

# Configure AnyConnect VPN en FTD usando Cisco ISE como servidor de RADIUS con el Servidor Windows 2012 raíz CA

## Contenido

[Contenido](#)

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Exporte certificado raíz CA del Servidor Windows](#)

[Instale certificado raíz CA encendido el empleado Windows/las PC del mac](#)

[Genere un CSR en FTD, consiga el CSR firmado por el Servidor Windows raíz CA, y instale ese certificado firmado en FTD](#)

[Descargue la imagen de AnyConnect + el editor del perfil de AnyConnect y cree un perfil .xml](#)

[Configure Anyconnect VPN en FTD \(utilice certificado raíz CA\)](#)

[Configure la regla FTD NAT para eximir el tráfico VPN del NAT puesto que será descifrado de todos modos y crear la directiva del control de acceso/las reglas](#)

[Agregue FTD como dispositivo de red y configure el conjunto de la directiva en Cisco ISE \(el secreto compartido del uso RADIUS\)](#)

[La transferencia directa, instala y conecta con el FTD usando el cliente de AnyConnect VPN en el empleado Windows/las PC del mac](#)

[Verificación](#)

[FTD](#)

[Cisco ISE](#)

[Cliente de AnyConnect VPN](#)

[Troubleshooting](#)

[DNS](#)

[Fuerza del certificado \(para la compatibilidad del buscador\)](#)

[Conectividad y configuración del Firewall](#)

## Contenido

## Introducción

Este documento describe cómo configurar AnyConnect VPN (Virtual Private Network) en un Firewall FTD (defensa de la amenaza de FirePOWER) usando Cisco ISE (Identity Services Engine) como servidor de RADIUS. Utilizamos a un Servidor Windows 2012 como nuestro raíz CA (autoridad de certificación) de modo que la comunicación sobre el VPN sea asegurada por los

Certificados es decir la PC del empleado confiará en el certificado del FTD porque el certificado FTD VPN ha sido firmado por nuestro Servidor Windows 2012 raíz CA

## Prerrequisitos

## Requisitos

Usted debe tener haber desplegado siguiente y ejecutarse en su red:

- Centro de administración de FirePOWER y Firewall de la defensa de la amenaza de FirePOWER desplegado con la conectividad básica
- Cisco ISE desplegado y que se ejecuta en su red
- Servidor Windows (con el Active Directory) desplegado y PC de Windows/del mac de los empleados unida al dominio del ANUNCIO (Active Directory)

En nuestro ejemplo abajo, los empleados abrirán al cliente de AnyConnect en su PC de Windows/del mac, y conectarán con seguridad con la interfaz exterior del FTD vía el VPN usando sus credenciales. El FTD controlará su nombre de usuario y contraseña contra Cisco ISE (que controlen con el Active Directory del Servidor Windows para verificar su username, la contraseña, y a los usuarios del grupo es decir solamente en el grupo “empleados” del ANUNCIO podrá al VPN en la red de la compañía.

## Componentes Utilizados

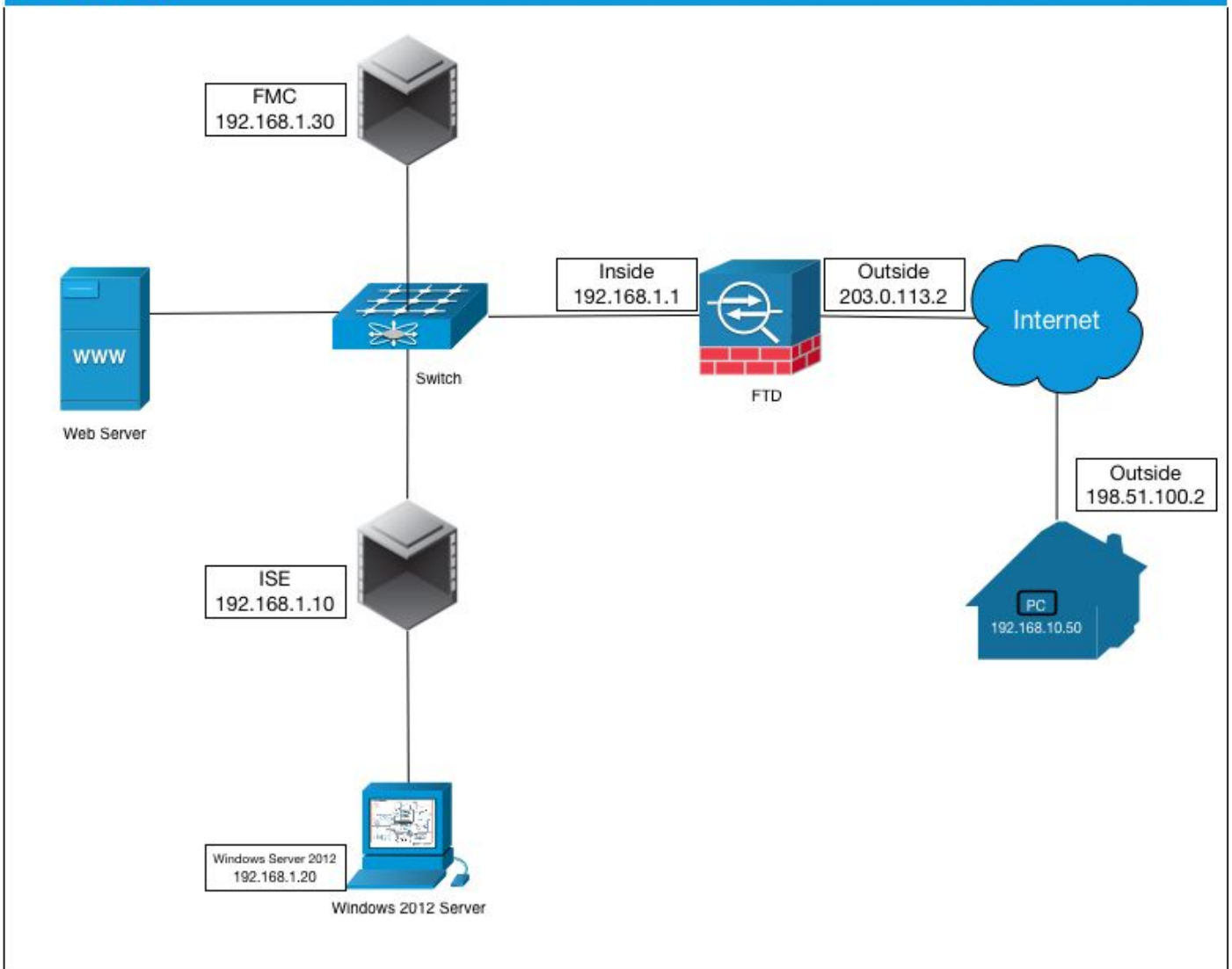
La información que contiene este documento se basa en estas versiones de software:

- Centro de administración de FirePOWER y defensa de la amenaza de FirePOWER que ejecuta 6.2.3
- Cisco Identity Services Engine que ejecuta 2.4
- Cliente de movilidad Cisco AnyConnect Secure que ejecuta 4.6.03049
- Servicios corrientes del Active Directory R2 y del certificado del Servidor Windows 2012 (éste es nuestro raíz CA para todos los Certificados)
- Windows 7, Windows 10, PC del mac

## Configurar

### Diagrama de la red

## Topology



En este caso del uso, la PC de Windows del empleado/del mac que funciona con al cliente de Anyconnect VPN conectará con la dirección IP pública exterior del Firewall FTD, y Cisco ISE los concederá dinámicamente limitó o acceso total a cierto interno o a los recursos de Internet (configurables) una vez que están conectados vía el VPN dependiendo de qué grupo del ANUNCIO son un miembro en del Active Directory

Dispositivo	Hostname/FQDN	Dirección IP pública	Dirección IP privada	Dirección IP de AnyConnect
PC de Windows	-	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	-
Servidor Windows 2012	ciscodc.cisco.com	-	192.168.1.20	-
Servidores internos	-	-	192.168.1.x	-

## Configuración

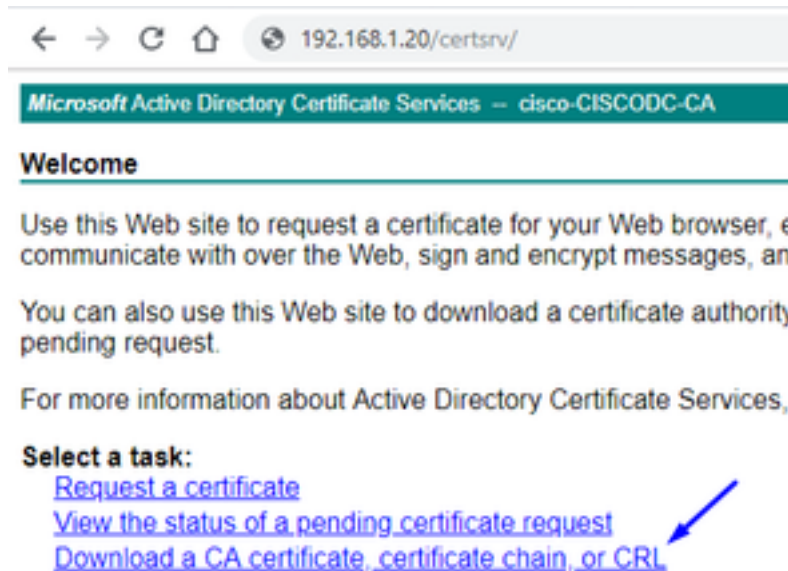
### Exporte certificado raíz CA del Servidor Windows

En este documento, utilizaremos el servidor 2012 de Microsoft Windows como nuestros raíz CA

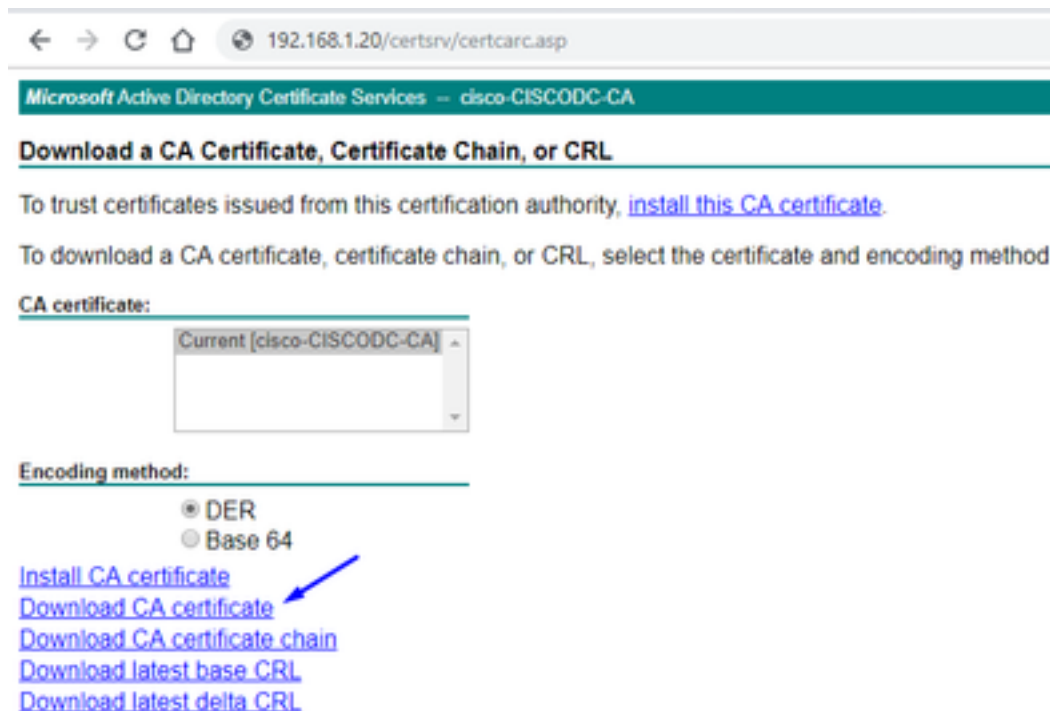
para los Certificados. La confianza de la voluntad De la PC del cliente esto raíz CA a conectar con seguridad con el FTD vía el VPN (véase los pasos abajo). Esto se asegurará de que puedan conectar con seguridad con el FTD sobre los recursos internos de Internet y del acceso del hogar. Su PC confiará en la conexión en su navegador y cliente de AnyConnect.

