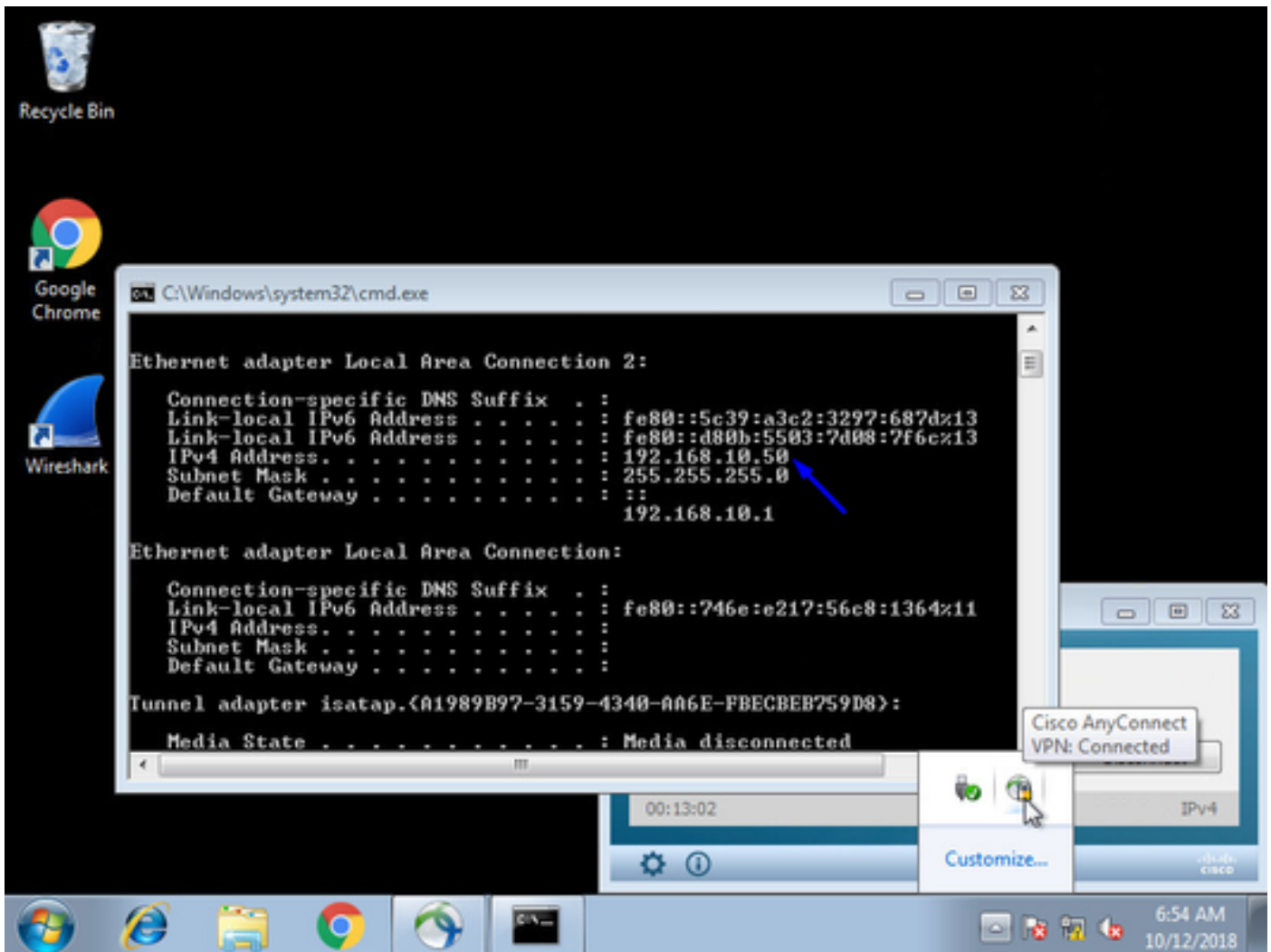
AnyConnect VPN Secure Mobility Client op Windows/Mac installeren en uitvoeren



Typ uw gebruikersnaam en wachtwoord voor de actieve map wanneer dit wordt gevraagd

U krijgt een IP-adres van de IP-adrespool die boven in stap 5 is gemaakt en een standaardgateway van de .1 in dat subprogramma





## Verifiëren

FTD

Opdrachten weergeven

Controleer op FTD dat de eindgebruiker is aangesloten op AnyConnect VPN:

```
> show ip
```

```
System IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.240	CONFIG
GigabitEthernet0/1	outside	203.0.113.2	255.255.255.240	CONFIG

```
Current IP Addresses:
```

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.240	CONFIG
GigabitEthernet0/1	outside	203.0.113.2	255.255.255.240	CONFIG

```
> show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : jsmith Index : 2
```

```
Assigned IP : 192.168.10.50 Public IP : 198.51.100.2
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
```

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 18458 Bytes Rx : 2706024  
Pkts Tx : 12 Pkts Rx : 50799  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : DfltGrpPolicy Tunnel Group : FTDAnyConnectVPN  
Login Time : 15:08:19 UTC Wed Oct 10 2018  
Duration : 0h:30m:11s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0ac9d68a000020005bbe15e3  
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 2.1

**Public IP : 198.51.100.2**

Encryption : none Hashing : none

TCP Src Port : 53956 TCP Dst Port : 443

Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 0 Minutes

Client OS : win

Client OS Ver: 6.1.7601 Service Pack 1

Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049

Bytes Tx : 10572 Bytes Rx : 289

Pkts Tx : 6 Pkts Rx : 0

Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 2.2

**Assigned IP : 192.168.10.50 Public IP : 198.51.100.2**

Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384

Encapsulation: TLSv1.2 TCP Src Port : 54634

TCP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes

Client OS : Windows

Client Type : SSL VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049

Bytes Tx : 7886 Bytes Rx : 2519

Pkts Tx : 6 Pkts Rx : 24

Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 2.3

**Assigned IP : 192.168.10.50 Public IP : 198.51.100.2**

Encryption : AES256 Hashing : SHA1

Ciphersuite : DHE-RSA-AES256-SHA

Encapsulation: DTLSv1.0 UDP Src Port : 61113

UDP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes

Client OS : Windows

Client Type : DTLS VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049

Bytes Tx : 0 Bytes Rx : 2703216

Pkts Tx : 0 Pkts Rx : 50775

Pkts Tx Drop : 0 Pkts Rx Drop : 0

Zodra u op de Windows 7 PC bent en op 'Koppelen' klikt op Cisco AnyConnect-client, krijgt u:

```
> show vpn-sessiondb detail anyconnect
INFO: There are presently no active sessions
```

## Bijleggen

Hoe een werkopname er uitziet op Outside Interface wanneer u op AnyConnect Client klikt

Voorbeeld:

De openbare IP van de eindgebruiker zal bijvoorbeeld het openbare IP van hun router thuis zijn

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
```

```
<now hit Connect on AnyConnect Client from employee PC>
```

```
ciscofp3# show cap
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153
bytes]
match ip any host 198.51.100.2
```

Bekijk de pakketten die vanuit de pc van de eindgebruiker naar de buiteninterface van de FTD zijn gekomen om er zeker van te zijn dat ze op onze buiteninterface op FTD aankomen:

```
ciscofp3# show cap capin
2375 packets captured
1: 17:05:56.580994      198.51.100.2.55928 > 203.0.113.2.443: S 2933933902:2933933902(0) win
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
2: 17:05:56.581375      203.0.113.2.443 > 198.51.100.2.55928: S 430674106:430674106(0) ack
2933933903 win 32768 <mss 1460>
3: 17:05:56.581757      198.51.100.2.55928 > 203.0.113.2.443: . ack 430674107 win 64240
4: 17:05:56.582382      198.51.100.2.55928 > 203.0.113.2.443: P 2933933903:2933934036(133) ack
430674107 win 64240
5: 17:05:56.582458      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933934036 win 32768
6: 17:05:56.582733      203.0.113.2.443 > 198.51.100.2.55928: P 430674107:430675567(1460) ack
2933934036 win 32768
7: 17:05:56.790211      198.51.100.2.55928 > 203.0.113.2.443: . ack 430675567 win 64240
8: 17:05:56.790349      203.0.113.2.443 > 198.51.100.2.55928: P 430675567:430676672(1105) ack
2933934036 win 32768
9: 17:05:56.791691      198.51.100.2.55928 > 203.0.113.2.443: P 2933934036:2933934394(358) ack
430676672 win 63135
10: 17:05:56.794911      203.0.113.2.443 > 198.51.100.2.55928: P 430676672:430676763(91) ack
2933934394 win 32768
11: 17:05:56.797077      198.51.100.2.55928 > 203.0.113.2.443: P 2933934394:2933934703(309) ack
430676763 win 63044
12: 17:05:56.797169      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933934703 win 32768
13: 17:05:56.797199      198.51.100.2.55928 > 203.0.113.2.443: P 2933934703:2933935524(821) ack
430676763 win 63044
14: 17:05:56.797276      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935524 win 32768
15: 17:05:56.798634      203.0.113.2.443 > 198.51.100.2.55928: P 430676763:430677072(309) ack
2933935524 win 32768
16: 17:05:56.798786      203.0.113.2.443 > 198.51.100.2.55928: P 430677072:430677829(757) ack
2933935524 win 32768
17: 17:05:56.798817      203.0.113.2.443 > 198.51.100.2.55928: P 430677829:430677898(69) ack
2933935524 win 32768
18: 17:05:56.799397      198.51.100.2.55928 > 203.0.113.2.443: . ack 430677898 win 64240
19: 17:05:56.810215      198.51.100.2.55928 > 203.0.113.2.443: P 2933935524:2933935593(69) ack
430677898 win 64240
20: 17:05:56.810398      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935593 win 32768
21: 17:05:56.810428      198.51.100.2.55928 > 203.0.113.2.443: F 2933935593:2933935593(0) ack
```

