

Configurar AnyConnect VPN em FTD usando Cisco ISE como um servidor Radius com a CA raiz de Windows Server 2012

Índice

[Índice](#)

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Exporte o certificado CA raiz de Windows Server](#)

[Instale o certificado CA raiz no empregado Windows/PCes do Mac](#)

[Gerencia um CSR em FTD, obtenha o CSR assinado pela CA raiz de Windows Server, e instale esse certificado assinado em FTD](#)

[Transfira a imagem de AnyConnect + o editor do perfil de AnyConnect e crie um perfil do .xml](#)

[Configurar Anyconnect VPN em FTD \(use o certificado CA raiz\)](#)

[Configurar a regra FTD NAT para isentar o tráfego VPN do NAT desde que será decifrado de qualquer maneira e para criar a política do controle de acesso/regras](#)

[Adicionar FTD como o dispositivo de rede e configurar o grupo da política em Cisco ISE \(o segredo compartilhado RAI0 do uso\)](#)

[A transferência, instala e conecta ao FTD usando o cliente VPN de AnyConnect no empregado Windows/PCes do Mac](#)

[Verificar](#)

[FTD](#)

[Cisco ISE](#)

[Cliente VPN de AnyConnect](#)

[Troubleshooting](#)

[DNS](#)

[Certifique a força \(para a compatibilidade do navegador\)](#)

[Conectividade e configuração de firewall](#)

Índice

Introdução

Este original descreve como configurar AnyConnect VPN (Virtual Private Network) em um Firewall FTD (defesa da ameaça de FirePOWER) usando Cisco ISE (Identity Services Engine) como um servidor Radius. Nós usamos Windows Server 2012 como nossa CA raiz (Certificate Authority) de modo que a comunicação sobre o VPN seja fixada por Certificados isto é o empregado que o PC

confiará o certificado do FTD porque o certificado FTD VPN foi assinado por nossa CA raiz de Windows Server 2012

Pré-requisitos

Requisitos

Você deve ter seguinte distribuída e ser executado em sua rede:

- Centro de gerenciamento de FirePOWER e Firewall da defesa da ameaça de FirePOWER distribuído com a conectividade básica
- Cisco ISE distribuído e que é executado em sua rede
- Windows Server (com diretório ativo) distribuído e de Windows/Mac dos empregados PC juntado ao domínio AD (diretório ativo)

Em nosso exemplo abaixo, os empregados abrirão o cliente de AnyConnect em seu PC de Windows/Mac, e conectarão firmemente à interface externa do FTD através do VPN usando suas credenciais. O FTD verificará seu nome de usuário e senha contra Cisco ISE (que verificarão com o diretório ativo de Windows Server para verificar seu username, a senha, e usuários do grupo isto é somente no grupo “empregados” AD poderá ao VPN na rede de empresa.