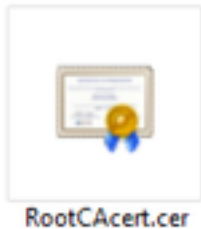
Vaya a <http://192.168.1.20/certsrv> y siga los pasos abajo para descargar a su Servidor Windows certificado raíz CA:

Haga clic la **transferencia directa un certificado CA, una Cadena de certificados, o un CRL**



Haga clic el **certificado de la transferencia directa** y retítúlelo a 'RootCAcert3.cer'





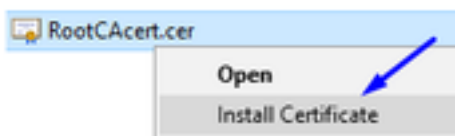
Instale certificado raíz CA encendido el empleado Windows/las PC del mac

**Método 1:** Instale el certificado en toda la PC del empleado empujándola vía la directiva del grupo de Servidor Windows (ideal para cualquier cosa sobre 10 usuarios de VPN):

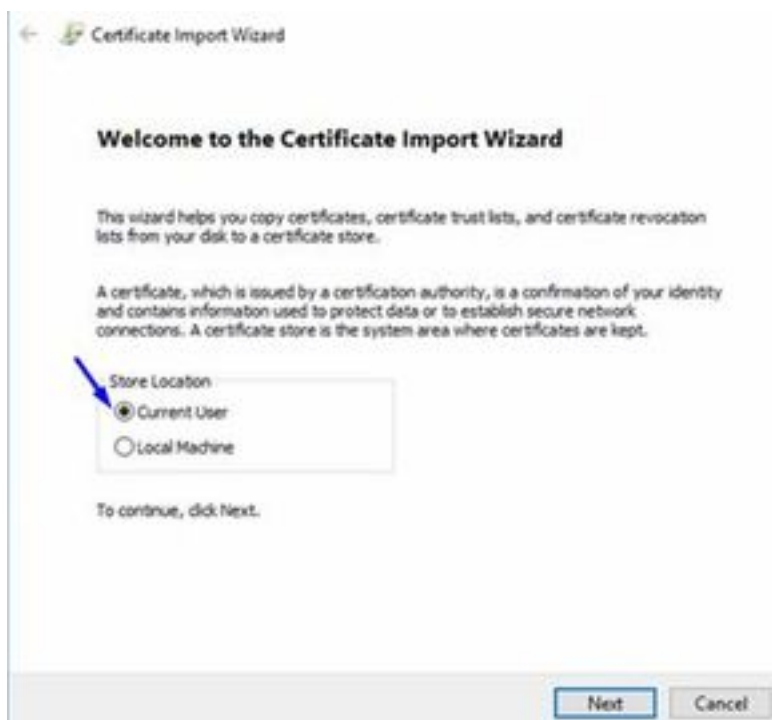
[Cómo utilizar al Servidor Windows para distribuir los Certificados a las computadoras cliente usando la directiva del grupo](#)

**Método 2:** Instale el certificado en toda la PC del empleado instalandola individualmente en cada PC (ideal probar a un usuario de VPN):

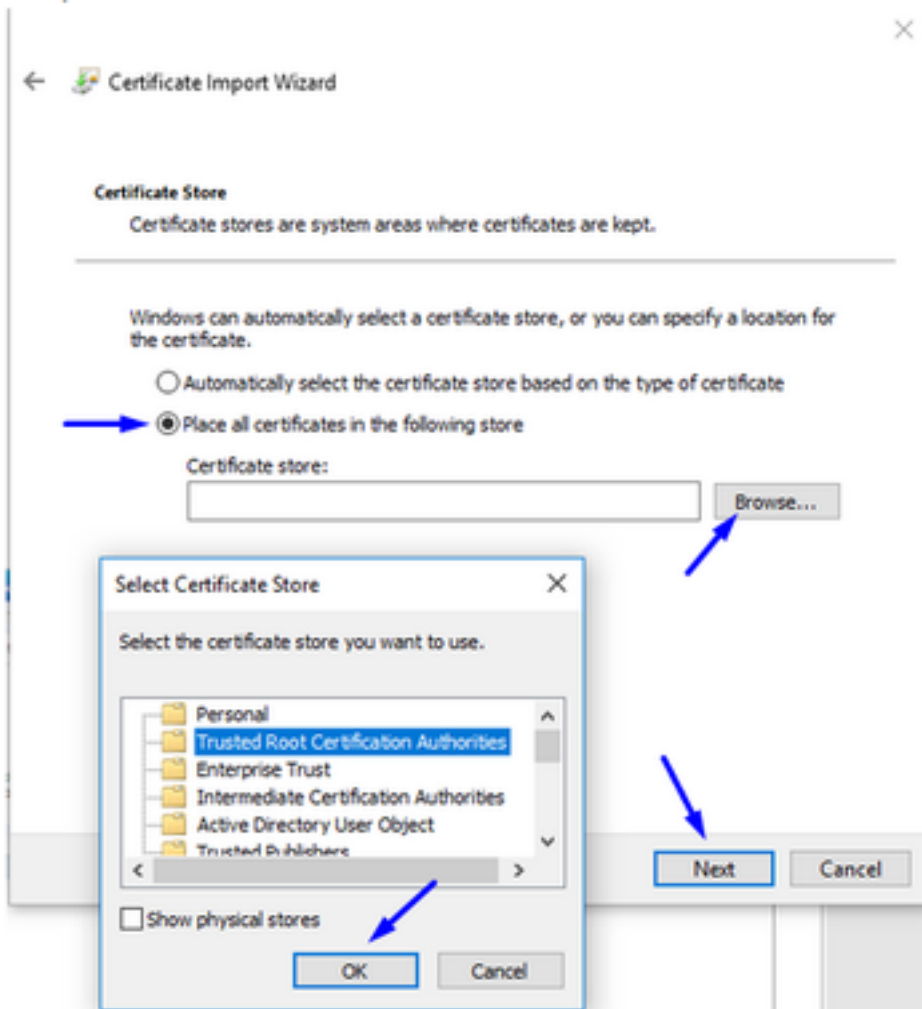
Haga clic derecho el certificado en la PC de Windows/del mac de sus empleados y el tecleo **instala el certificado**



Seleccione al "Usuario usuario actual"

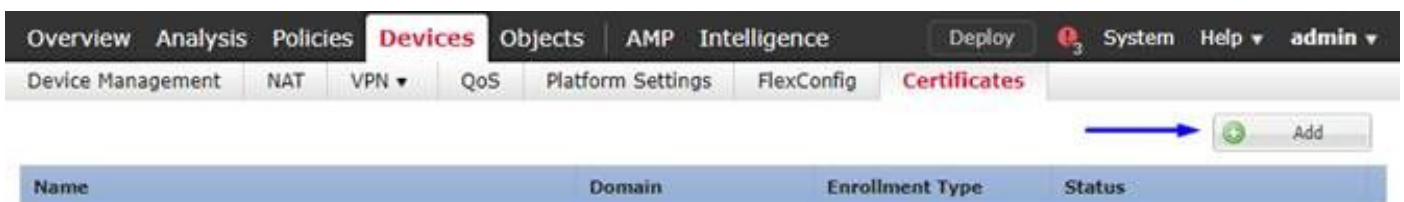


Seleccione el **lugar todos los Certificados en el almacén siguiente** y los **Trusted Root Certification Authority** selectos, hacen clic la **autorización**, el tecleo **después**, y el clic en **Finalizar**



Genere un CSR en FTD, consiga el CSR firmado por el Servidor Windows raíz CA, y instale ese certificado firmado en FTD

Vaya a los objetos > a la Administración del objeto > a PKI > a la inscripción CERT, haga clic en agregan la inscripción CERT



El tecleo **agrega** el botón de la inscripción CERT

**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

Seleccione el **tipo** > el **manual de la inscripción**

Como se ve en la imagen abajo, necesitamos pegar nuestro certificado raíz CA aquí:

**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

Aquí es cómo descargar su certificado raíz CA, lo ve en el formato de texto, y lo pega en el cuadro arriba:

Vaya a <http://192.168.1.20/certsrv>

Haga clic la **transferencia directa un certificado CA**, una **Cadena de certificados**, o un **CRL**

← → ↻ 🏠 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](#)

Haga clic el botón del base 64 > el certificado CA de la transferencia directa del teclado

← → ↻ 🏠 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

Abra el fichero de RootCAcertBase64.cer en la libreta

La copia y pega el contenido de .cer (certificado raíz CA) del servidor del ANUNCIO de Windows aquí:



## Add Cert Enrollment



Name: \*

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: \* 

```
QgIZR0KCRWERA8INZPIHQWCWTDVK0PBRQDAGGDMR6GR10UEW
EB/wQFMAMBAf8wHQYD
VR00BBYEF0lpC7y9musCkmDJaKVus9bJUoMIMBAGCSsGAQQBg
jcVAQQDAgEBMCMG
CSsGAQQBgjcVAgQWBBQXIqPq2/dCT41fyYZHPxKhGEYNnzANBg
kqhkiG9w0BAQsF
AAOCAQEAOTaS58Zw7RfarjTGm7HHJHZsA2p9CHdsvB/I35nYeqc
OnxyeTWFN7by6
C43uyBFTWTPu3LJjr1mCgEo72qJErJOoU/Y4y7ADAKJF8RtUIb4H
Zq13XNW7Tu9X
DbZCTeYL7INbzZxPyfcuZWIBk5I8uHRvqq2YkBdx6YUYJocNTshH
WwZIXYvQPwwc
yjHrFjm0/YIQIJMhyIVULXXxWGP7diLIEQ67aHsdz+UZq9JofVYa
heHBjzbzIF
zvN2WWFXQs3mFMUxkrjEyzNIDws6vrm6ZhqvOupzmeC6YqByK
QIEAggjevemL7Zd
8DufTZQ4E4VQ9Kp4hrSdzuHSggDTuw==
-----END CERTIFICATE-----
```

Allow Overrides:

Haga clic la tabulación >> el tipo de los **parámetros del certificado** su información del certificado

Nota:

El campo de encargo FQDN debe ser el FQDN de su FTD

El campo de nombre común debe ser el FQDN de su FTD

## 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

Consejo: usted puede conseguir el FQDN de su FTD pulsando el comando siguiente del FTD CLI:

```
> 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
```