430677898 win 64240  
22: 17:05:56.810489 203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935594 win 32768  
23: 17:05:56.810627 203.0.113.2.443 > 198.51.100.2.55928: FP 430677898:430677898(0) ack  
2933935594 win 32768  
24: 17:05:56.811008 198.51.100.2.55928 > 203.0.113.2.443: . ack 430677899 win 64240  
25: 17:05:59.250566 198.51.100.2.56228 > 203.0.113.2.443: S 2614357960:2614357960(0) win  
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>  
26: 17:05:59.250963 203.0.113.2.443 > 198.51.100.2.56228: S 3940915253:3940915253(0) ack  
2614357961 win 32768 <mss 1460>  
27: 17:05:59.251406 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940915254 win 64240  
28: 17:05:59.252062 198.51.100.2.56228 > 203.0.113.2.443: P 2614357961:2614358126(165) ack  
3940915254 win 64240  
29: 17:05:59.252138 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358126 win 32768  
30: 17:05:59.252458 203.0.113.2.443 > 198.51.100.2.56228: P 3940915254:3940915431(177) ack  
2614358126 win 32768  
31: 17:05:59.253450 198.51.100.2.56228 > 203.0.113.2.443: P 2614358126:2614358217(91) ack  
3940915431 win 64063  
32: 17:05:59.253679 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358217 win 32768  
33: 17:05:59.255235 198.51.100.2.56228 > 203.0.113.2.443: P 2614358217:2614358526(309) ack  
3940915431 win 64063  
34: 17:05:59.255357 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358526 win 32768  
35: 17:05:59.255388 198.51.100.2.56228 > 203.0.113.2.443: P 2614358526:2614359555(1029)  
ack 3940915431 win 64063  
36: 17:05:59.255495 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359555 win 32768  
37: 17:05:59.400110 203.0.113.2.443 > 198.51.100.2.56228: P 3940915431:3940915740(309) ack  
2614359555 win 32768  
38: 17:05:59.400186 203.0.113.2.443 > 198.51.100.2.56228: P 3940915740:3940917069(1329)  
ack 2614359555 win 32768  
39: 17:05:59.400675 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940917069 win 64240  
40: 17:05:59.400736 203.0.113.2.443 > 198.51.100.2.56228: P 3940917069:3940918529(1460)  
ack 2614359555 win 32768  
41: 17:05:59.400751 203.0.113.2.443 > 198.51.100.2.56228: P 3940918529:3940919979(1450)  
ack 2614359555 win 32768  
42: 17:05:59.401544 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940919979 win 64240  
43: 17:05:59.401605 203.0.113.2.443 > 198.51.100.2.56228: P 3940919979:3940921439(1460)  
ack 2614359555 win 32768  
44: 17:05:59.401666 203.0.113.2.443 > 198.51.100.2.56228: P 3940921439:3940922899(1460)  
ack 2614359555 win 32768  
45: 17:05:59.401727 203.0.113.2.443 > 198.51.100.2.56228: P 3940922899:3940923306(407) ack  
2614359555 win 32768  
46: 17:05:59.401743 203.0.113.2.443 > 198.51.100.2.56228: P 3940923306:3940923375(69) ack  
2614359555 win 32768  
47: 17:05:59.402185 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940923375 win 64240  
48: 17:05:59.402475 198.51.100.2.56228 > 203.0.113.2.443: P 2614359555:2614359624(69) ack  
3940923375 win 64240  
49: 17:05:59.402597 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359624 win 32768  
50: 17:05:59.402628 198.51.100.2.56228 > 203.0.113.2.443: F 2614359624:2614359624(0) ack  
3940923375 win 64240  
51: 17:05:59.402673 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359625 win 32768  
52: 17:05:59.402765 203.0.113.2.443 > 198.51.100.2.56228: FP 3940923375:3940923375(0) ack  
2614359625 win 32768  
53: 17:05:59.413384 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940923376 win 64240  
54: 17:05:59.555665 198.51.100.2.56280 > 203.0.113.2.443: S 1903869753:1903869753(0) win  
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>  
55: 17:05:59.556154 203.0.113.2.443 > 198.51.100.2.56280: S 2583094766:2583094766(0) ack  
1903869754 win 32768 <mss 1460>  
56: 17:05:59.556627 198.51.100.2.56280 > 203.0.113.2.443: . ack 2583094767 win 64240  
57: 17:05:59.560502 198.51.100.2.56280 > 203.0.113.2.443: P 1903869754:1903869906(152) ack  
2583094767 win 64240  
58: 17:05:59.560578 203.0.113.2.443 > 198.51.100.2.56280: . ack 1903869906 win 32768  
59: 17:05:59.563996 203.0.113.2.443 > 198.51.100.2.56280: P 2583094767:2583096227(1460)  
ack 1903869906 win 32768  
60: 17:05:59.780034 198.51.100.2.56280 > 203.0.113.2.443: . ack 2583096227 win 64240  
61: 17:05:59.780141 203.0.113.2.443 > 198.51.100.2.56280: P 2583096227:2583097673(1446)

```

ack 1903869906 win 32768
62: 17:05:59.998376      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583097673 win 62794
63: 17:06:14.809253      198.51.100.2.56280 > 203.0.113.2.443: P 1903869906:1903870032(126) ack
2583097673 win 62794
64: 17:06:14.809970      203.0.113.2.443 > 198.51.100.2.56280: P 2583097673:2583097724(51) ack
1903870032 win 32768
65: 17:06:14.815768      198.51.100.2.56280 > 203.0.113.2.443: P 1903870032:1903870968(936) ack
2583097724 win 64240
66: 17:06:14.815860      203.0.113.2.443 > 198.51.100.2.56280: . ack 1903870968 win 32768
67: 17:06:14.816913      203.0.113.2.443 > 198.51.100.2.56280: P 2583097724:2583099184(1460)
ack 1903870968 win 32768
68: 17:06:14.816928      203.0.113.2.443 > 198.51.100.2.56280: P 2583099184:2583099306(122) ack
1903870968 win 32768
69: 17:06:14.816959      203.0.113.2.443 > 198.51.100.2.56280: P 2583099306:2583100766(1460)
ack 1903870968 win 32768
70: 17:06:14.816974      203.0.113.2.443 > 198.51.100.2.56280: P 2583100766:2583100888(122) ack
1903870968 win 32768
71: 17:06:14.816989      203.0.113.2.443 > 198.51.100.2.56280: P 2583100888:2583102142(1254)
ack 1903870968 win 32768
72: 17:06:14.817554      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583102142 win 64240
73: 17:06:14.817615      203.0.113.2.443 > 198.51.100.2.56280: P 2583102142:2583103602(1460)
ack 1903870968 win 32768
74: 17:06:14.817630      203.0.113.2.443 > 198.51.100.2.56280: P 2583103602:2583103930(328) ack
1903870968 win 32768
75: 17:06:14.817630      203.0.113.2.443 > 198.51.100.2.56280: P 2583103930:2583104052(122) ack
1903870968 win 32768
76: 17:06:14.817645      203.0.113.2.443 > 198.51.100.2.56280: P 2583104052:2583105512(1460)
ack 1903870968 win 32768
77: 17:06:14.817645      203.0.113.2.443 > 198.51.100.2.56280: P 2583105512:2583105634(122) ack
1903870968 win 32768
78: 17:06:14.817660      203.0.113.2.443 > 198.51.100.2.56280: P 2583105634:2583105738(104) ack
1903870968 win 32768
79: 17:06:14.818088      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583105512 win 64240
80: 17:06:14.818530      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583105738 win 64014
81: 17:06:18.215122      198.51.100.2.58944 > 203.0.113.2.443: udp 99
82: 17:06:18.215610      203.0.113.2.443 > 198.51.100.2.58944: udp 48
83: 17:06:18.215671      198.51.100.2.56280 > 203.0.113.2.443: P 1903870968:1903872025(1057)
ack 2583105738 win 64014
84: 17:06:18.215763      203.0.113.2.443 > 198.51.100.2.56280: . ack 1903872025 win 32768
85: 17:06:18.247011      198.51.100.2.58944 > 203.0.113.2.443: udp 119
86: 17:06:18.247728      203.0.113.2.443 > 198.51.100.2.58944: udp 188
87: 17:06:18.249285      198.51.100.2.58944 > 203.0.113.2.443: udp 93
88: 17:06:18.272309      198.51.100.2.58944 > 203.0.113.2.443: udp 93
89: 17:06:18.277680      198.51.100.2.58944 > 203.0.113.2.443: udp 93
90: 17:06:18.334501      198.51.100.2.58944 > 203.0.113.2.443: udp 221
91: 17:06:18.381541      198.51.100.2.58944 > 203.0.113.2.443: udp 109
92: 17:06:18.443565      198.51.100.2.58944 > 203.0.113.2.443: udp 109
93: 17:06:18.786702      198.51.100.2.58944 > 203.0.113.2.443: udp 157
94: 17:06:18.786870      198.51.100.2.58944 > 203.0.113.2.443: udp 157
95: 17:06:18.786931      198.51.100.2.58944 > 203.0.113.2.443: udp 157
96: 17:06:18.952755      198.51.100.2.58944 > 203.0.113.2.443: udp 109
97: 17:06:18.968272      198.51.100.2.58944 > 203.0.113.2.443: udp 109
98: 17:06:18.973902      198.51.100.2.58944 > 203.0.113.2.443: udp 109
99: 17:06:18.973994      198.51.100.2.58944 > 203.0.113.2.443: udp 109
100: 17:06:18.989267      198.51.100.2.58944 > 203.0.113.2.443: udp 109