Componentes Utilizados

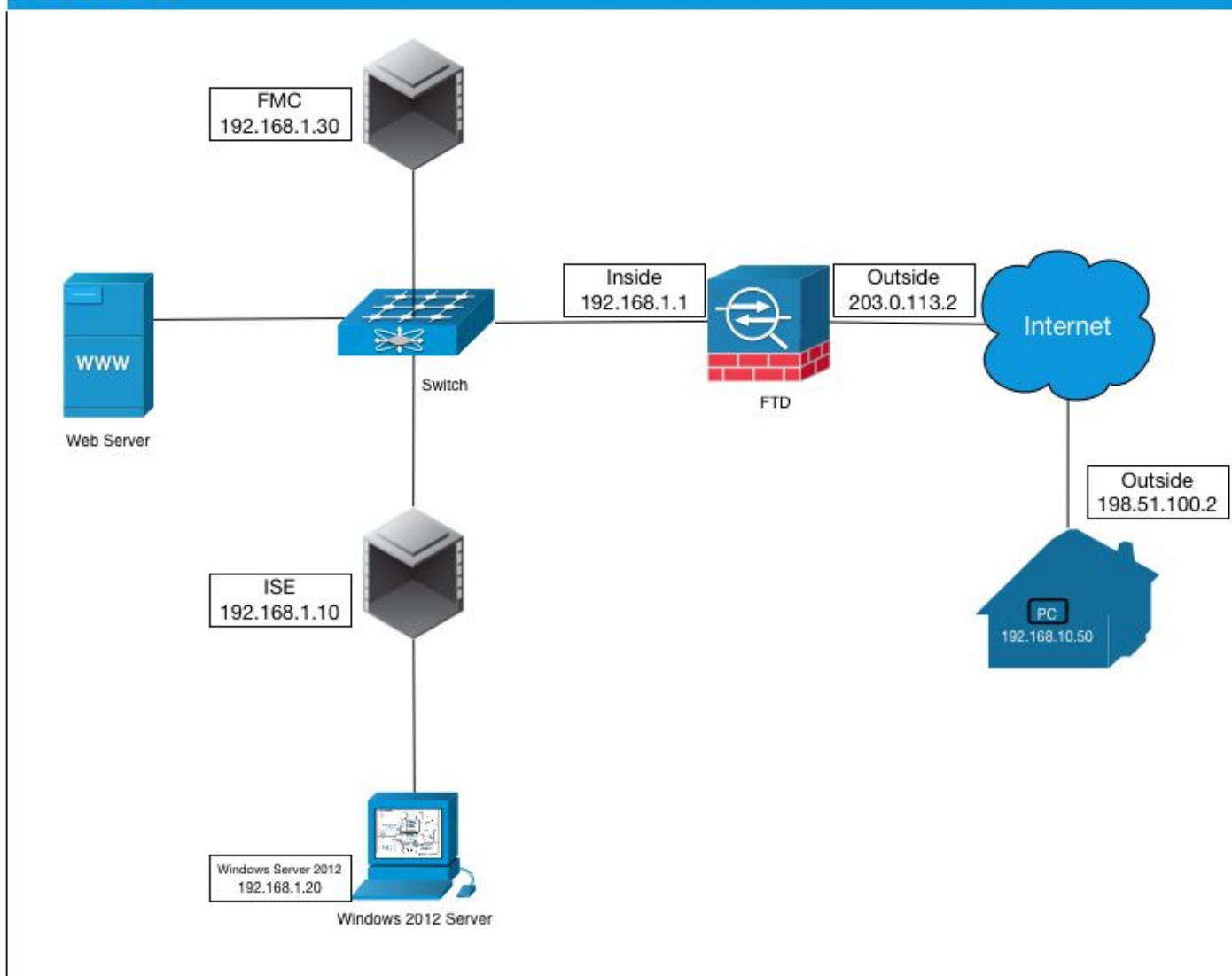
As informações neste documento são baseadas nestas versões de software:

- Centro de gerenciamento de FirePOWER e defesa da ameaça de FirePOWER que executa 6.2.3
- Cisco Identity Services Engine que executa 2.4
- Cliente de mobilidade Cisco AnyConnect Secure que executa 4.6.03049
- Diretório ativo R2 de Windows Server 2012 e serviços certificados running (esta é nossa CA raiz para todos os Certificados)
- Windows 7, Windows 10, PCes do Mac

Configurar

Diagrama de Rede

Topology



Neste caso do uso, o PC de Windows do empregado/Mac que executa o cliente VPN de Anyconnect conectará ao endereço IP público exterior do Firewall FTD, e Cisco ISE concedê-los-á dinamicamente limitou ou acesso direto a determinado interno ou aos recursos de Internet (configurável) uma vez que são conectados através do VPN segundo que grupo AD são um membro no diretório ativo

Dispositivo	Hostname/FQDN	Endereço IP público	Endereço IP privado	IP address de AnyConnect
PC 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	-
Windows Server 2012	ciscodc.cisco.com	-	192.168.1.20	-
Servidores internos	-	-	192.168.1.x	-

Configuração

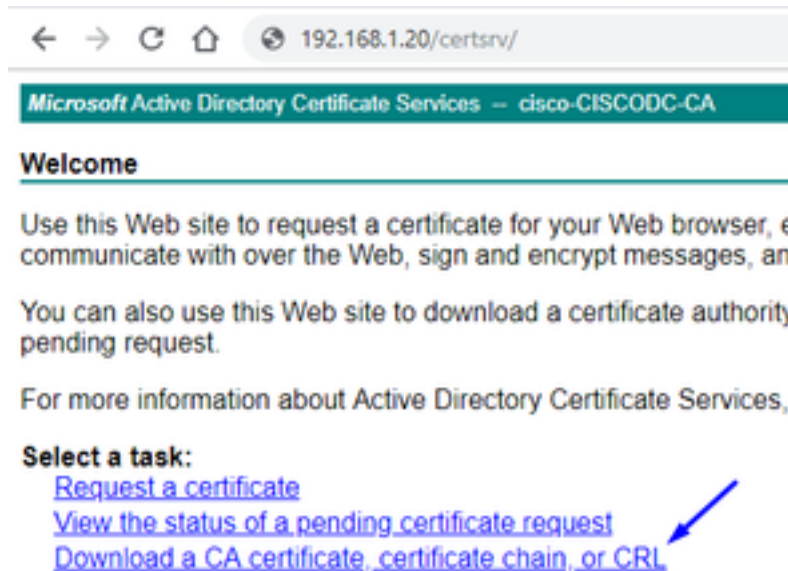
Exporte o certificado CA raiz de Windows Server