La tabulación **dominante** del teclado y pulsa cualquier nombre de la clave

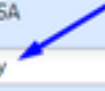
**Add Cert Enrollment** ? X

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


### Salvaguardia del teclado

Seleccione su FTDVPNServerCert que acabamos de crear arriba y el tecleo **agrega**

**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

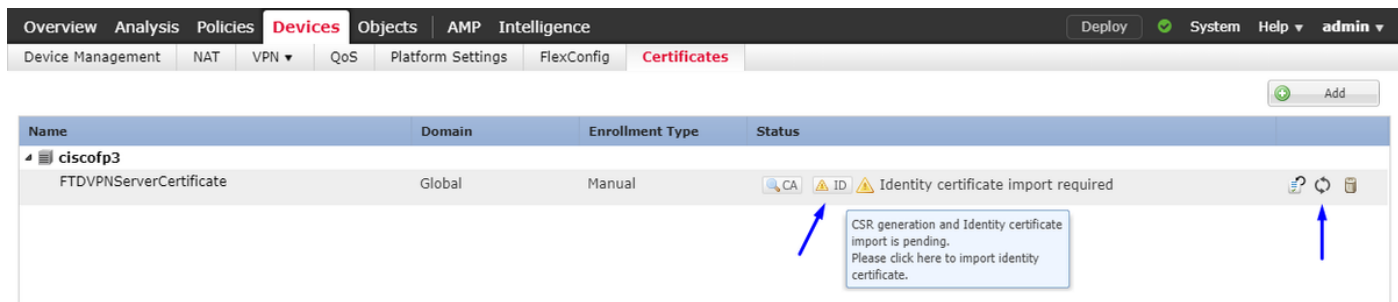
Enrollment Type: Manual

SCEP URL: NA

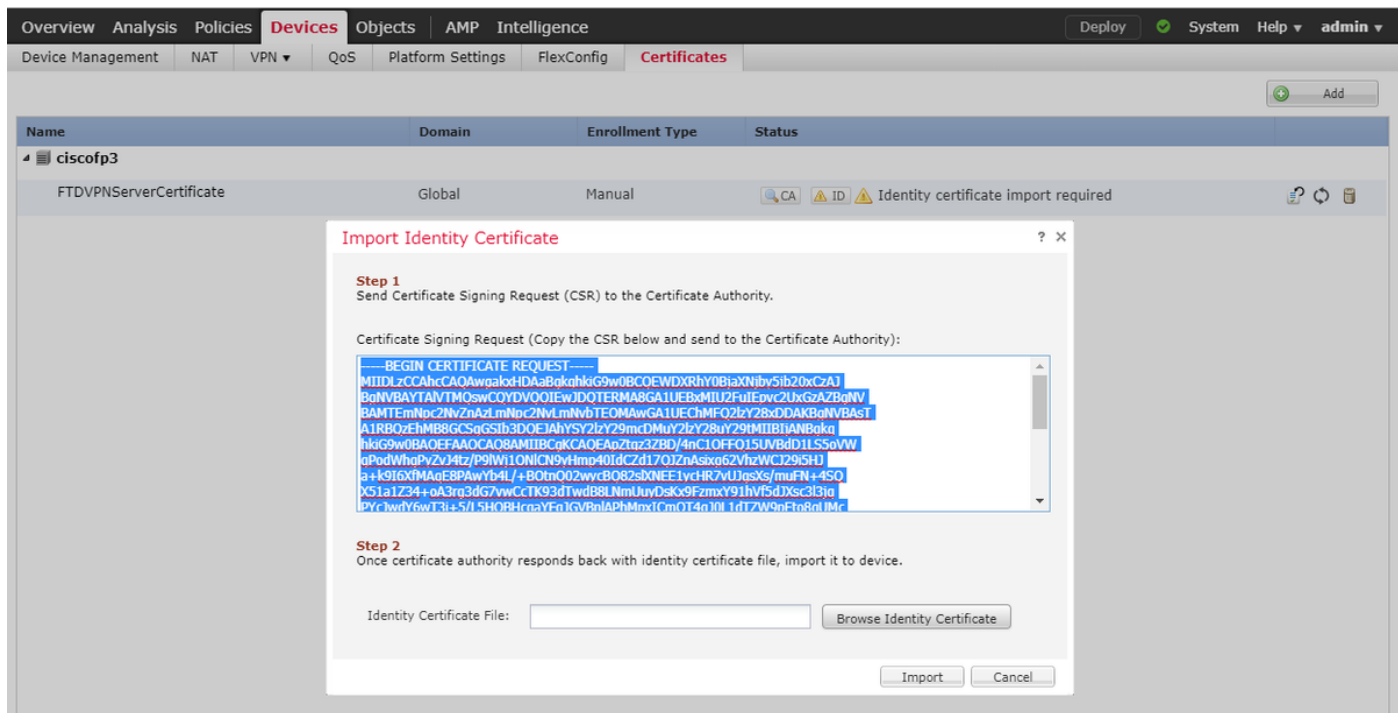


Consejo: Espere cerca de 10-30 segundos FMC + FTD para verificar y para instalar certificado raíz CA (el tecleo restaura el icono si no lo hace demostración)

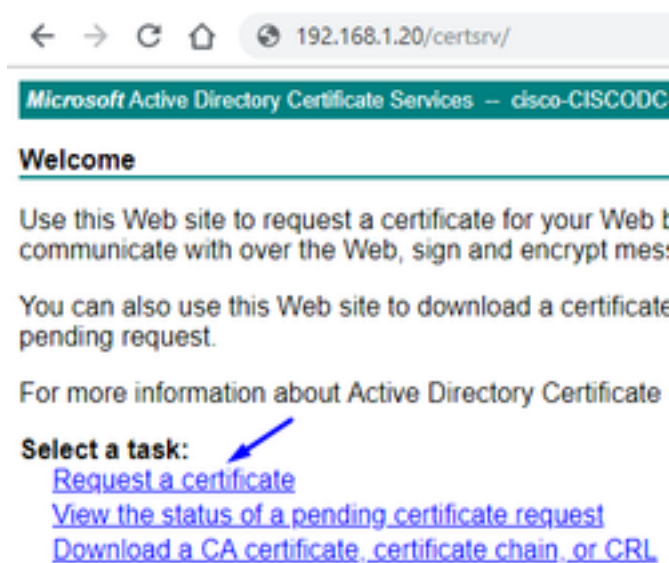
Haga clic el botón **identificación**:



La copia y pega este CSR, y lo lleva su Servidor Windows raíz CA:



Vaya a <http://192.168.1.20/certsrv>



Haga clic la **solicitud de certificado avanzada**

← → ↻ 🏠 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](#).

Pegue su pedido de firma de certificado (CSR) en el campo abajo y seleccione al **servidor Web** como el Certificate Template plantilla de certificado

← → ↻ 🏠 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/YlIQI7jMhyIVULXXxwGP7diLlEQ67.
zvN2wMFXQs3mFMUxkrjEyzNlDws6vrm6Zhaiv0
8DuFTZQ4E4VQ9Kp4hrSdzuh5ggDTuw==
-----END CERTIFICATE-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >


El tecleo **somete**

Haga clic el botón **codificado base 64** y haga clic el **certificado de la transferencia directa**

### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)





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

AUTORIZACIÓN y File (Archivo) > Save as (Guardar como) del tecleo...

VPNprofile.xml

Descargue las imágenes de Windows y del mac .package de [aquí](#)

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		

Vaya a los **objetos** > a la **Administración del objeto** > al **VPN** > al **fichero** > al tecleo de **AnyConnect** agregan el fichero de AnyConnect

**Edit AnyConnect File** ? x

Name: \*

File Name: \*

File Type: \*  v

Description:

**Add AnyConnect File** ? x

Name: \*

File Name: \*

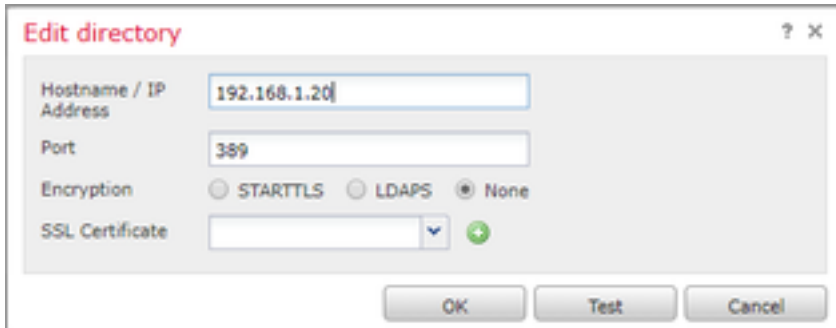
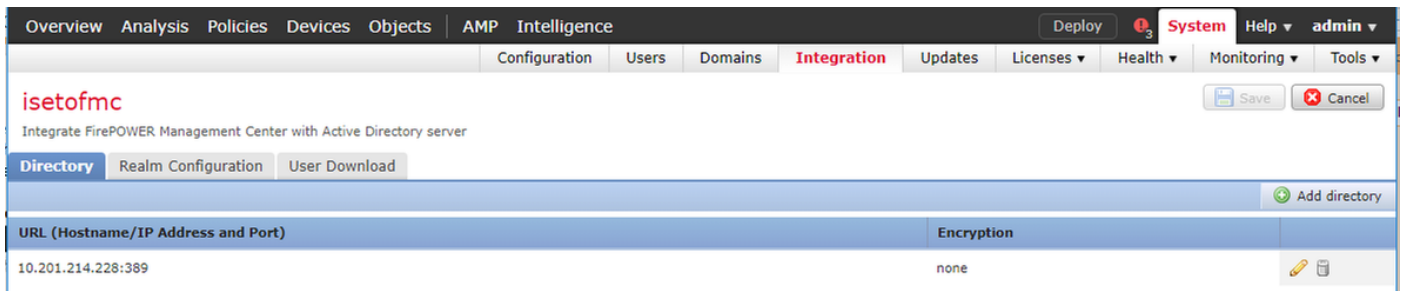
File Type: \*  v

Description:

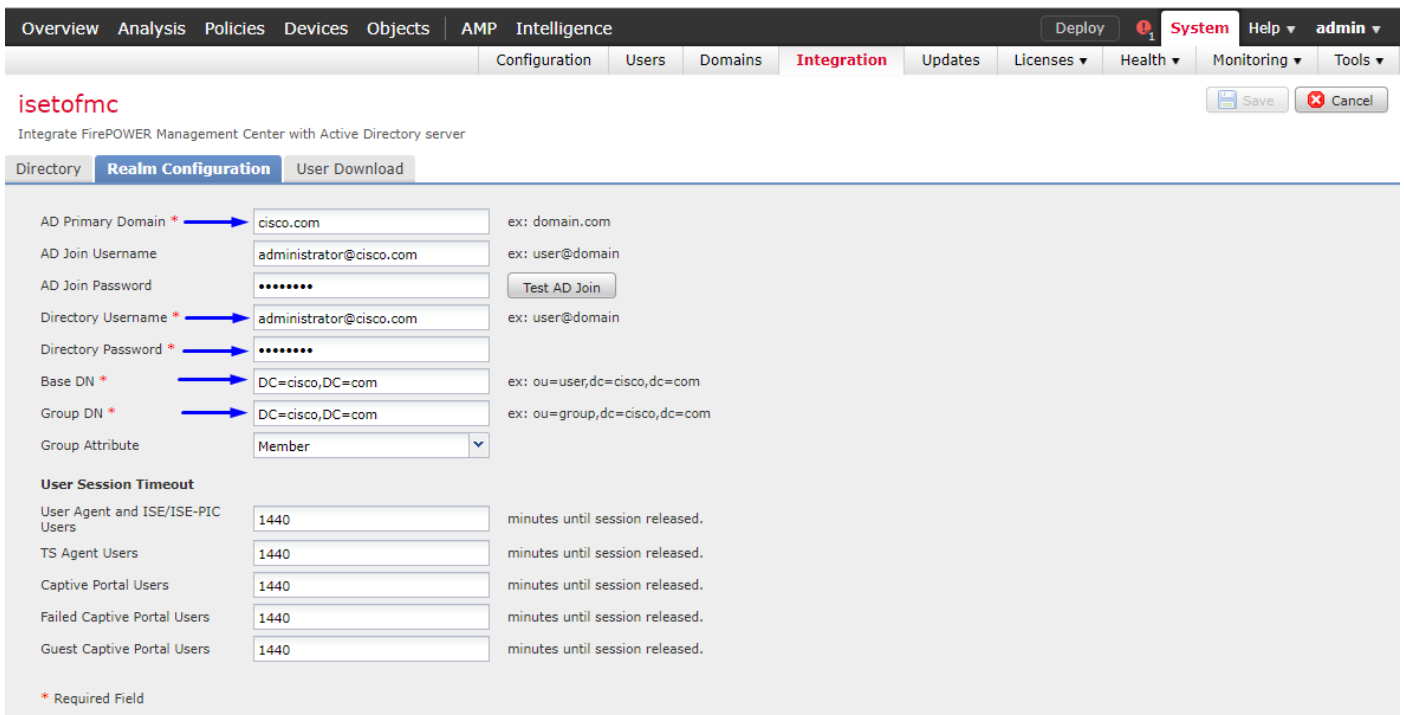
Configure Anyconnect VPN en FTD (utilice certificado raíz CA)

Ábrase una sesión al **centro de administración de FirePOWER**  
El sistema del tecleo > la **integración** > los **reinos** > reino del tecleo el nuevos >> **ficha de directorio del tecleo** > tecleo **agregan el directorio**





Tabulación de la **configuración del reino del teclado** - configure la información de su regulador del dominio aquí



Nota: En el ejemplo antedicho, un username del ANUNCIO con “los privilegios Admin del dominio” en el servidor del ANUNCIO de Windows se utiliza. Si usted quiere configurar a un usuario con permisos más específicos, más mínimos para que el FMC se una a su dominio de Active Directory para su configuración del reino, usted puede ver los pasos [aquí](#)

Tabulación de la **transferencia directa del usuario del teclado** - asegúrese de que transferencia directa del usuario tenga éxito

The screenshot shows the 'User Download' configuration page in the FirePOWER Management Center. The page is titled 'isetofmc' and includes a navigation menu with 'Directory', 'Realm Configuration', and 'User Download'. A 'Download Now' button is highlighted with a blue arrow. Below it, there are fields for 'Begin automatic download at' (8 PM, America/New York) and 'Repeat Every' (24 Hours). A list of 'Available Groups' is shown, including 'Enterprise Admins', 'Hyper-V Administrators', and 'Users'. There are also sections for 'Groups to Include (0)' and 'Groups to Exclude (0)'. A notification box in the top right corner indicates a successful LDAP download: 'LDAP Download', 'Download users/groups from isetofmc', 'LDAP download successful: 51 groups, 25 users download'.

Los dispositivos del teclado > el VPN > el Acceso Remoto > el teclado agregan

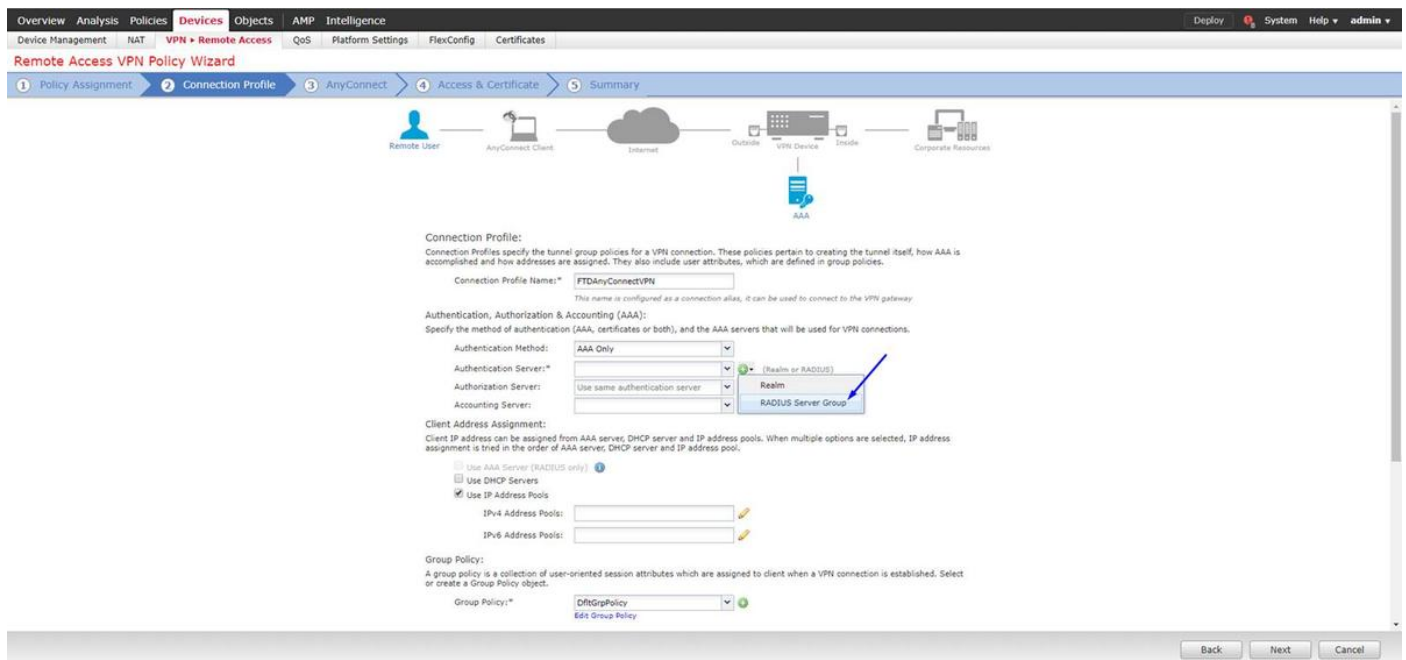
The screenshot shows the 'VPN Remote Access' configuration page in the FirePOWER Management Center. The page is titled 'VPN Remote Access' and includes a navigation menu with 'Device Management', 'NAT', 'VPN Remote Access', 'QoS', 'Platform Settings', 'FlexConfig', and 'Certificates'. A table with columns for 'Name', 'Status', and 'Last Modified' is shown, with the text 'No configuration available' and a link to 'Add a new configuration'. An 'Add' button is highlighted with a blue arrow.

Pulse un nombre, descripción, y el teclado agrega para seleccionar el dispositivo FTD en el cual usted quiere configurar Anyconnect VPN

The screenshot shows the 'Remote Access VPN Policy Wizard' configuration page in the FirePOWER Management Center. The page is titled 'Remote Access VPN Policy Wizard' and includes a navigation menu with 'Policy Assignment', 'Connection Profile', 'AnyConnect', 'Access & Certificate', and 'Summary'. The 'AnyConnect' step is selected. The page includes a 'Name' field with the value 'FTDAnyConnectVPN', a 'Description' field with the value 'AnyConnect VPN configuration for this FTD', and a 'Targeted Devices' section with 'Available Devices' and 'Selected Devices' lists. The 'Selected Devices' list contains the IP address '10.201.214.134'. A 'Before You Start' section provides additional configuration instructions.

Haga clic agrega para el servidor de la autenticación y elige al grupo de servidor de RADIUS -

éste será su PSN del Cisco Identity Services Engine (la directiva mantiene el nodo)



Pulse un **nombre** para el servidor de RADIUS

Seleccione su **reino** configurado arriba

El tecleo **agrega**

### 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: isetofmc

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
No records to display

Save Cancel

Pulse la siguiente información para su nodo de Cisco ISE:

**Dirección IP/hostname:** La dirección IP de PSN de Cisco ISE (nodo del servicio de la directiva) -

esto es donde irán las peticiones de la autenticación

Clave: cisco123

**Confirme la clave:** cisco123

**Precaución:** el antedicho es su clave secreta compartida RADIUS - utilizaremos esta clave en un paso posterior

**Edit RADIUS Server** ? x

IP Address/Hostname: \* 192.168.1.10  
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port: \* 1812 (1-65535)

Key: \* .....

Confirm Key: \* .....

Accounting Port: 1813 (1-65535)

Timeout: 10 (1-300) Seconds

Connect using:  Routing  Specific Interface ⓘ

Redirect ACL:

Save Cancel

Nota: Cuando el usuario final intenta conectar con el FTD vía AnyConnect VPN, el username + la contraseña que pulsán serán enviados como petición de la autenticación a este FTD. El FTD transmitirá a esa petición el nodo PSN de Cisco ISE para la autenticación (Cisco ISE entonces controlará el Active Directory de Windows para saber si hay ese nombre de usuario y contraseña, y aplica el control de acceso/el acceso a la red dependiendo de la condición que hemos configurado actualmente en Cisco ISE)

## 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

## Salvaguardia del teclado

El teclado corrige para el pool del direccionamiento IPv4

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: FTDAnyConnectVPN  
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: [ ]

IPv6 Address Pools: [ ]

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

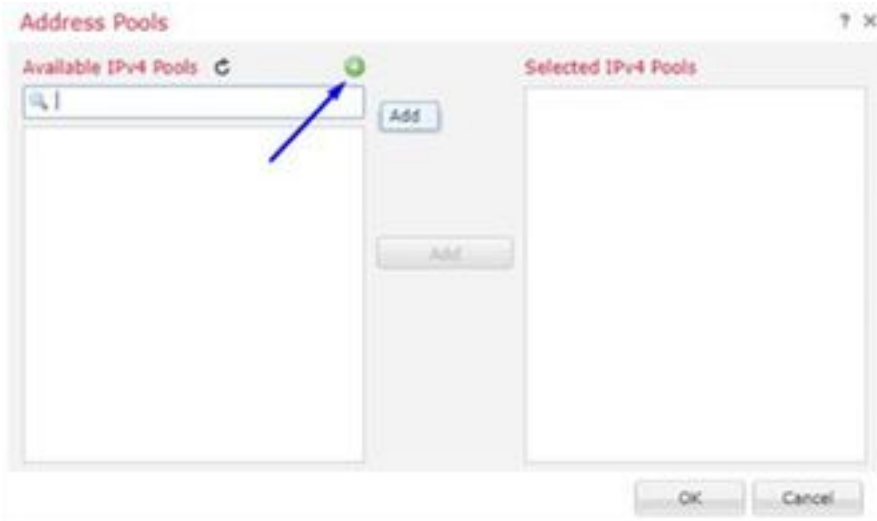
Group Policy: DftGrpPolicy (Edit Group Policy)