```

Bekijk de details van wat er gebeurt met het pakket dat afkomstig is van de eindgebruiker binnen de firewall

```
ciscofp3# show cap capin packet-number 1 trace detail
```

2943 packets captured

1: 17:05:56.580994 006b.f1e7.6c5e 000c.294f.ac84 0x0800 Length: 66  
198.51.100.2.55928 > 203.0.113.2.443: S [tcp sum ok] 2933933902:2933933902(0) win 8192 <mss  
1460,nop,wscale 8,nop,nop,sackOK> (DF) (ttl 127, id 31008)

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace13beec90, priority=13, domain=capture, deny=false

hits=2737, user\_data=0x2ace1232af40, cs\_id=0x0, l3\_type=0x0

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0000.0000.0000

input\_ifc=outside, output\_ifc=any

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace107c8480, priority=1, domain=permit, deny=false

hits=183698, user\_data=0x0, cs\_id=0x0, l3\_type=0x8

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0100.0000.0000

input\_ifc=outside, output\_ifc=any

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 203.0.113.2 using egress ifc identity

Phase: 4

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace1199f680, priority=119, domain=permit, deny=false

hits=68, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=6

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0

input\_ifc=outside, output\_ifc=identity

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace1199efd0, priority=8, domain=conn-set, deny=false

hits=68, user\_data=0x2ace1199e5d0, cs\_id=0x0, reverse, flags=0x0, protocol=6

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=identity

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace0fa81330, priority=0, domain=nat-per-session, deny=false  
hits=178978, user\_data=0x0, cs\_id=0x0, reverse, use\_real\_addr, flags=0x0, protocol=6  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=any, output\_ifc=any

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2acel07cdb00, priority=0, domain=inspect-ip-options, deny=true  
hits=174376, user\_data=0x0, cs\_id=0x0, reverse, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=any

Phase: 8

Type: CLUSTER-REDIRECT

Subtype: cluster-redirect

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2acel07c90c0, priority=208, domain=cluster-redirect, deny=false  
hits=78, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=identity

Phase: 9

Type: TCP-MODULE

Subtype: webvpn

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2acel199df20, priority=13, domain=soft-np-tcp-module, deny=false  
hits=58, user\_data=0x2ace061efb00, cs\_id=0x0, reverse, flags=0x0, protocol=6  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=identity

Phase: 10

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2acel1d455e0, priority=13, domain=ipsec-tunnel-flow, deny=true

hits=87214, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=any

Phase: 11

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace11da7000, priority=13, domain=capture, deny=false  
hits=635, user\_data=0x2ace1232af40, cs\_id=0x2ace11f21620, reverse, flags=0x0, protocol=0  
src ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any  
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
input\_ifc=outside, output\_ifc=any

Phase: 12

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

out id=0x2ace10691780, priority=13, domain=capture, deny=false  
hits=9, user\_data=0x2ace1232af40, cs\_id=0x2ace11f21620, reverse, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any  
dst ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any, dscp=0x0  
input\_ifc=any, output\_ifc=outside

Phase: 13

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 87237, packet dispatched to next module

Module information for forward flow ...

snp\_fp\_inspect\_ip\_options  
snp\_fp\_tcp\_normalizer  
snp\_fp\_tcp\_mod  
snp\_fp\_adjacency  
snp\_fp\_fragment  
snp\_fp\_drop

Module information for reverse flow ...

snp\_fp\_inspect\_ip\_options  
snp\_fp\_tcp\_normalizer  
snp\_fp\_adjacency  
snp\_fp\_fragment  
snp\_ifc\_stat

Result:

input-interface: outside  
input-status: up  
input-line-status: up  
output-interface: NP Identity Ifc  
Action: allow

1 packet shown

ciscofp3#

Kopieert de opname naar schijf0: van uw FTD. U kunt het vervolgens downloaden via SCP, FTP



## of TFTP

(of vanuit FirePOWER Management Center Web UI > Systeem > Health > Health Monitor > Klik op Advanced Problemen opsporen > Klik op het tabblad Downloadbestand)

```
ciscofp3# copy /pcap capture:capin disk0:/capin.pcap
```

```
Source capture name [capin]? <hit Enter>
```

```
Destination filename [capin.pcap]? <hit Enter>
```

```
!!!!!!!!!!!!!!!!!!!!
```

```
207 packets copied in 0.0 secs
```

```
ciscofp3# dir
```

```
Directory of disk0:/
```

```
122 -rwx 198 05:13:44 Apr 01 2018 lina_phase1.log
```

```
49 drwx 4096 21:42:20 Jun 30 2018 log
```

```
53 drwx 4096 21:42:36 Jun 30 2018 coredumpinfo
```

```
110 drwx 4096 14:59:51 Oct 10 2018 csm
```

```
123 -rwx 21074 01:26:44 Oct 10 2018 backup-config.cfg
```

```
124 -rwx 21074 01:26:44 Oct 10 2018 startup-config
```

```
125 -rwx 20354 01:26:44 Oct 10 2018 modified-config.cfg
```

```
160 -rwx 60124 17:06:22 Oct 10 2018 capin.pcap
```

```
ciscofp3# copy disk0:/capin.pcap tftp:/
```

```
Source filename [capin.pcap]? <hit Enter>
```

```
Address or name of remote host []? 192.168.1.25 (your TFTP server IP address (your PC if using tftpd32 or Solarwinds TFTP Server))
```

```
Destination filename [capin.pcap]? <hit Enter>
```

```
113645 bytes copied in 21.800 secs (5411 bytes/sec)
```

```
ciscofp3#
```

(or from FirePOWER Management Center Web GUI >> System >> Health >> Health Monitor >> click Advanced Troubleshooting >> click Download File tab)

Controleer of de NAT-regel correct is ingesteld:

```
ciscofp3# packet-tracer input outside tcp 192.168.10.50 1234 192.168.1.30 443 detailed
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2ace0fa90e70, priority=13, domain=capture, deny=false
```

```
hits=11145169, user_data=0x2acel20c4910, cs_id=0x0, l3_type=0x0
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=0000.0000.0000, mask=0000.0000.0000
```

```
input_ifc=outside, output_ifc=any
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2acel07c8480, priority=1, domain=permit, deny=false
```

```
hits=6866095, user_data=0x0, cs_id=0x0, l3_type=0x8
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

dst mac=0000.0000.0000, mask=0100.0000.0000  
input\_ifc=outside, output\_ifc=any

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop **192.168.1.30** using egress ifc inside

Phase: 4

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

**nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup**

Additional Information:

NAT divert to egress interface inside

Untranslate 192.168.1.30/443 to 192.168.1.30/443

Phase: 5

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM\_FW\_ACL\_ global

access-list CSM\_FW\_ACL\_ advanced trust ip ifc outside any any rule-id 268436481 event-log flow-end

access-list CSM\_FW\_ACL\_ remark rule-id 268436481: PREFILTER POLICY:

Example\_Company\_Prefilter\_Policy

access-list CSM\_FW\_ACL\_ remark rule-id 268436481: RULE: AllowtoVPNOutsideinterface

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace0fa8f4e0, priority=12, domain=permit, trust

hits=318637, user\_data=0x2ace057b9a80, cs\_id=0x0, use\_real\_addr, flags=0x0, protocol=0

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=outside

dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0

input\_ifc=any, output\_ifc=any

...

Phase: 7

Type: NAT

Subtype:

Result: ALLOW

Config:

**nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup**

Additional Information:

Static translate 192.168.10.50/1234 to 192.168.10.50/1234

Forward Flow based lookup yields rule:

in id=0x2acell1975cb0, priority=6, domain=nat, deny=false

hits=120, user\_data=0x2ace0f29c4a0, cs\_id=0x0, flags=0x0, protocol=0

src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0

input\_ifc=outside, output\_ifc=inside

...

Phase: 10 Type: VPN Subtype: ipsec-tunnel-flow Result: ALLOW Config: Additional Information:

Forward Flow based lookup yields rule: in id=0x2acell1d455e0, priority=13, domain=ipsec-tunnel-flow, deny=true hits=3276174, user\_data=0x0, cs\_id=0x0, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0