Neste original, nós usaremos o Microsoft Windows server 2012 como nossa CA raiz para

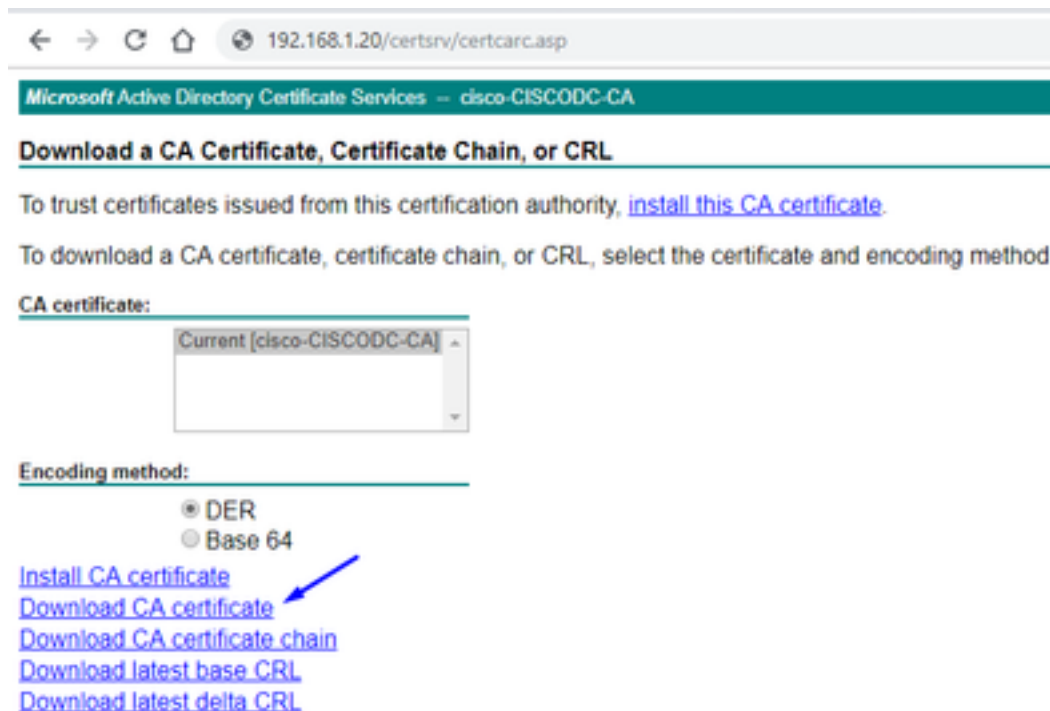
Certificados. A confiança da vontade Do PC do cliente esta CA raiz a conectar firmemente ao FTD através do VPN (veja as etapas abaixo). Isto certificar-se-á que podem conectar firmemente ao FTD sobre os recursos internos do Internet e do acesso da HOME. Seu PC confiará a conexão em seus navegador e cliente de AnyConnect.

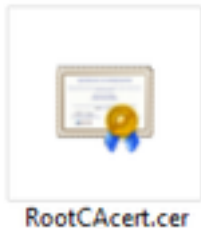
Vá a <http://192.168.1.20/certsrv> e siga as etapas abaixo para transferir seu certificado CA raiz de Windows Server:

Clique a **transferência um certificado de CA, um certificate chain, ou um CRL**



Clique o **certificado da transferência** e rebatize-o a 'RootCAcert3.cer





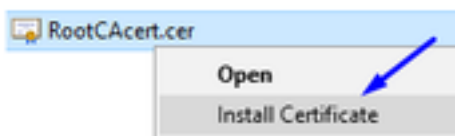
Instale o certificado CA raiz no empregado Windows/PCes do Mac