Back Next Cancel

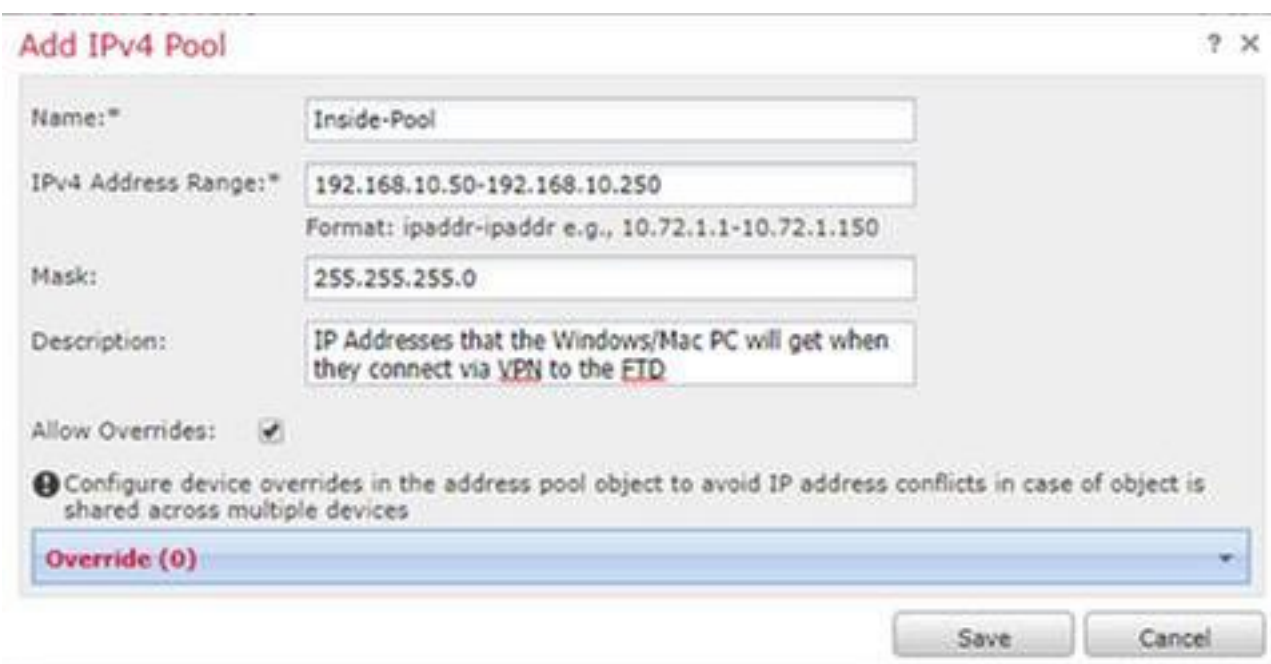
Last login on Wednesday, 2018-10-10 at 10:30:14 AM from 10.152.21.157

How-To Cisco

El teclado agrega

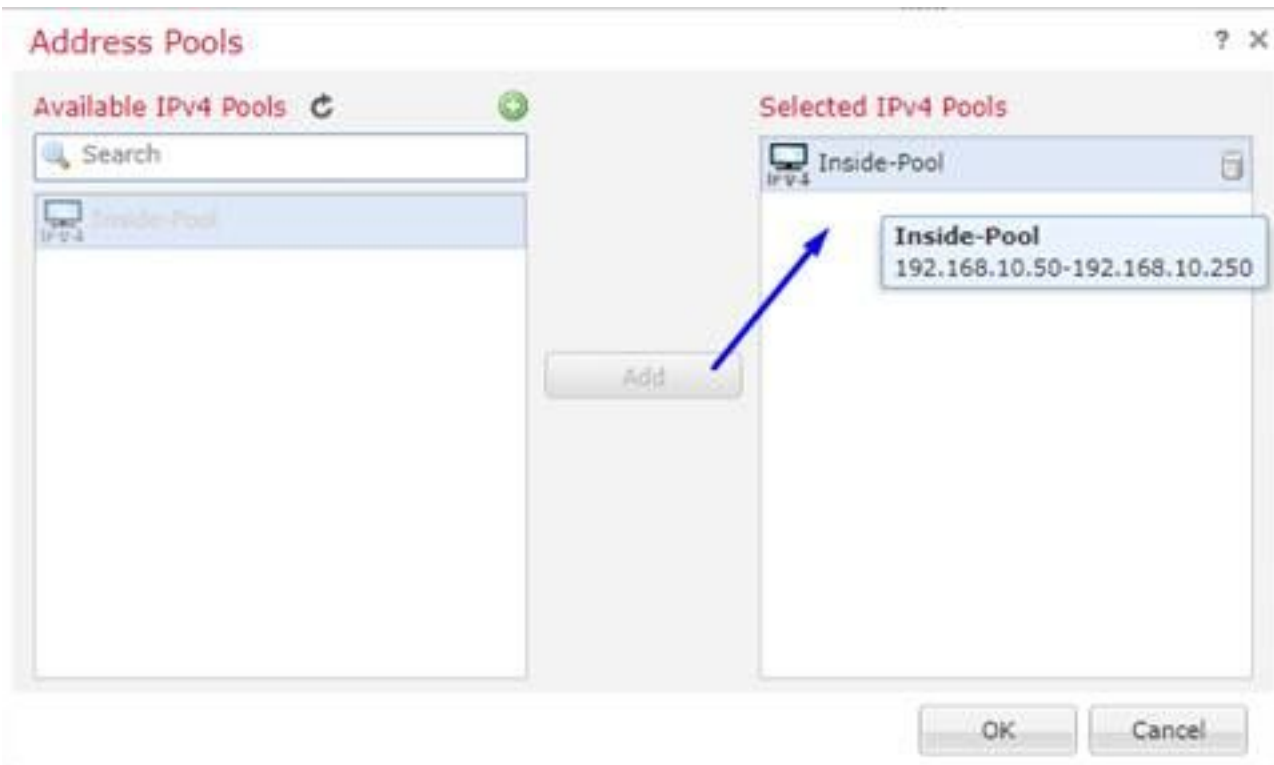


Pulse un rango del nombre, de direccionamiento IPv4, y máscara de subred

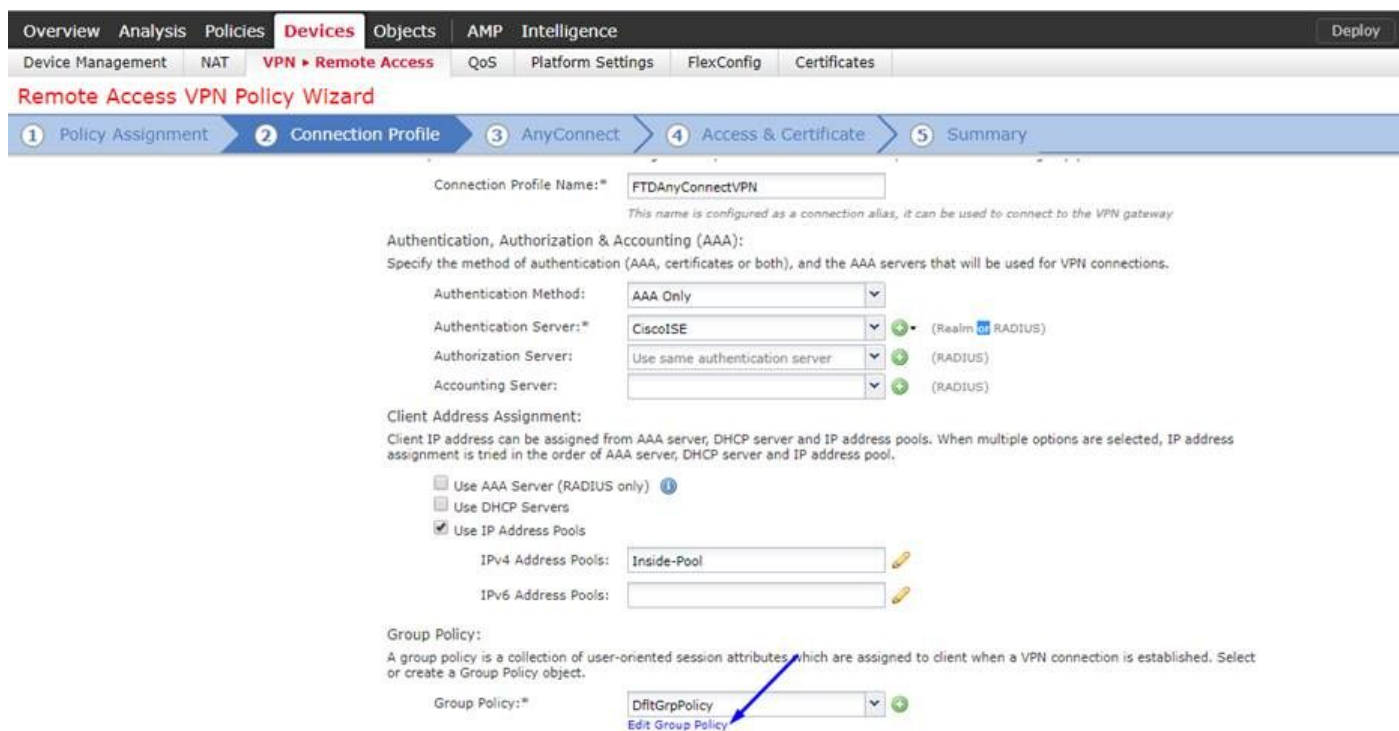


Seleccione su pool de la dirección IP y haga clic la **autorización**





El tecleo corrige la directiva del grupo



La tabulación > los perfiles > el tecleo de Anyconnect del tecleo agregan

## 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.

Pulse un **nombre** y el teclado **hojea...** y selecciona su fichero VPNprofile.xml del paso 4 antedicho

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

**Salvaguardia del teclado y teclado después**

Seleccione los checkboxes para su fichero de AnyConnect Windows/del mac del paso 4 antedicho



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](#). Show Re-order buttons

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyConnect_Mac_4.603049	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

Haga clic después  
 Seleccione la **zona del grupo de interfaces/Seguridad** como **exterior**  
 Seleccione la **inscripción del certificado** como su certificado que hicimos en el paso 3 antedicho

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:  Show Re-order buttons  
 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

Revise su configuración y haga clic **después**

**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: DftGrpPolicy

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 CA 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.