```

input_ifc=outside, output_ifc=any Phase: 11 Type: NAT Subtype: rpf-check Result: ALLOW Config:
nat (inside,outside) source static inside-subnet inside-subnet destination static outside-
subnet-anyconnect-po ol outside-subnet-anyconnect-pool no-proxy-arp route-lookup
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ace0d5a9800, priority=6, domain=nat-reverse, deny=false
hits=121, user_data=0x2ace1232a4c0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=inside

```

...

```

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3279248, packet dispatched to next module

```

Module information for reverse flow ...  
...

```

Phase: 15
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.30 using egress ifc inside

```

```

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow

```

ciscofp3#

Opname op de PC waar de PC met succes is aangesloten, die via AnyConnect VPN op de FTD is aangesloten

The screenshot shows a Wireshark capture of network traffic. The interface is 'anyconnectinitiation.pcapng'. The packet list pane shows a series of packets from source 56501 to destination 443. Packet 129 is a SYN packet (Seq=0, Win=8192, Len=0). Packet 130 is a SYN-ACK packet (Seq=0, Ack=1, Win=32768, Len=0). Packet 131 is an ACK packet (Seq=1, Ack=1, Win=64240, Len=0). Packet 132 is a Client Hello packet (Len=187). Packet 133 is a SYN-ACK packet (Seq=1, Ack=134, Win=32768, Len=0). Packet 134 is a Server Hello packet (Len=1514). Packet 142 is an ACK packet (Seq=134, Ack=1461, Win=64240, Len=0). Packet 143 is a Certificate, Server Hello Done packet (Len=1159). Packet 144 is a Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message packet (Len=412). Packet 145 is a Change Cipher Spec, Encrypted Handshake Message packet (Len=145). Packet 146 is an Application Data packet (Len=363). Packet 147 is another Application Data packet (Len=875). Packet 148 is an ACK packet (Seq=2657, Ack=801, Win=32768, Len=0). Packet 149 is another ACK packet (Seq=2657, Ack=1622, Win=32768, Len=0). Packet 150 is an Application Data packet (Len=363). Packet 151 is another Application Data packet (Len=811). The packet details pane at the bottom shows the selected packet (No. 148) as a Transmission Control Protocol packet with Source Port: 56501 and Destination Port: 443.

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
129	3.685253		56501		443	TCP	66	56501 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
130	3.685868		443		56501	TCP	60	443 → 56501 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
131	3.685917		56501		443	TCP	54	56501 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
132	3.687035		56501		443	TLSv1.2	187	Client Hello
133	3.687442		443		56501	TCP	60	443 → 56501 [ACK] Seq=1 Ack=134 Win=32768 Len=0
134	3.687806		443		56501	TLSv1.2	1514	Server Hello
142	3.899719		56501		443	TCP	54	56501 → 443 [ACK] Seq=134 Ack=1461 Win=64240 Len=0
143	3.900303		443		56501	TLSv1.2	1159	Certificate, Server Hello Done
144	3.901003		56501		443	TLSv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
145	3.904245		443		56501	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
146	3.907281		56501		443	TLSv1.2	363	Application Data
147	3.907374		56501		443	TLSv1.2	875	Application Data
148	3.907797		443		56501	TCP	60	443 → 56501 [ACK] Seq=2657 Ack=801 Win=32768 Len=0
149	3.907868		443		56501	TCP	60	443 → 56501 [ACK] Seq=2657 Ack=1622 Win=32768 Len=0
150	3.909600		443		56501	TLSv1.2	363	Application Data
151	3.909759		443		56501	TLSv1.2	811	Application Data

Transmission Control Protocol, Src Port: 56501, Dst Port: 443, Seq: 0, Len: 0  
Source Port: 56501  
Destination Port: 443

U kunt ook zien dat de DTLS-tunnel later in dezelfde opname wordt gevormd

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets with columns for No., Time, Source, Src port, Destination, Dst port, Protocol, and Length Info. The packets show a sequence of events: a TCP segment (No. 76), application data (Nos. 77-80), a Client Hello (No. 81), a Hello Verify Request (No. 82), more application data (Nos. 83-84), another Client Hello (No. 85), a Server Hello and Change Cipher Spec (Nos. 86-87), and final application data (Nos. 88-90). The protocols involved are TCP, TLSv1.2, and DTLS 1.0 (OpenSSL pre 0.9.8f).

Below the packet list, the details pane for Frame 81 is expanded, showing the following structure:

- > Frame 81: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)
- > Ethernet II, Src: Cisco\_e7:6c:5e (00:6b:f1:e7:6c:5e), Dst: Vmware\_4f:ac:84 (00:0c:29:4f:ac:84)
- > Internet Protocol Version 4, Src: ..., Dst: ...
- > User Datagram Protocol, Src Port: 58944, Dst Port: 443
- ▼ Datagram Transport Layer Security
  - ▼ DTLS 1.0 (OpenSSL pre 0.9.8f) Record Layer: Handshake Protocol: Client Hello
    - Content Type: Handshake (22)
    - Version: DTLS 1.0 (OpenSSL pre 0.9.8f) (0x0100)
    - Epoch: 0
    - Sequence Number: 0
    - Length: 86
    - ▼ Handshake Protocol: Client Hello
      - Handshake Type: Client Hello (1)
      - Length: 74
      - Message Sequence: 0
      - Fragment Offset: 0
      - Fragment Length: 74

Opname op de buiteninterface van de FTD waarop de AnyConnect PC met succes wordt aangesloten, met VPN

capin.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	12:05:56.580994		55928		443	TCP	66	55928 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	12:05:56.581375		443		55928	TCP	58	443 → 55928 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
3	12:05:56.581757		55928		443	TCP	54	55928 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	12:05:56.582382		55928		443	TLV1.2	187	Client Hello
5	12:05:56.582458		443		55928	TCP	54	443 → 55928 [ACK] Seq=1 Ack=134 Win=32768 Len=0
6	12:05:56.582733		443		55928	TLV1.2	1514	Server Hello ←
7	12:05:56.790211		55928		443	TCP	54	55928 → 443 [ACK] Seq=134 Ack=1461 Win=64240 Len=0
8	12:05:56.790349		443		55928	TLV1.2	1159	Certificate, Server Hello Done
9	12:05:56.791691		55928		443	TLV1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	12:05:56.794911		443		55928	TLV1.2	145	Change Cipher Spec, Encrypted Handshake Message
11	12:05:56.797077		55928		443	TLV1.2	363	Application Data
12	12:05:56.797169		443		55928	TCP	54	443 → 55928 [ACK] Seq=2657 Ack=801 Win=32768 Len=0
13	12:05:56.797199		55928		443	TLV1.2	875	Application Data
14	12:05:56.797276		443		55928	TCP	54	443 → 55928 [ACK] Seq=2657 Ack=1622 Win=32768 Len=0
15	12:05:56.798634		443		55928	TLV1.2	363	Application Data
16	12:05:56.798786		443		55928	TLV1.2	811	Application Data

> Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: Vmware\_4f:ac:84 (00:0c:29:4f:ac:84), Dst: Cisco\_e7:6c:5e (00:6b:f1:e7:6c:5e)

> Internet Protocol Version 4, Src: , Dst:

> Transmission Control Protocol, Src Port: 443, Dst Port: 55928, Seq: 1, Ack: 134, Len: 1460

Source Port: 443

Destination Port: 55928

[Stream index: 0]

[TCP Segment Len: 1460]

Sequence number: 1 (relative sequence number)

[Next sequence number: 1461 (relative sequence number)]

Acknowledgment number: 134 (relative ack number)

0101 ... = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 32768

[Calculated window size: 32768]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x3693 [unverified]