Método 1: Instale o certificado em todo o PC do empregado empurrando o através da política do grupo de Windows Server (ideal para qualquer coisa sobre usuários 10 VPN):

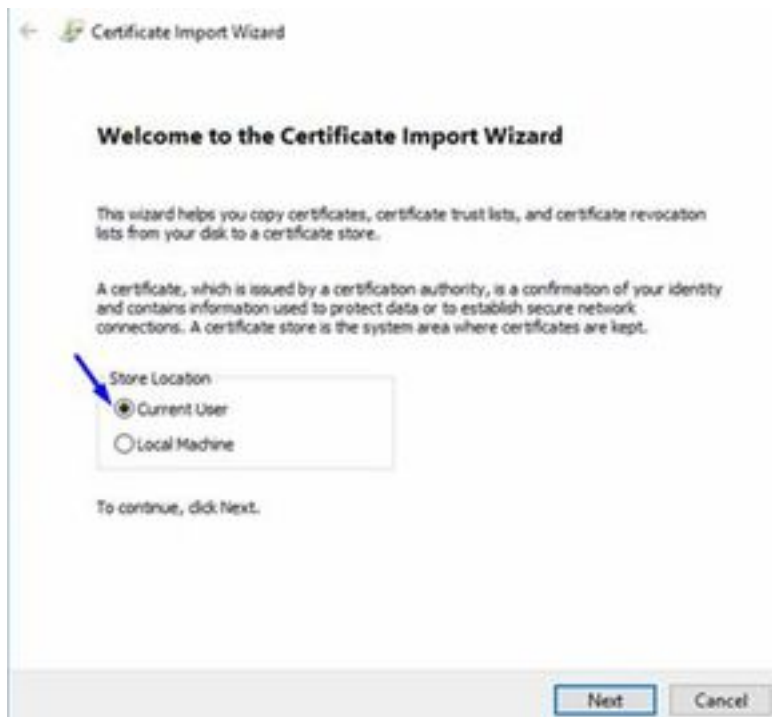
[Como usar Windows Server para distribuir Certificados aos computadores de cliente usando a política do grupo](#)

Método 2: Instale o certificado em todo o PC do empregado instalando o individualmente em cada PC (ideal testar um usuário VPN):

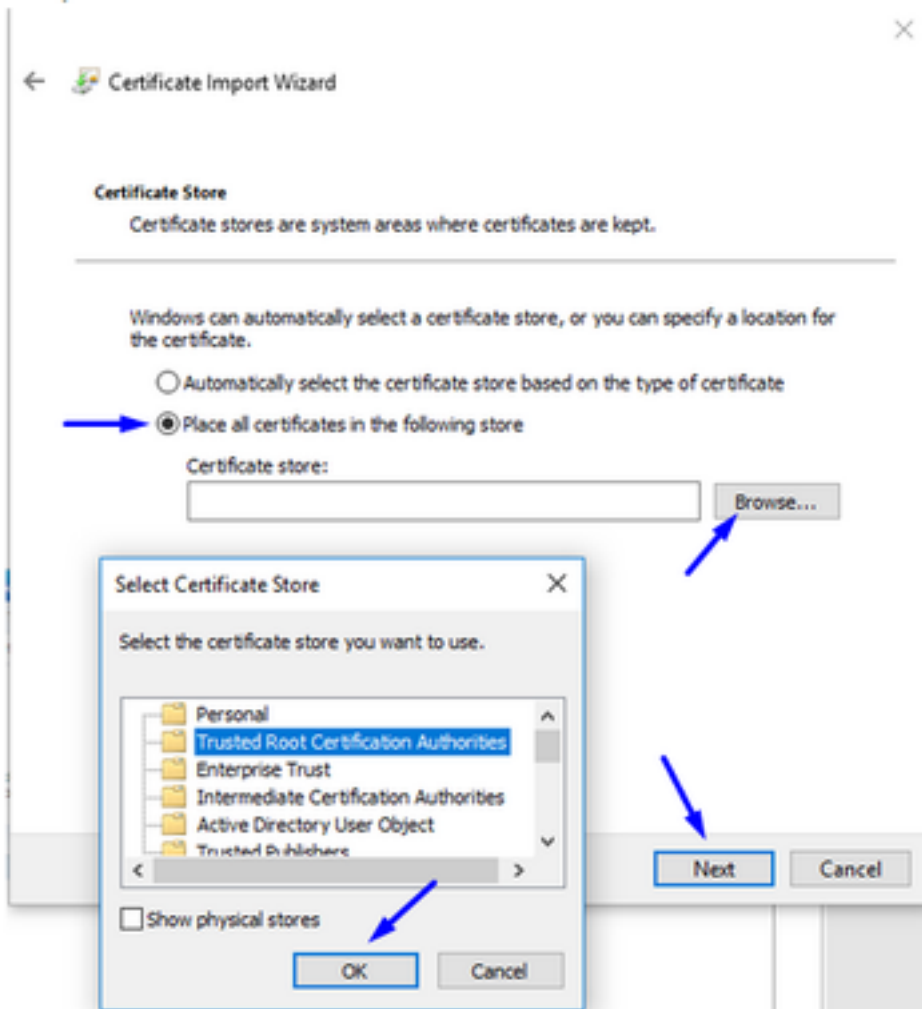
o Direito-clique o certificado em Windows dos seus empregados/PC e clique do Mac **instala o certificado**