Buttons: Back, Finish, Cancel

Configure la regla FTD NAT para eximir el tráfico VPN del NAT puesto que será descifrado de todos modos y crear la directiva del control de acceso/las reglas

Cree una regla NAT estática para asegurarse de que el tráfico VPN no consigue NAT'd (FTD descifra ya los paquetes de AnyConnect mientras que vienen a la interfaz exterior, así que es como si esa PC esté ya detrás de la interfaz interior, y tienen ya una dirección IP privada - todavía necesitamos configurar una regla Nacional-exenta (Ninguno-NAT) para ese tráfico VPN):  
Vaya a los objetos > al teclado agregan la red > el teclado agregan el objeto

**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:

Buttons: Save, Cancel

### Edit Network Objects ? X

Name:

Description:

Network:

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

Allow Overrides:

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

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Example\_Company\_NAT\_Policy NAT policy Save Cancel

Policy Assignments (1) Add Rule

#	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									

Además, usted debe permitir que el tráfico de datos fluya después del usuario VPN adentro. Usted tiene dos opciones para esto:

- Cree permiten o niegan las reglas para permitir que o nieguen los usuarios de VPN tengan acceso a ciertos recursos
- Active “la directiva del control de acceso de puente para el tráfico descriptado” - esto deja a cualquier persona que pueda conectar con éxito con el FTD vía puente ACL VPN y el acceso que cualquier cosa detrás del FTD sin ir permite o que niega a través las reglas en la directiva del control de acceso

Active la **directiva del control de acceso de puente para el tráfico descriptado** debajo: **Dispositivos > VPN > Acceso Remoto > perfil > interfaces de acceso VPN:**

#### Access Control for VPN Traffic

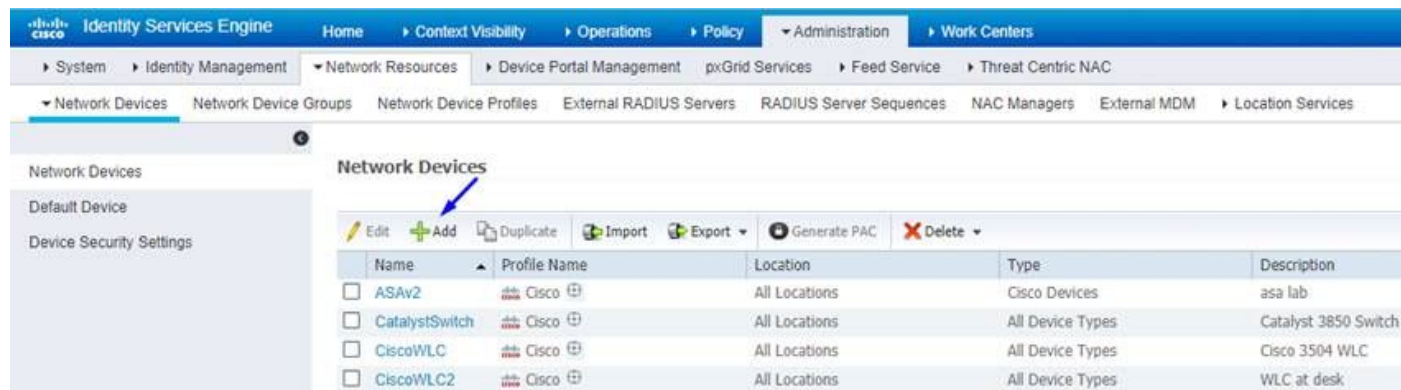
- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**  
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Nota: Si usted no activa esta opción, usted necesitará ir a las **directivas > a la directiva del control de acceso** y crear permita que las reglas para que los usuarios de VPN puedan tener acceso a las cosas detrás interiores o al dmz

ClickDeployin la esquina superior derecha del centro de administración de FirePOWER

**Agregue FTD como dispositivo de red y configure el conjunto de la directiva en Cisco ISE (el secreto compartido del uso RADIUS)**

Ábrase una sesión al Cisco Identity Services Engine y la **administración** > los **dispositivos de red** > el tecleo del tecleo **agregan**



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, there are sub-menus for System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The Network Resources menu is expanded, showing Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The Network Devices page is active, displaying a table of network devices. The 'Add' button is highlighted with a blue arrow.

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

Pulse un **nombre**, pulse la **dirección IP** de su FTD, y pulse su **secreto compartido RADIUS** de los pasos arriba

Precaución: Éste debe ser el interfaz/el IP address hacia fuera que el FTD puede alcanzar su Cisco ISE (servidor de RADIUS) es decir el interfaz FTD sobre el cual su Cisco ISE puede alcanzar el FTD

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

Default Device.

Device Security Settings.

\* 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

La directiva del teclado > la directiva fija > crean un conjunto de la directiva para cualquier autenticación pide que venido adentro del siguiente tipo:

### El Radio-NAS-puerto-tipo IGUALA virtual

Esto significa si algunos pedidos de RADIUS que entren en ISE que parezcan las conexiones VPN, ellos golpean este conjunto de la directiva

Identity Services Engine Administration Work Centers License Warning

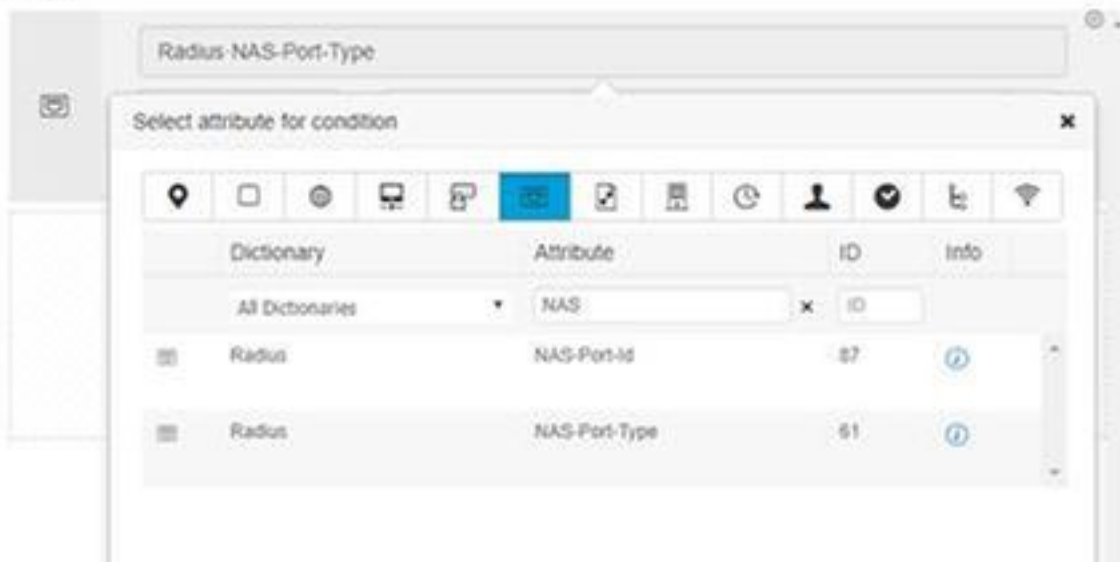
Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✔	GuestSSID		Airspace Airspace-Wlan-Id EQUAL S 1	Default Network Access	181	<input type="button" value="⊖"/> <input type="button" value="⊕"/>	<input type="button" value="⚙"/> <input type="button" value="➔"/>
	✔	EmployeeSSID		Airspace Airspace-Wlan-Id EQUAL S 2	Default Network Access	686	<input type="button" value="⊖"/> <input type="button" value="⊕"/>	<input type="button" value="⚙"/> <input type="button" value="➔"/>
	✔	Users		Radius-NAS-Port-Type EQUALS Virtual	Default Network Access		<input type="button" value="⊖"/> <input type="button" value="⊕"/>	<input type="button" value="⚙"/> <input type="button" value="➔"/>
	✔	Default	Default policy set		Default Network Access	1380	<input type="button" value="⊖"/> <input type="button" value="⊕"/>	<input type="button" value="⚙"/> <input type="button" value="➔"/>

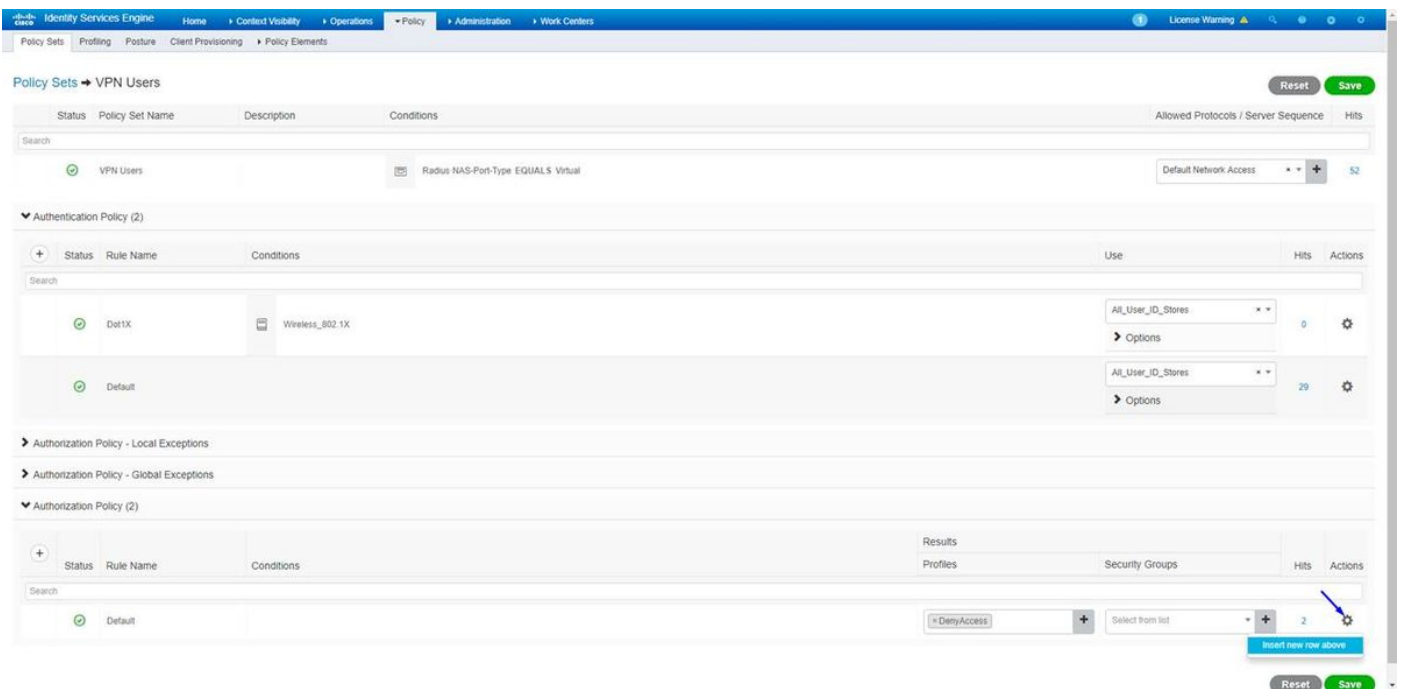
Aquí es donde usted puede encontrar esa condición en Cisco ISE:

## Editor



Corrija la **directiva le fijan** creado arriba

Agregue una regla sobre la regla de bloques de valor por defecto para dar del “el perfil de la autorización **acceso del permiso**” de la gente solamente si están en el grupo del Active Directory llamado los “**empleados**”:



Abajo es cómo su regla parecerá una vez completa



The screenshot displays the Cisco ISE Policy Sets configuration interface. The main table shows the following data:

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

Below this, the 'Authentication Policy (2)' section contains a table of rules:

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

The 'Authorization Policy - Local Exceptions' and 'Authorization Policy - Global Exceptions' sections are currently empty. The 'Authorization Policy (2)' section contains a table of rules:

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

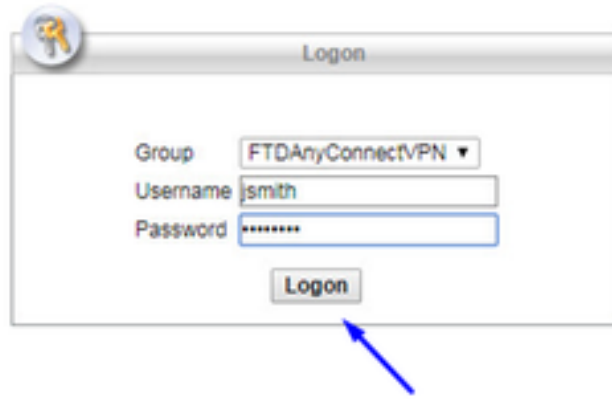
Two blue arrows in the image point to the 'Conditions' column of the 'Allow FTD VPN connections if AD Group VPNUsers' rule and the 'Results' column of the same rule.