```

00c0 99 2a 86 48 86 f7 0d 01 01 0b 05 00 30 51 31 15 ..*H....0Q1
00d0 30 13 06 0a 09 92 26 89 93 f2 2c 64 01 19 16 05 0.....&...d...
00e0 6c 6f 63 61 6c 31 19 30 17 06 0a 09 92 26 89 93 local1-0....&...
00f0 f2 2c 64 01 19 16 09 63 6f 68 61 64 6c 65 79 33 ..,d....>...
0100 31 1d 30 1b 06 03 55 04 03 13 14 63 6f 68 61 64 1-0...U....CA6
0110 6c 65 79 33 2d 43 4f 52 42 44 43 33 2d 43 41 30 ..201009 024500Z
0120 1e 17 0d 31 38 31 30 31 30 32 34 35 30 30 5a 30 ..1805..*H....
0130 17 0d 32 30 31 30 30 39 30 32 34 35 30 30 5a 30 ..201009 024500Z
0140 81 b3 31 26 30 24 06 09 2a 86 48 86 f7 0d 01 09 ..1805..*H....
0150 92 13 17 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 ... f p3...
0160 6c 65 79 33 2e 6c 6f 63 61 6c 31 0b 30 09 06 03 ..U...US1-0...U...
0170 55 04 06 13 02 55 53 11 0b 30 09 06 03 55 04 08 ..CA1-0-..U...S
0180 13 02 43 41 31 11 30 0f 06 03 55 04 07 13 08 53 ..an Jose1-0...U...
0190 61 6e 20 4a 6f 73 65 31 0e 30 0c 06 03 55 04 0a ..Cisco1-0...U...
01a0 13 05 43 69 73 63 6f 31 0c 30 0a 06 03 55 04 0b ..TAC1 0-..U...
01b0 13 03 54 41 43 31 20 30 1e 06 03 55 04 03 13 17 ..rfp3.
01c0 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 6c 65 79 3. local1-0...*H...
01d0 33 2e 6c 6f 63 61 6c 31 1c 30 1a 06 09 2a 86 48 ..... tac@cisc
01e0 86 f7 0d 01 09 01 16 0d 74 61 63 40 63 69 73 63 ..o.com0...0...*H...
01f0 6f 2e 63 6f 6d 30 82 01 22 30 0d 06 09 2a 86 48 .....
0200 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 .....0...

```

capin.pcap

Opmerking: U kunt het FTD VPN Server certificaat in het pakket van "Server Hallo" zien aangezien we verbinding maken met de externe interface van de FTD via VPN. De PC van de werknemer zal dit certificaat vertrouwen omdat de PC van de werknemer het certificaat van de Root CA op het heeft en het certificaat van de FTD VPN Server werd ondertekend door die zelfde CA van de Root.

Leg de FTD van de FTD vragende RADIUS-server vast als de gebruikersnaam + het wachtwoord juist is (Cisco ISE)

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	13:05:36.771841		3238		1812	RADIUS	701	Access-Request id=93
2	13:05:42.865342		1812		3238	RADIUS	201	Access-Accept id=93
3	13:05:42.865937		3238		1812	RADIUS	701	Access-Request id=94
4	13:05:42.911314		1812		3238	RADIUS	62	Access-Reject id=94
5	13:05:43.302825		19500		1813	RADIUS	756	Accounting-Request id=95
6	13:05:43.309294		1813		19500	RADIUS	62	Accounting-Response id=95

```

> Frame 2: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
> Ethernet II, Src: Cisco_e7:6c:5e (00:6b:f1:e7:6c:5e), Dst: Vmware_4f:ac:84 (00:0c:29:4f:ac:84)
> Internet Protocol Version 4, Src: ..., Dst: ...
> User Datagram Protocol, Src Port: 1812, Dst Port: 3238
RADIUS Protocol
  Code: Access-Accept (2)
0000  00 0c 29 4f ac 84 00 6b f1 e7 6c 5e 08 00 45 00  ..)O..k..l^..E.
0010  00 bb 5f 66 40 00 3f 11 18 bc 0a c9 d6 e6 0a c9  .._f@?......
0020  d6 97 07 14 0c a6 00 a7 4e 17 02 5d 00 9f 7f b9  .....N..]....
0030  c7 a6 65 6d e7 75 c7 64 7f 0f d5 54 d7 59 01 08  ..em u d ...T.Y..
0040  6a 73 6d 69 74 68 18 28 52 65 61 75 74 68 53 65  jsmith( ReauthSe
0050  73 73 69 6f 6e 3a 30 61 63 39 64 36 38 61 30 30  ssion:0a c9d68a00
0060  30 31 61 30 30 30 35 62 62 66 39 30 66 30 19 3b  01a0005b bf90f0;
0070  43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30  CACS:0ac 9d68a000
0080  31 61 30 30 30 35 62 62 66 39 30 66 30 3a 63 6f  1a0005bb f90f0:co
0090  72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38  rbinise/ 32234408
00a0  34 2f 31 39 37 34 32 39 39 1a 20 00 00 09 01     4/197429 9. ....
00b0  1a 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f  .profile -name=Wo
00c0  72 6b 73 74 61 74 69 6f 6e                      rkstatio n

```

Zoals u hierboven kunt zien, krijgt onze VPN-verbinding een access-Accept en is onze AnyConnect VPN-client met succes verbonden met de FTD via VPN

Capture (CLI) van FTD waarin Cisco ISE wordt gevraagd of de gebruikersnaam + het wachtwoord geldig is (Controleer dus of de RADIUS-verzoeken succesvol verlopen tussen FTD en ISE en controleer of de interface weg is)

```

ciscofp3# capture capout interface inside trace detail trace-count 100 [Capturing - 35607 bytes]
ciscofp3# show cap
ciscofp3# show cap capout | i 192.168.1.10
37: 01:23:52.264512 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
38: 01:23:52.310210 192.168.1.10.1812 > 192.168.1.1.3238: udp 159
39: 01:23:52.311064 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
40: 01:23:52.326734 192.168.1.10.1812 > 192.168.1.1.3238: udp 20
82: 01:23:52.737663 192.168.1.1.19500 > 192.168.1.10.1813: udp 714
85: 01:23:52.744483 192.168.1.10.1813 > 192.168.1.1.19500: udp 20

```

Onder de Cisco ISE RADIUS-server toont dat de verificatie succesvol is. Klik op het vergrootglas om de details van de succesvolle authenticatie te zien

Oct 11, 2018 06:10:08.808 PM			0	jsmith	00:0C:29:37:EF:BF	Workstation	VPN Users >> Default	VPN Users >> Allow FTD VPN connections if AD Group VPNusers	PermitAccess	
Oct 11, 2018 06:10:08.808 PM				jsmith	00:0C:29:37:EF:BF	FTDVPN	Workstation	VPN Users >> Default	VPN Users >> Allow FTD VPN connections if AD Group VPNusers	PermitAccess



### Overview

Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	00:0C:29:37:EF:BF ⓘ
Endpoint Profile	Workstation
Authentication Policy	VPN Users >> Default
Authorization Policy	VPN Users >> Allow FTD VPN connections if AD Group VPNusers
Authorization Result	PermitAccess

Opnemen op de AnyConnect-adapter van de PC van de medewerker die naar een website met interne gebruiker via HTTPS gaat (d.w.z. terwijl deze met succes VPN'd in staat is):

The screenshot shows a Wireshark capture of network traffic on the interface '\*Local Area Connection 2'. A filter is applied to 'tcp.port == 443'. The capture shows a series of packets from source IP 192.168.10.50 to destination IP 192.168.10.50. The traffic includes a SYN packet (No. 49), a SYN-ACK packet (No. 50), and subsequent TLS handshake packets (Nos. 51-67) such as Client Hello, Server Hello, Key Exchange, Change Cipher Spec, and Application Data. The bottom pane shows the details of the selected packet (No. 67), identifying it as a Transmission Control Protocol (tcp) packet, 32 bytes in length, with source port 63576 and destination port 443. The packet bytes are displayed in hexadecimal and ASCII.

### Debugs

Straal verwijderen

debug van webversie 25



# Start 'debug Straal' opdracht op FTD diagnostic CLI (>systemondersteuning voor diagnostiek-CLI) en druk 'Connect' op Windows/Mac PC op Cisco Any Connect Client

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
ciscofp3> enable
```

```
Password: <hit enter>
```

```
ciscofp3# terminal monitor
```

```
ciscofp3# debug radius all
```

```
<hit Connect on Anyconnect client on PC>
```

```
radius mkreq: 0x15
```

```
alloc_rip 0x00002ace10875428
```

```
new request 0x15 --> 16 (0x00002ace10875428)
```

```
got user 'jsmith'
```

```
got password
```

```
add_req 0x00002ace10875428 session 0x15 id 16
```

```
RADIUS_REQUEST
```

```
radius.c: rad_mkpkt
```

```
rad_mkpkt: ip:source-ip=198.51.100.2
```

```
RADIUS packet decode (authentication request)
```

```
-----  
Raw packet data (length = 659).....
```

```
01 10 02 93 fb 19 19 df f6 b1 c7 3e 34 fc 88 ce | .....>4...  
75 38 2d 55 01 08 6a 73 6d 69 74 68 02 12 a0 83 | u8-U..jsmith....  
c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 05 06 | ...r...$4.c.....  
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...198.51.100.2  
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .151..198.51.100.2  
2e 32 35 31 3d 06 00 00 05 42 10 31 30 2e 32 | .4=.....B.198.  
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 09 | 51.100.2#....  
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device  
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win,..  
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....&mdm-tlv=dev  
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29  
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 09 01 | -37-ef-bf.3.....  
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-  
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c  
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf:...  
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u  
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon  
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6  
2e 30 33 30 34 39 1a 3f 00 00 09 01 39 6d 64 | .03049.?......9md  
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla  
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.  
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P  
61 63 6b 20 31 1a 40 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm  
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type  
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM  
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla  
74 66 6f 72 6d 1a 5b 00 00 09 01 55 6d 64 6d | tform.[.....Umdm  
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=  
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251  
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731  
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3  
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1  
04 06 00 00 00 00 1a 31 00 00 09 01 2b 61 75 | .....1.....+au  
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0  
61 63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 | ac9d68a000050005  
62 62 65 31 66 39 31 1a 23 00 00 09 01 1d 69 | bbelf91.#.....i  
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
```

```
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50.....
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN.....
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | .....coa-push=t
72 75 65 | rue
```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 16 (0x10)