Selecione “o usuário atual”

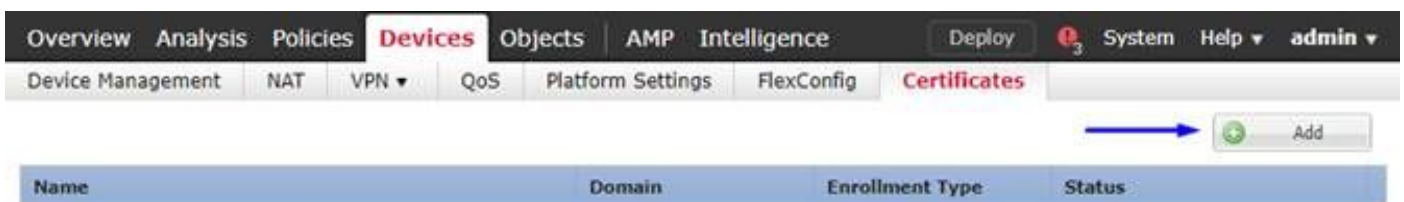


Selecione o lugar todos os Certificados na seguinte loja e nas Autoridades de certificação de raiz confiável seletas, clique a aprovação, clique-a em seguida, e clique-ao revestimento



Gerencia um CSR em FTD, obtenha o CSR assinado pela CA raiz de Windows Server, e instale esse certificado assinado em FTD

Vá aos objetos > ao Gerenciamento do objeto > ao PKI > ao registro CERT, clique sobre o registro CERT Add



O clique adiciona o botão do registro 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

Selecione o **tipo** > o **manual do registro**

Como visto na imagem abaixo, nós precisamos de colar aqui nosso certificado CA raiz:

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

É aqui como transferir seu certificado CA raiz, vê-lo no formato de texto, e colá-lo na caixa acima:

Vá a <http://192.168.1.20/certsrv>

Clique a transferência um certificado de CA, um certificate chain, ou um 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](#)

Clique o botão da base 64 > o certificado de CA da transferência do clique

← → ↻ 🏠 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 o arquivo de RootCAcertBase64.cer no bloco de notas

A cópia e cola os índices de .cer (certificado CA raiz) do server de Windows AD aqui:

Add Cert Enrollment



Name: *

Description:

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: *

```
QgizA0KCRWEA88tZPnQWCWTDVk0PBRQD8jGDMR6GR10UEW
EB/wQFMAMBAf8wHQYD
VR00BBYEF0lpC7y9musCkmDJaKVus9bJUoMIMBAGCSsGAQQBg
jcVAQQDAgEBMCMG
CSsGAQQBgjcVAgQWBBQXIqPq2/dCT41fyYZHPxKhGEYNnzANBg
kqhkiG9w0BAQsF
AAOCAQEAOTaS58Zw7RfarjTGm7HHJHZsA2p9CHdsvB/I35nYeac
OnxyeTWFN7by6
C43uyBFTWTpU3LJjr1mCgEo72qJErJOoU/Y4y7ADAKJF8RtUIb4H
Zq13XNW7Tu9X
DbZCTeYL7INbzZxPyfcuZWIBk5I8uHRvqq2YkBdx6YUYJocNTshH
WwZIXYvQPwwc
yjHrFjm0/YIQIJMhyIVULXXxWGP7diLIEQ67aHsdz+UZq9JofvYa
heHBjzbzIF
zvN2WWFXQs3mFMUxkrjEyzNlDws6vrm6ZhqvOupzmeC6YqByK
QIEAggjevemL7Zd
8DufTZQ4E4VQ9Kp4hrSdzuHSggDTuw==
-----END CERTIFICATE-----
```