La transferencia directa, instala y conecta con el FTD usando el cliente de AnyConnect VPN en el empleado Windows/las PC del mac

Abra a su navegador en el empleado Windows/la PC del mac, y vaya a la dirección externa de su FTD en su navegador

← → ↻ <https://cisconfp3.cisco.com>

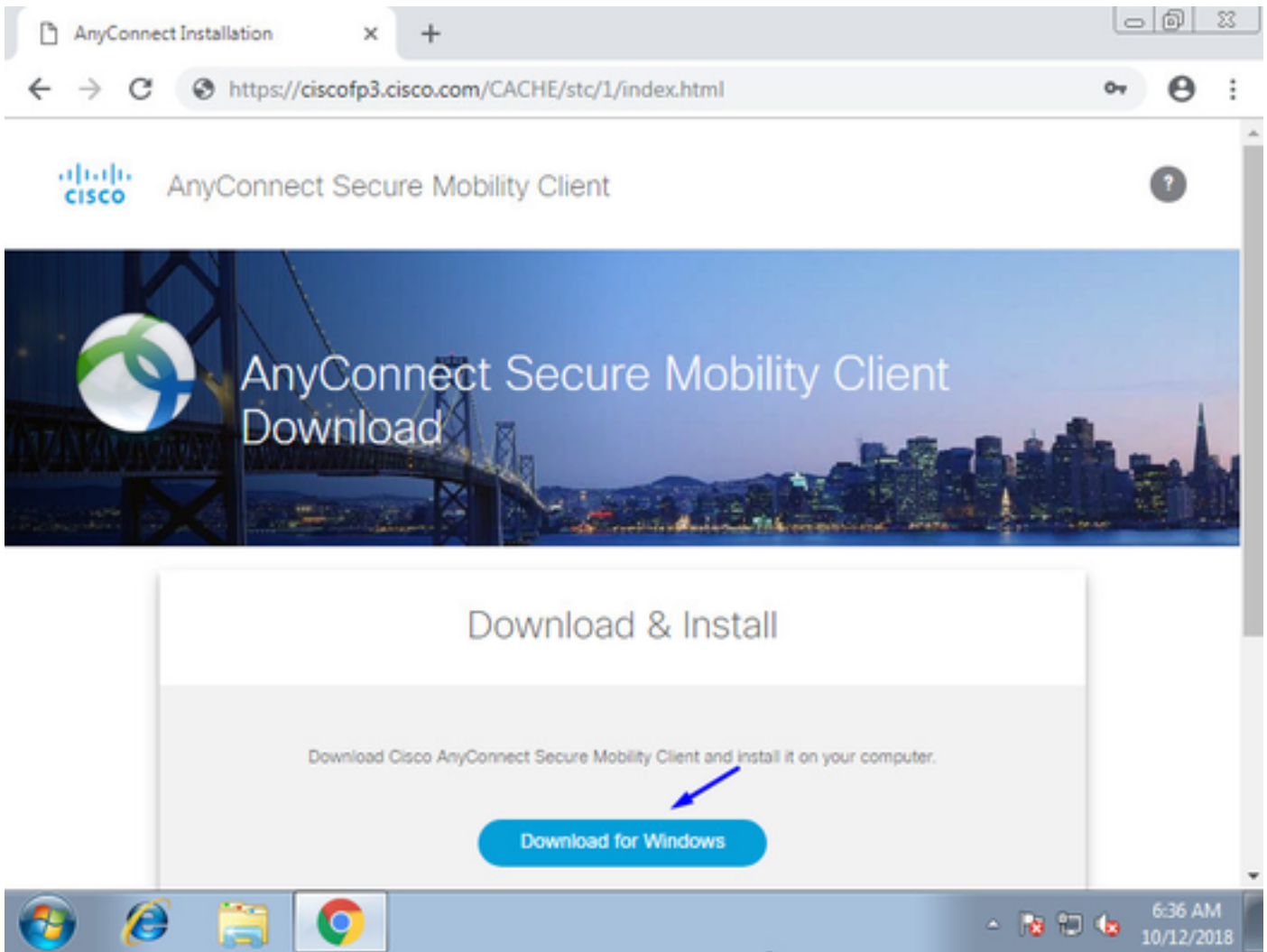
Pulse su nombre de usuario y contraseña del Active Directory



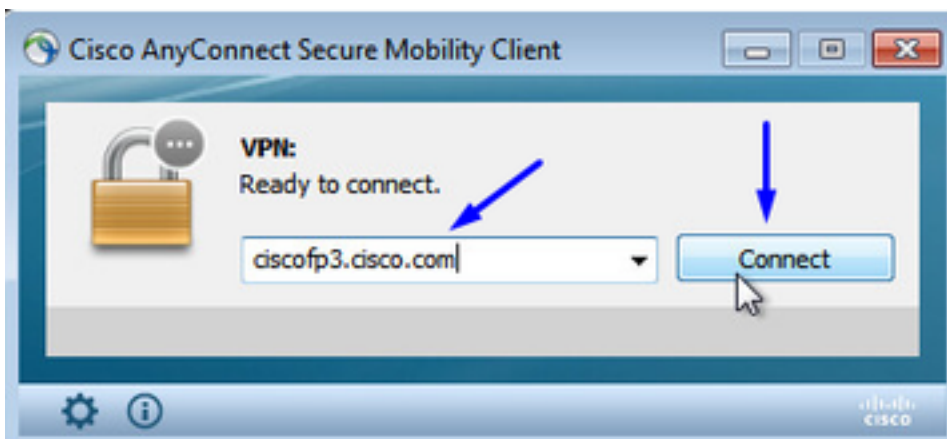
The screenshot shows a web browser window with a 'Logon' form. The form has a title bar with a key icon and the text 'Logon'. Below the title bar, there are three input fields: 'Group' with a dropdown menu showing 'FTDAnyConnectVPN', 'Username' with the text 'smith', and 'Password' with a masked password '\*\*\*\*\*'. Below these fields is a 'Logon' button. A blue arrow points to the 'Logon' button.

Haga clic la **transferencia directa**



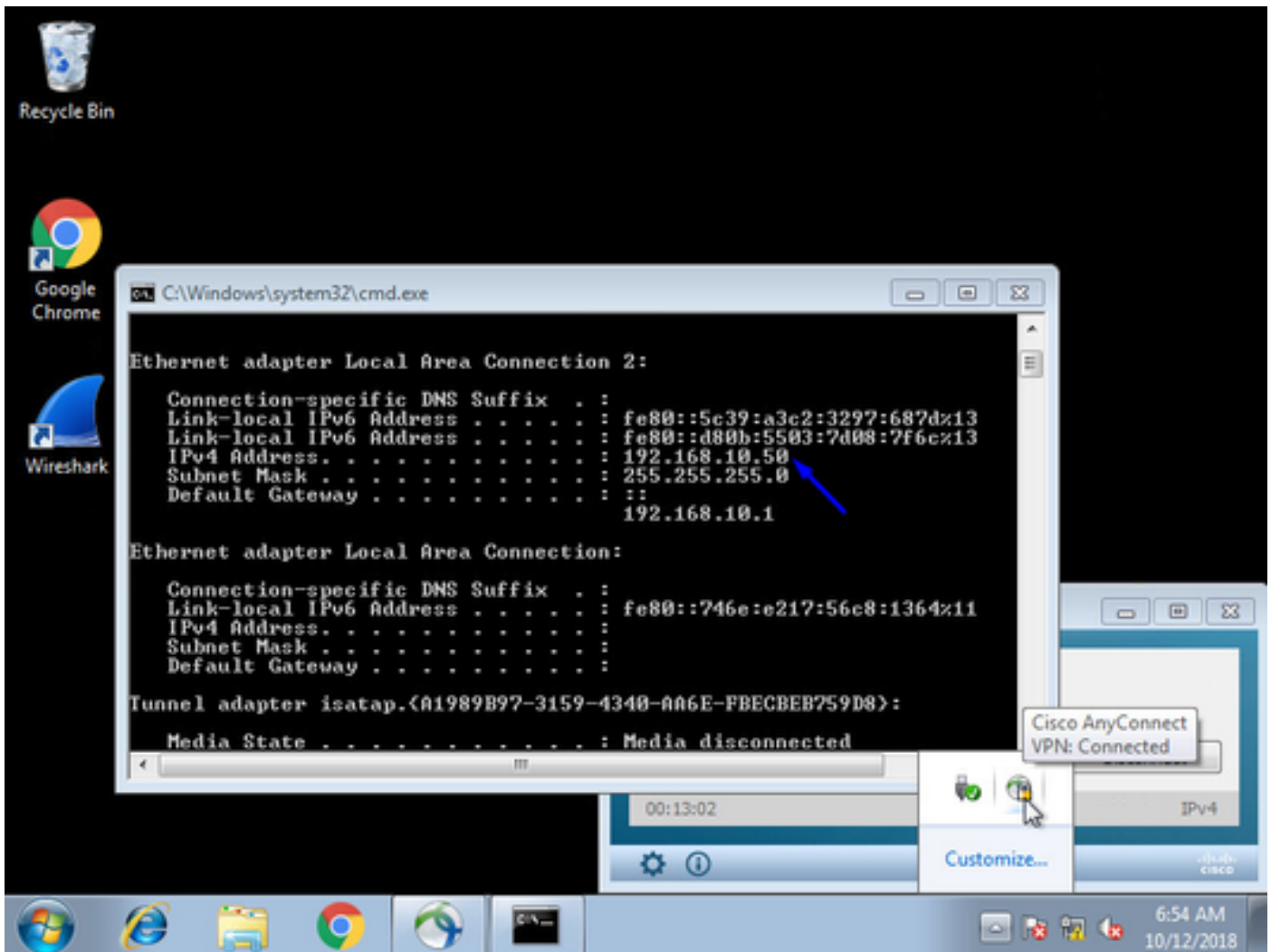


Instale y funcione con al cliente seguro de la movilidad de AnyConnect VPN en la PC de Windows/del mac



Pulse su nombre de usuario y contraseña del Active Directory cuando está incitado

Le darán una dirección IP del pool de la dirección IP creado arriba en el paso 5 y un gateway de valor por defecto del .1 en esa subred



## Verificación

FTD

Comandos show

Verifique en FTD que el usuario final esté conectado con 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

Una vez que usted va en la PC de Windows 7 y hace clic la “desconexión” en el cliente de Cisco AnyConnect, usted conseguirá:

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

## Capturas

Cómo una captura de trabajo parece en la interfaz exterior cuando usted golpea conecta en el cliente de AnyConnect

Ejemplo:

El IP del público del usuario final será el IP del público de su router en casa por ejemplo

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
<enduser'sPublicIPAddress>
<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
```

Vea los paquetes que vinieron a la interfaz exterior del FTD de la PC del usuario final asegurarse de que llegan en nuestro interfaz exterior FTD:

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
<enduser'sPublicIPAddress>
<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
```