Radius: Length = 659 (0x0293)

Radius: Vector: FB1919DFF6B1C73E34FC88CE75382D55

Radius: Type = 1 (0x01) User-Name

Radius: Length = 8 (0x08)

Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)

Radius: Value (String) =

a0 83 c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 | .....r...\$4.c...

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 35 (0x23)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 29 (0x1D)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p

6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 44 (0x2C)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 38 (0x26)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m

61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e

66 2d 62 66 | f-bf

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 51 (0x33)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 45 (0x2D)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p

75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-

32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 58 (0x3A)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 52 (0x34)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-  
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect  
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030  
34 39 | 49  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 63 (0x3F)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 57 (0x39)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=  
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service  
20 50 61 63 6b 20 31 | Pack 1  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 64 (0x40)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 58 (0x3A)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t  
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.  
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual  
50 6c 61 74 66 6f 72 6d | Platform  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 91 (0x5B)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 85 (0x55)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u  
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925  
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8  
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154  
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961  
34 41 31 | 4A1  
Radius: Type = 4 (0x04) NAS-IP-Address  
Radius: Length = 6 (0x06)  
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 49 (0x31)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 43 (0x2B)  
Radius: Value (String) =  
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id  
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500  
30 35 62 62 65 31 66 39 31 | 05bbelf91  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 35 (0x23)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 29 (0x1D)  
Radius: Value (String) =  
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.  
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 24 (0x18)  
Radius: Vendor ID = 3076 (0x00000C04)

```
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10875428 state 7 id 16
rad_vrfy() : response message verified
rip 0x00002ace10875428
: chall_state ''
: state 0x7
: reqauth:
fb 19 19 df f6 b1 c7 3e 34 fc 88 ce 75 38 2d 55
: info 0x00002ace10875568
session_id 0x15
request_id 0x10
user 'jsmith'
response '***'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1
```

RADIUS packet decode (response)

```
-----
Raw packet data (length = 159).....
02 10 00 9f 39 45 43 cf 05 be df 2f 24 d5 d7 05 | ....9EC..../$...
47 67 b4 fd 01 08 6a 73 6d 69 74 68 18 28 52 65 | Gg....jsmith.(Re
61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 63 39 | authSession:0ac9
64 36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 | d68a000050005bbe
31 66 39 31 19 3b 43 41 43 53 3a 30 61 63 39 64 | 1f91.;CACS:0ac9d
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1a | 2344084/1931682.
20 00 00 00 09 01 1a 70 72 6f 66 69 6c 65 2d 6e | .....profile-n
61 6d 65 3d 57 6f 72 6b 73 74 61 74 69 6f 6e | ame=Workstation
```

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 16 (0x10)
Radius: Length = 159 (0x009F)
Radius: Vector: 394543CF05BEDF2F24D5D7054767B4FD
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 24 (0x18) State
Radius: Length = 40 (0x28)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 | ReauthSession:0a
```

```

63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 62 | c9d68a000050005b
62 65 31 66 39 31 | belf91
Radius: Type = 25 (0x19) Class
Radius: Length = 59 (0x3B)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbelf91:co
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408
34 2f 31 39 33 31 36 38 32 | 4/1931682
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 32 (0x20)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 26 (0x1A)
Radius: Value (String) =
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f 72 | profile-name=Wor
6b 73 74 61 74 69 6f 6e | kstation
rad_procpkt: ACCEPT
Got AV-Pair with value profile-name=Workstation
RADIUS_ACCESS_ACCEPT: normal termination
radius mkreq: 0x16
alloc_rip 0x00002ace10874b80
new request 0x16 --> 17 (0x00002ace10874b80)
got user 'jsmith'
got password
add_req 0x00002ace10874b80 session 0x16 id 17
RADIUS_DELETE
remove_req 0x00002ace10875428 session 0x15 id 16
free_rip 0x00002ace10875428
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

```

RADIUS packet decode (authentication request)

```

-----
Raw packet data (length = 659).....
01 11 02 93 c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 | .....
83 c1 e4 88 01 08 6a 73 6d 69 74 68 02 12 79 41 | .....jsmith..yA
0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 05 06 | .q.8..I.<...e...
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...203.0.113
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .2..203.0.113
2e 32 35 31 3d 06 00 00 05 42 10 31 30 2e 32 | .2=.....<ip addr
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 00 09 | ess>.#....
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win.,.
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ...&mdm-tlv=dev
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 00 09 01 | -37-ef-bf.3.....
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf:...
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6
2e 30 33 30 34 39 1a 3f 00 00 00 09 01 39 6d 64 | .03049.?.....9md
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P
61 63 6b 20 31 1a 40 00 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla
74 66 6f 72 6d 1a 5b 00 00 00 09 01 55 6d 64 6d | tform.[.....Umdm

```

```
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1
04 06 00 00 00 00 1a 31 00 00 00 09 01 2b 61 75 | .....1.....+au
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0
61 63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 | ac9d68a000050005
62 62 65 31 66 39 31 1a 23 00 00 00 09 01 1d 69 | bbe1f91.#.....i
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50.....
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN.....
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | .....coa-push=t
72 75 65 | rue
```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 17 (0x11)

Radius: Length = 659 (0x0293)

Radius: Vector: C6FC11C10EC481AC09A785A883C1E488

Radius: Type = 1 (0x01) User-Name

Radius: Length = 8 (0x08)

Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)

Radius: Value (String) =

79 41 0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 | yA.q.8..I.<...e.

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 35 (0x23)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 29 (0x1D)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p

6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 44 (0x2C)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 38 (0x26)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m

61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e

66 2d 62 66 | f-bf

Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 51 (0x33)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 45 (0x2D)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-  
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 58 (0x3A)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 52 (0x34)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-  
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect  
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030  
34 39 | 49  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 63 (0x3F)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 57 (0x39)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=  
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service  
20 50 61 63 6b 20 31 | Pack 1  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 64 (0x40)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 58 (0x3A)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t  
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.  
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual  
50 6c 61 74 66 6f 72 6d | Platform  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 91 (0x5B)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 85 (0x55)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u  
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925  
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8  
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154  
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961  
34 41 31 | 4A1  
Radius: Type = 4 (0x04) NAS-IP-Address  
Radius: Length = 6 (0x06)  
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 49 (0x31)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 43 (0x2B)  
Radius: Value (String) =  
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id  
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500  
30 35 62 62 65 31 66 39 31 | 05bbelf91  
Radius: Type = 26 (0x1A) Vendor-Specific



```
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10874b80 state 7 id 17
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x7
: reqauth:
c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 83 c1 e4 88
: info 0x00002ace10874cc0
session_id 0x16
request_id 0x11
user 'jsmith'
response '***'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1
```

RADIUS packet decode (response)

```
-----
Raw packet data (length = 20).....
03 11 00 14 15 c3 44 44 7d a6 07 0d 7b 92 f2 3b | .....DD}...{...;
0b 06 ba 74 | ...t
```

Parsed packet data.....