Allow Overrides:

Clique a aba >> o tipo dos **parâmetros do certificado** sua informação do certificado

Nota:

O campo FQDN do costume deve ser o FQDN de seu FTD

O campo do Common Name deve ser o FQDN de seu 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:

Dica: você pode obter o FQDN de seu FTD datilografando o comando seguinte do 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
```

Clique a aba **chave** e datilografe todo o nome chave

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

Clique a **salv guarda**

Selecione seu FTDVPNServerCert que nós apenas criamos acima e o clique **adiciona**

Add New Certificate ? X

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

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: FTDVPNServerCert

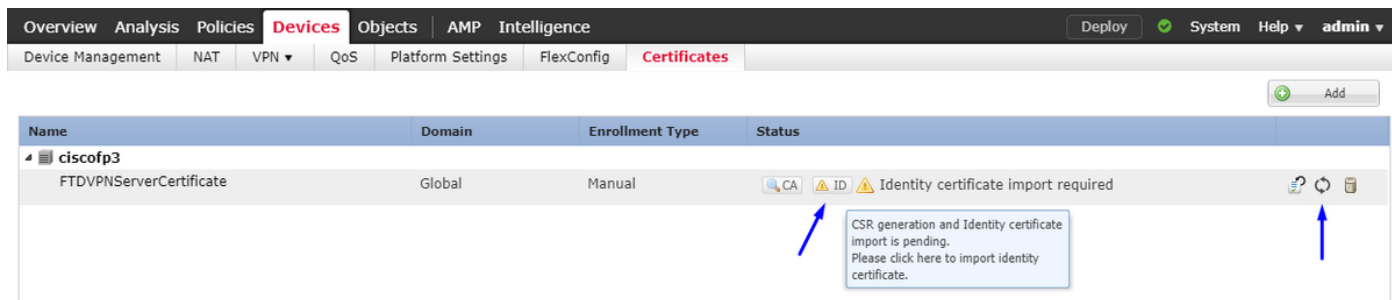
Enrollment Type: Manual

SCEP URL: NA

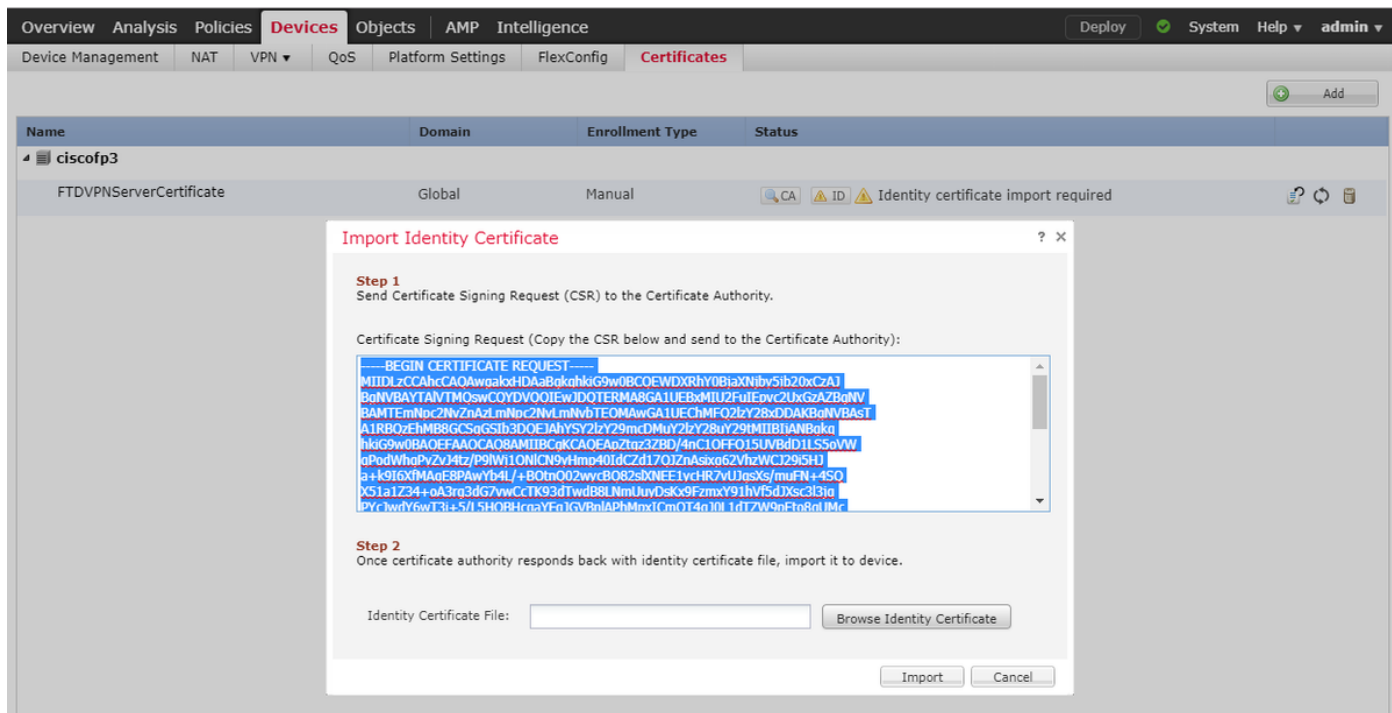
Add Cancel

Dica: Espere aproximadamente 10-30 segundos pelo FMC + FTD para verificar e instalar o certificado CA raiz (o clique refresca o ícone se não faz mostra)