Vea los detalles de qué sucede a ese paquete que venga adentro del usuario final dentro del 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=0x2ace107cdb00, 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=0x2ace107c90c0, 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=0x2ace1199df20, 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=0x2ace11d455e0, 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#

Copie la captura a disk0: de su FTD. Usted puede entonces descargarlo vía SCP, el FTP, o el TFTP

(o de la red de centro de administración de FirePOWER UI >> sistema >> salud >> control de salud >> troubleshooting del teclado >> tabulación avanzados del fichero de la transferencia directa del teclado)

```
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)

Verifique que regla NAT esté configurado correctamente:

```
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=0x2ace120c4910, 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=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-po ol 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=0x2ace11975cb0, 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=0x2ace11d455e0, 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-pool 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: ALLLOW  
 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#

Capture tomado en la PC del empleado de la PC que conecta con éxito con el FTD vía AnyConnect VPN

Usted puede también ver el túnel DTL el formar más adelante en esta misma captura

La captura adquirida la interfaz exterior del FTD que muestra la PC de AnyConnect conecta con éxito con el 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	TLsv1.2	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	TLsv1.2	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	TLsv1.2	1159	Certificate, Server Hello Done
9	12:05:56.791691		55928		443	TLsv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	12:05:56.794911		443		55928	TLsv1.2	145	Change Cipher Spec, Encrypted Handshake Message
11	12:05:56.797077		55928		443	TLsv1.2	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	TLsv1.2	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	TLsv1.2	363	Application Data
16	12:05:56.798786		443		55928	TLsv1.2	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 09 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 85 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....
0110 6c 65 79 33 2d 43 4f 52 42 44 43 33 2d 43 41 30 6c 65 79 33 2d 43 41 30 ..18101 0024500Z
0120 1e 17 0d 31 38 31 30 31 30 32 34 35 30 30 5a 30 ..201009 024500Z
0130 17 0d 32 30 31 30 30 39 30 32 34 35 30 30 5a 30 ..1805..*H....
0140 81 b3 31 26 30 24 06 09 2a 86 48 86 f7 0d 01 09 ... f p3...
0150 02 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 0b 6c 65 79 33 2e 6c 6f 63 ..0...
0170 55 04 06 13 02 55 53 11 0b 30 09 06 03 55 04 08 U....US1~0...U...
0180 13 02 43 41 31 11 30 0f 06 03 55 04 07 13 08 53 ..CA1~0~..U....S
0190 61 6e 20 4a 6f 73 65 31 0e 30 0c 06 03 55 04 0a an Jose1~0...U...
01a0 13 05 43 69 73 63 6f 31 0c 30 0a 06 03 55 04 0b ..Cisco1~0...U...
01b0 13 03 54 41 43 31 20 30 1e 06 03 55 04 03 13 17 ..TAC1 0 ~..U...
01c0 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 6c 65 79 6c 6f 72 62 66 70 33 2e ..rfp3.
01d0 33 2e 6c 6f 63 61 6c 31 1c 30 1a 06 09 2a 86 48 3..local1~0...*H...
01e0 86 f7 0d 01 09 01 16 0d 74 61 63 40 63 69 73 63 .....tac@cisc
01f0 6f 2e 63 6f 6d 30 82 01 22 30 0d 06 09 2a 86 48 o.com0...0...*H...
0200 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 .....0...

```

Nota: usted puede ver el certificado de servidor VPN FTD en paquete el “de los saludos del servidor mientras que conectamos con la interfaz exterior del FTD vía el VPN. La PC del empleado confiará en este certificado porque la PC del empleado lo tiene certificado raíz CA encendido, y el certificado de servidor VPN FTD fue firmado por ése lo mismo raíz CA.

Capture tomado en el FTD al servidor de RADIUS FTD que pregunta si el username + la contraseña están correctos (Cisco ISE)

capaaa.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	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

```

Como usted puede ver arriba, nuestra conexión VPN consigue un Acceso-validar, y nuestro cliente de AnyConnect VPN conecta con éxito con el FTD vía el VPN

La captura (CLI) de FTD que pide Cisco ISE si el username + la contraseña son válidos (es decir se asegura de que los pedidos de RADIUS van con éxito entre FTD e ISE y verifica hacia fuera qué interfaz es que se van)

```

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

```

Debajo del servidor de RADIUS de Cisco ISE muestra esa autenticación satisfactoria. Haga clic la lupa para ver los detalles de la autenticación satisfactoria

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



### 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

Capture en el adaptador de AnyConnect de la PC del empleado de la PC del empleado que va a un sitio web interior vía el HTTPS (es decir mientras que es con éxito VPN'd adentro):

The screenshot shows a Wireshark capture on the interface '\*Local Area Connection 2'. The filter is 'tcp.port == 443'. The packet list shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
49	1.545946	192.168.10.50		TCP	66	63576 → 443 [SYN] Seq=0 Win=8192
50	1.547622		192.168.10.50	TCP	66	443 → 63576 [SYN, ACK] Seq=0 Ack=
51	1.547675	192.168.10.50		TCP	54	63576 → 443 [ACK] Seq=1 Ack=1 Win
52	1.549052	192.168.10.50		TLSv1.2	240	Client Hello
53	1.550413		192.168.10.50	TLSv1.2	900	Server Hello, Certificate, Server
54	1.550909	192.168.10.50		TLSv1.2	372	Client Key Exchange, Change Ciper
58	1.562066			TLSv1.2	105	Change Cipher Spec, Encrypted Har
59	1.562718	192.168.10.50		TLSv1.2	469	Application Data
60	1.595405		192.168.10.50	TLSv1.2	1007	Application Data
61	1.628938	192.168.10.50		TLSv1.2	437	Application Data
64	1.666995		192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=1851 Ack=13
65	1.667232		192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=3217 Ack=13
66	1.667284	192.168.10.50		TCP	54	63576 → 443 [ACK] Seq=1303 Ack=45
67	1.667423		192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=4583 Ack=13

The packet details pane for the selected packet (No. 49) shows:

- Transmission Control Protocol (tcp), Src Port: 63576, Dst Port: 443, Seq: 0, Len: 0
- Source Port: 63576
- Destination Port: 443

The packet bytes pane shows the raw data of the SYN packet:

```

0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00  .."3DU...<Z...E.
0010 00 34 25 44 40 00 80 06 29 59 c0 a8 0a 32 0a c9  -4%D@... )Y...2..
0020 d6 83 f8 58 01 bb 21 bb a9 32 00 00 00 80 02    ...X...!..2.....
0030 20 00 de 45 00 00 02 04 05 56 01 03 03 08 01 01  ..E....~V...|...
0040 04 02
  
```

Summary: Transmission Control Protocol (tcp), 32 bytes | Packets: 260 · Displayed: 125 (48.1%) · Dropped: 0 (0.0%) | Profile: Default

### Depuraciones

radio todo de la depuración

anyconnect 255 del webvpn de la depuración

Ejecute el “radio de la depuración todo el” comando en FTD CLI de diagnóstico (ayuda de diagnóstico-cli del >system) y golpee el “Conectar” en la PC de Windows/del mac en el cliente de Cisco Anyconnect

```
> 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 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 | 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 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#

```

Funcione con 'el comando del anyconnect 255' del webvpn de la depuración en FTD CLI de diagnóstico (ayuda de diagnóstico-cli del >system) y golpee el "Conectar" en la PC de Windows/del mac en el cliente de Cisco Anyconnect

```
> 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, 0x00002acdf1d6440, 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(dtls_iv) = 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 > operaciones > RADIUS > registros vivos > detalles del tecleo de cada autenticación

Verifique en Cisco ISE su clave y el resultado "PermitAccess" VPN ACL se da  
Vive el jsmith de la demostración de los registros autenticado a FTD vía el VPN con éxito

**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
Acs SessionID	corbinise/322344084/1870108
SelectedAuthenticationIdentity Stores	Internal Users
SelectedAuthenticationIdentity Stores	All_AD_Join_Points
SelectedAuthenticationIdentity Stores	Guest Users
Authentication Status	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Allow ASA VPN connections if AD Group VPNusers
CPMSessionID	00000000000070005bbc08c3

CPMSessionID	00000000000070005bbc08c3
ISEPolicySetName	VPN Users
Identity SelectionMatchedRule	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

## Ciente de AnyConnect VPN

Manejo del DARDO

[Cómo recoger el manajo del DARDO para AnyConnect](#)

## Troubleshooting

### DNS

Verifique que pueda Cisco ISE, FTD, Servidor Windows 2012, y PC de Windows/del mac toda la resolución adelante y el revés (control DNS en todos los dispositivos)

PC de Windows

Ponga en marcha un comando prompt, y asegúrese de que usted puede realizar un “nslookup” en el hostname del FTD

## FTD CLI

```
> 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, 0x00002acdf1d6440, 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
```

> **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(dtlsHdr) - 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

```

## ISE CLI:

```
> 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(dtls_iv) = 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
```

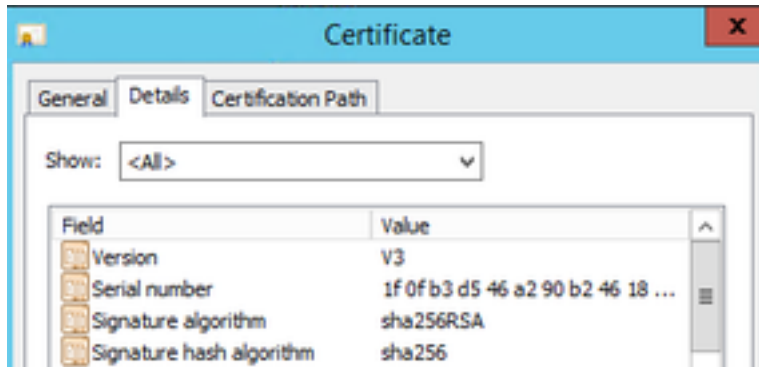
Sending X-CSTP-Disable-Always-On-VPN: false  
Sending X-CSTP-Client-Bypass-Protocol: false

## Servidor Windows 2012

Ponga en marcha un comando prompt, y asegúrese de que usted puede realizar un “nslookup” en el hostname/FQDN del FTD

### Certifique la fuerza (para la compatibilidad del buscador)

Verifique los Certificados de las muestras del Servidor Windows 2012 como SHA256 o más arriba. Haga doble clic su certificado raíz CA adentro Windows y controle “los campos del algoritmo de la firma”



Si son SHA1, la mayoría de los navegadores mostrarán una advertencia del navegador para esos Certificados. Para cambiarla, usted puede controlar aquí:

### [Cómo actualizar las autoridades de certificación del Servidor Windows a SHA256](#)

Verifique que el certificado de servidor VPN FTD tenga los campos siguientes correctos (cuando usted conecta en el navegador con FTD)

Nombre común = <FTDFQDN>

Nombre alternativo sujeto (SAN) = <FTDFQDN>

Ejemplo:

Nombre común: **ciscofp3.cisco.com**

Nombre alternativo sujeto (SAN): **DNS Name=ciscofp3.cisco.com**

### Conectividad y configuración del Firewall

Verifique usando las capturas en FTD CLI y las capturas en la PC del empleado usando Wireshark para verificar que los paquetes estén viniendo sobre TCP+UDP 443 al IP exterior del FTD. Verifique que esos paquetes sean originarios de la dirección IP pública del router casero del empleado

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host  
<enduser'sPublicIPAddress>  
<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  
<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
```

```
...
```