```
Radius: Code = 3 (0x03)
Radius: Identifier = 17 (0x11)
Radius: Length = 20 (0x0014)
Radius: Vector: 15C344447DA6070D7B92F23B0B06BA74
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x16 id 17
free_rip 0x00002ace10874b80
radius: send queue empty
radius mkreq: 0x18
```

alloc\_rip 0x00002ace10874b80  
new request 0x18 --> 18 (0x00002ace10874b80)  
add\_req 0x00002ace10874b80 session 0x18 id 18  
ACCT\_REQUEST  
radius.c: rad\_mkpkt

RADIUS packet decode (accounting request)

```
-----  
Raw packet data (length = 714).....  
04 12 02 ca be a0 6e 46 71 af 5c 65 82 77 c7 b5 | .....nFq.\e.w..  
50 78 61 d7 01 08 6a 73 6d 69 74 68 05 06 00 00 | Pxa...jsmith....  
50 00 06 06 00 00 00 02 07 06 00 00 00 01 08 06 | P.....  
c0 a8 0a 32 19 3b 43 41 43 53 3a 30 61 63 39 64 | ...2.;CACS:0ac9d  
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1  
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32  
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1e | 2344084/1931682.  
10 31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 1f | .203.0.113.2.  
10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 28 | .198.51.100.2(  
06 00 00 00 01 29 06 00 00 00 00 2c 0a 43 31 46 | .....),.....,C1F  
30 30 30 30 35 2d 06 00 00 00 01 3d 06 00 00 00 | 00005-.....=....  
05 42 10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 | .B.203.0.113.2  
31 1a 18 00 00 0c 04 92 12 46 54 44 41 6e 79 43 | .....FTDAnyC  
6f 6e 6e 65 63 74 56 50 4e 1a 0c 00 00 0c 04 96 | onnectVPN.....  
06 00 00 00 02 1a 0c 00 00 0c 04 97 06 00 00 00 | .....  
01 1a 0c 00 00 0c 04 98 06 00 00 00 03 1a 23 00 | .....#.  
00 00 09 01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....mdm-tlv=dev  
69 63 65 2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e | ice-platform=win  
1a 2c 00 00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d | ,.....&mdm-tlv=  
64 65 76 69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 | device-mac=00-0c  
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 31 00 00 | -29-37-ef-bf.1..  
00 09 01 2b 61 75 64 69 74 2d 73 65 73 73 69 6f | ...+audit-sessio  
6e 2d 69 64 3d 30 61 63 39 64 36 38 61 30 30 30 | n-id=0ac9d68a000  
30 35 30 30 30 35 62 62 65 31 66 39 31 1a 33 00 | 050005bbelf91.3.  
00 00 09 01 2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....-mdm-tlv=dev  
69 63 65 2d 70 75 62 6c 69 63 2d 6d 61 63 3d 30 | ice-public-mac=0  
30 2d 30 63 2d 32 39 2d 33 37 2d 65 66 2d 62 66 | 0-0c-29-37-ef-bf  
1a 3a 00 00 00 09 01 34 6d 64 6d 2d 74 6c 76 3d | .:.....4mdm-tlv=  
61 63 2d 75 73 65 72 2d 61 67 65 6e 74 3d 41 6e | ac-user-agent=An  
79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f 77 73 | yConnect Windows  
20 34 2e 36 2e 30 33 30 34 39 1a 3f 00 00 00 09 | 4.6.03049.?....  
01 39 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | .9mdm-tlv=device  
2d 70 6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f | -platform-versio  
6e 3d 36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 | n=6.1.7601 Servi  
63 65 20 50 61 63 6b 20 31 1a 40 00 00 00 09 01 | ce Pack 1.@.....  
3a 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | :mdm-tlv=device-  
74 79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 | type=VMware, Inc  
2e 20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c | . VMware Virtual  
20 50 6c 61 74 66 6f 72 6d 1a 5b 00 00 00 09 01 | Platform.[.....  
55 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | Umdm-tlv=device-  
75 69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 | uid=3693C6407C92  
35 32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 | 5251FF72B6493BDD  
38 37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 | 87318ABFC90C6215  
34 32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 | 42C38FAF878EF496  
31 34 41 31 04 06 00 00 00 00 | 14A1.....
```

Parsed packet data.....  
Radius: Code = 4 (0x04)  
Radius: Identifier = 18 (0x12)  
Radius: Length = 714 (0x02CA)  
Radius: Vector: BEA06E4671AF5C658277C7B5507861D7  
Radius: Type = 1 (0x01) User-Name  
Radius: Length = 8 (0x08)  
Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith  
Radius: Type = 5 (0x05) NAS-Port  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x5000  
Radius: Type = 6 (0x06) Service-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x2  
Radius: Type = 7 (0x07) Framed-Protocol  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x1  
Radius: Type = 8 (0x08) Framed-IP-Address  
Radius: Length = 6 (0x06)  
Radius: Value (IP Address) = 192.168.10.50 (0xC0A80A32)  
Radius: Type = 25 (0x19) Class  
Radius: Length = 59 (0x3B)  
Radius: Value (String) =  
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000  
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbelf91:co  
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408  
34 2f 31 39 33 31 36 38 32 | 4/1931682  
Radius: Type = 30 (0x1E) Called-Station-Id  
Radius: Length = 16 (0x10)  
Radius: Value (String) =  
31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2  
Radius: Type = 31 (0x1F) Calling-Station-Id  
Radius: Length = 16 (0x10)  
Radius: Value (String) =  
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2  
Radius: Type = 40 (0x28) Acct-Status-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x1  
Radius: Type = 41 (0x29) Acct-Delay-Time  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x0  
Radius: Type = 44 (0x2C) Acct-Session-Id  
Radius: Length = 10 (0x0A)  
Radius: Value (String) =  
43 31 46 30 30 30 30 35 | C1F00005  
Radius: Type = 45 (0x2D) Acct-Authentic  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x1  
Radius: Type = 61 (0x3D) NAS-Port-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Hex) = 0x5  
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint  
Radius: Length = 16 (0x10)  
Radius: Value (String) =  
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 24 (0x18)  
Radius: Vendor ID = 3076 (0x00000C04)  
Radius: Type = 146 (0x92) Tunnel-Group-Name  
Radius: Length = 18 (0x12)  
Radius: Value (String) =  
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAAnyConnectVPN  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 12 (0x0C)  
Radius: Vendor ID = 3076 (0x00000C04)  
Radius: Type = 150 (0x96) Client-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Integer) = 2 (0x0002)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 12 (0x0C)  
Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 151 (0x97) VPN-Session-Type  
Radius: Length = 6 (0x06)  
Radius: Value (Integer) = 1 (0x0001)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 12 (0x0C)  
Radius: Vendor ID = 3076 (0x00000C04)  
Radius: Type = 152 (0x98) VPN-Session-Subtype  
Radius: Length = 6 (0x06)  
Radius: Value (Integer) = 3 (0x0003)  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 35 (0x23)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 29 (0x1D)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 44 (0x2C)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 38 (0x26)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m  
61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e  
66 2d 62 66 | f-bf  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 49 (0x31)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 43 (0x2B)  
Radius: Value (String) =  
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id  
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500  
30 35 62 62 65 31 66 39 31 | 05bbelf91  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 51 (0x33)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 45 (0x2D)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-  
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 58 (0x3A)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 52 (0x34)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-  
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect  
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030  
34 39 | 49  
Radius: Type = 26 (0x1A) Vendor-Specific  
Radius: Length = 63 (0x3F)  
Radius: Vendor ID = 9 (0x00000009)  
Radius: Type = 1 (0x01) Cisco-AV-pair  
Radius: Length = 57 (0x39)  
Radius: Value (String) =  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p  
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=  
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service  
20 50 61 63 6b 20 31 | Pack 1

```

Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
send pkt 192.168.1.10/1813
rip 0x00002ace10874b80 state 6 id 18
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x6
: reqauth:
be a0 6e 46 71 af 5c 65 82 77 c7 b5 50 78 61 d7
: info 0x00002ace10874cc0
session_id 0x18
request_id 0x12
user 'jsmith'
response '****'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 3

```

RADIUS packet decode (response)

```

-----
Raw packet data (length = 20).....
05 12 00 14 e5 fd b1 6d fb ee 58 f0 89 79 73 8e | .....m..X..ys.
90 dc a7 20 | ...

```

```

Parsed packet data.....
Radius: Code = 5 (0x05)
Radius: Identifier = 18 (0x12)
Radius: Length = 20 (0x0014)
Radius: Vector: E5FDB16DFBEE58F08979738E90DCA720
rad_procpkt: ACCOUNTING_RESPONSE
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x18 id 18
free_rip 0x00002ace10874b80
radius: send queue empty
ciscofp3#

```

Start 'debug web anyconnect 255' opdracht op FTD diagnostic CLI (>stysteemondersteuning

## diagnostisch-cli) en druk 'Connect' op Windows/Mac PC op Cisco AnyConnect Client

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
ciscofp3> enable
```

```
Password: <hit enter>
```

```
ciscofp3# terminal monitor
```

```
ciscofp3# debug webvpn anyconnect 255
```

```
<hit Connect on Anyconnect client on PC>
```

```
http_parse_cstp_method()
```

```
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'Host: ciscofp3.cisco.com'
```

```
Processing CSTP header line: 'Host: ciscofp3.cisco.com'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'Cookie: webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
Processing CSTP header line: 'Cookie:
```

```
webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
Found WebVPN cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
WebVPN Cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Version: 1'
```

```
Processing CSTP header line: 'X-CSTP-Version: 1'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Hostname: jsmith-PC'
```

```
Processing CSTP header line: 'X-CSTP-Hostname: jsmith-PC'
```

```
Setting hostname to: 'jsmith-PC'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-MTU: 1399'
```

```
Processing CSTP header line: 'X-CSTP-MTU: 1399'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
```

```
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
```

```
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Base-MTU: 1500'
```

```
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
```

```
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Full-IPv6-Capability: true'
```

```
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-Master-Secret:
```

```
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
```

```
'
```

```
Processing CSTP header line: 'X-DTLS-Master-Secret:
```

```
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
```

```
'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
```

```
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
```

```
SHA:DES-CBC3-SHA'
```

```
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
```

```
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address assigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdffd6440, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.50!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) - 16(iv) = 1439
mod-mtu = 1439(mtu) & 0xfff0(complement) = 1424
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtls_hdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cstp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
override computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
```