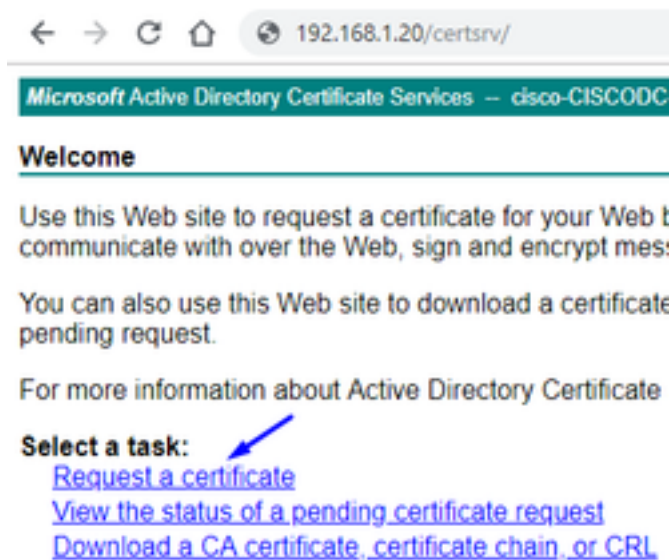
Clique o botão identificação:



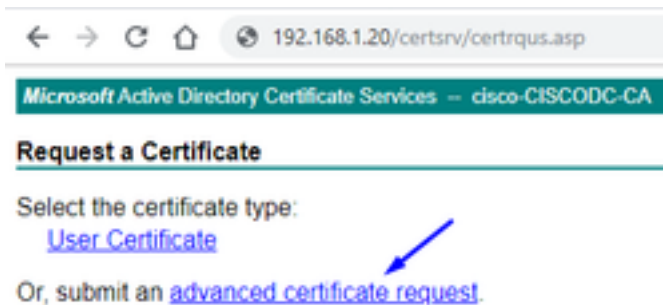
A cópia e cola este CSR, e toma-o a sua CA raiz de Windows Server:



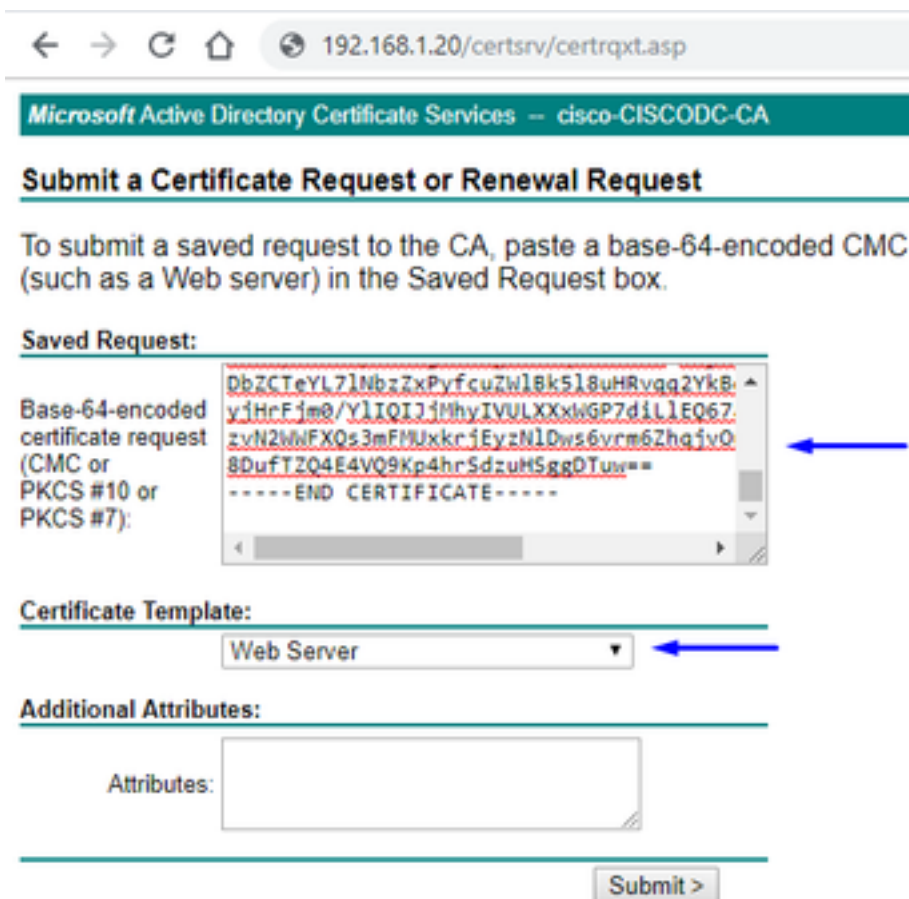
Vá a <http://192.168.1.20/certsrv>



Clique pedido do certificado avançado



Cole sua solicitação de assinatura de certificado (CSR) no campo abaixo e selecione o **servidor de Web** como o molde de certificado

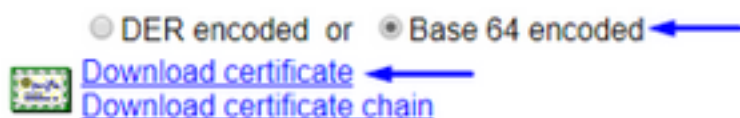


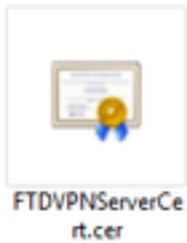
O clique **submete-se**

Clique **64** baixos o botão codificado e clique o certificado da transferência

Certificate Issued

The certificate you requested was issued to you.





O clique **consulta o certificado de identidade** e seleciona o certificado que nós apenas transferimos

Import Identity Certificate

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

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