## Cisco ISE

Cisco ISE > Operations > RADIUS > Live Logs > Klik op details van elke verificatie

Controleer op Cisco ISE uw VPN-inlognaam en het ACL-resultaat 'PermitAccess' wordt gegeven  
Live Logs laten zien dat jsmid via VPN echt is bevonden op FTD



### Overview

Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Endpoint Profile	
Authentication Policy	VPN Users >> Default
Authorization Policy	VPN Users >> Allow ASA VPN connections if AD Group VPNUsers
Authorization Result	PermitAccess

### Authentication Details

Source Timestamp	2018-10-09 01:47:55.112
Received Timestamp	2018-10-09 01:47:55.113
Policy Server	corbinise
Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Calling Station Id	
Authentication Identity Store	corbdc3
Audit Session Id	0000000000070005bbc08c3
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	FTDVPN
Device Type	All Device Types
Location	All Locations

### Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Airespace Airespace-Wlan-Id
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15041 Evaluating Identity Policy
- 15048 Queried PIP - Normalised Radius.RadiusFlowType
- 22072 Selected identity source sequence - All\_User\_ID\_Stores
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - jsmith
- 24216 The user is not found in the internal users identity store
- 15013 Selected Identity Source - All\_AD\_Join\_Points
- 24430 Authenticating user against Active Directory - All\_AD\_Join\_Points
- 24325 Resolving identity - jsmith (Step latency=7106 ms)
- 24313 Search for matching accounts at join point -
- 24319 Single matching account found in forest -
- 24313 Search for matching accounts at join point - windows\_ad\_server.com
- 24366 Skipping unjoined domain - Windows\_AD\_Server.com
- 24323 Identity resolution detected single matching account
- 24343 RPC Logon request succeeded - jsmith
- 24402 User authentication against Active Directory succeeded - All\_AD\_Join\_Points
- 22037 Authentication Passed
- 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 24432 Looking up user in Active Directory -
- 24355 LDAP fetch succeeded -
- 24416 User's Groups retrieval from Active Directory succeeded -
- 15048 Queried PIP - ExternalGroups
- 15016 Selected Authorization Profile - PermitAccess
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

Location	All Locations
NAS IPv4 Address	0.0.0.0
NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	7294 milliseconds

**Other Attributes**

ConfigVersionId	257
DestinationPort	1812
Protocol	Radius
NAS-Port	28672
Tunnel-Client-Endpoint	(tag=0)
CVPN3000/ASA/PIX7x-Tunnel-Group-Name	FTDAnyConnectVPN
OriginalUserName	jsmith
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	3
AcsSessionID	corbinise/322344084/1870108
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Allow ASA VPN connections if AD Group VPNusers
CPMSessionID	00000000000070005bbc08c3

CPMSessionID	00000000000070005bbc08c3
ISEPolicySetName	VPN Users
IdentitySelectionMatchedRule	Default
StepLatency	14=7106
AD-User-Resolved-Identities	jsmith@cohadley3.local
AD-User-Candidate-Identities	jsmith@cohadley3.local
AD-User-Join-Point	COHADLEY3.LOCAL
AD-User-Resolved-DNs	CN=John Smith,CN=Users,DC=cohadley3,DC=local
AD-User-DNS-Domain	cohadley3.local

AD-User-NetBios-Name	COHADLEY3
IsMachineIdentity	false
UserAccountControl	66048
AD-User-SamAccount-Name	jsmith
AD-User-Qualified-Name	jsmith@cohadley3.local
DTLS Support	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
ExternalGroups	S-1-5-21-872014162-156988481-842954196-1121
IdentityAccessRestricted	false
RADIUS Username	jsmith
Device IP Address	
Called-Station-ID	
CiscoAVPair	audit-session-id=00000000000070005bbc08c3, ip:source-ip= coa-push=true

## AnyConnect VPN-client

DART-bundel

[Hoe de DART-bundel voor AnyConnect wordt verzameld](#)

## Problemen oplossen

### DNS

Controleer Cisco ISE, FTD, Windows Server 2012 en Windows/Mac PCs kunnen elk ander vooruit- en achteruit oplossen (controleer DNS op alle apparaten)

Windows PC

Start een opdrachtmelding en zorg ervoor dat u een 'nslookup' kunt uitvoeren op de hostnaam van de FTD

## FTD CLI

```
>show network
```

```
> nslookup 192.168.1.10
Server: 192.168.1.10
Address: 192.168.1.10#53
10.1.168.192.in-addr.arpa name = ciscoise.cisco.com
```

## ISE CLI:

```
ciscoise/admin# nslookup 192.168.1.20
Trying "20.1.168.192.in-addr.arpa"
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 56529
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;20.1.168.192.in-addr.arpa. IN PTR

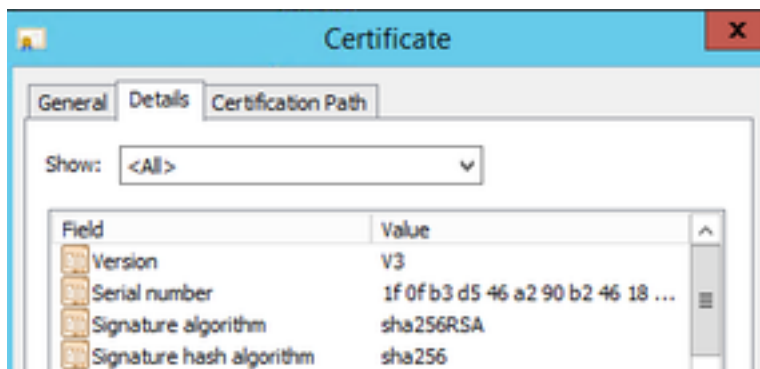
;; ANSWER SECTION:
20.1.168.192.in-addr.arpa. 1200 IN PTR ciscodc.cisco.com
```

## Windows Server 2012

Start een opdrachtmelding en zorg ervoor dat u een 'nslookup' kunt uitvoeren op de hostname/FQDN van de FTD

### certificaatsterkte (voor browser-compatibiliteit)

Controleer de Windows Server 2012-teken op certificaten als SHA256 of hoger. Dubbelklik in Windows op uw CA-certificaat en controleer de velden 'Signature algoritme'



Als zij SHA1 zijn, zullen de meeste browsers een browser waarschuwing voor deze certificaten tonen. U kunt deze functie hier wijzigen:

[Hoe u Windows Server-certificeringsinstantie voor upgrade naar SHA256 kunt upgraden](#)

Controleer of het VPN-servercertificaat van FTD de volgende velden correct heeft (wanneer u in browser aan FTD koppelt)

Algemene naam = <FTDFQDN>

Onderwerp Alternatieve naam (SAN) = <FTDFQDN>

Voorbeeld:

Vaak voorkomende naam: **ciscofp3.cisco.com**

Onderwerp Alternatieve naam (SAN): **DNS-naam=cisco.fp3.cisco.com**

## Connectiviteit en firewallconfiguratie

Controleer met behulp van Captures op FTD CLI en Captures op PC met Wireshark om te controleren dat pakketten over TCP+UDP 443 naar de Outside IP van de FTD worden verzonden. Controleer dat die pakketten zijn afgeleid van het openbare IP-adres van de router van het startpunt van de werknemer

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
```

```
<now hit Connect on AnyConnect Client from employee PC>
```

```
ciscofp3# show cap
```

```
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153 bytes]
```

```
match ip any host 198.51.100.2
```

```
ciscofp3# show cap capin
```

```
2375 packets captured
```

```
1: 17:05:56.580994 198.51.100.2.55928 > 203.0.113.2.443: S 2933933902:2933933902(0) win 8192
```

```
2: 17:05:56.581375 203.0.113.2.443 > 198.51.100.2.55928: S 430674106:430674106(0) ack 2933933903 win 32768
```

```
3: 17:05:56.581757 198.51.100.2.55928 > 203.0.113.2.443: . ack 430674107 win 64240
```

```
...
```