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDLzCCAhcCAQAwgskxHDAaBokohkiG9w0BCEwWDXRhy0BjaXNjby5ib20xZzA1  
BaNvBAyTANVjQSwcCQYDQOIEwJQOIERMARGA1UEExMIUzEulEpyc2UxGzA7BaNv  
BAMTEmlhc2NvZnAALmNpc2NvLmNybTEOMAwGA1UEChMFQ2lyZ28xODAKBaNvBAsI  
A1RBozEhMB8GCSqGSIb3DQEJAHYSY2iz29mcDMuY2lyZ28x29HMIIBHANBake  
hkiG9w0BAQEFAAQCAQ8AMITBCKCAQEAz2oz3ZRD/4nClOFFQ15UVBdD1L55oVW  
qPdWWhPzYz14tz/P9lW11ONICN9vHmc40IdCZd17QJZnAsix62VhzWCJ295H1  
a+k916xMAnE8PAwYb4L/+BQtmQ02wvrcB082sIXNEE1vcHR7yUJgsXs/muEN+45Q  
YS1a1Z34+gA3rg3dG7yWcTK93dTwdB8LNmLuvDskX9FzmxY91hVf5d1Xsc33iq  
PYclwdY6wT3i+5/l5H0BhcnaYFn1GvBnLAPhMnx1CmOT4n10l1rT7W9nFto8nlJMc
```

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

Identity Certificate File:

O certificado de servidor de VPN FTD (assinado pela CA raiz de Windows Server) foi instalado com sucesso

Name	Domain	Enrollment Type	Status
FTDVPNServerCertificate	Global	Manual	CA ID

Transfira a imagem de AnyConnect + o editor do perfil de AnyConnect e crie um perfil do .xml

Transfira e instale o [editor do perfil de Cisco AnyConnect](#)

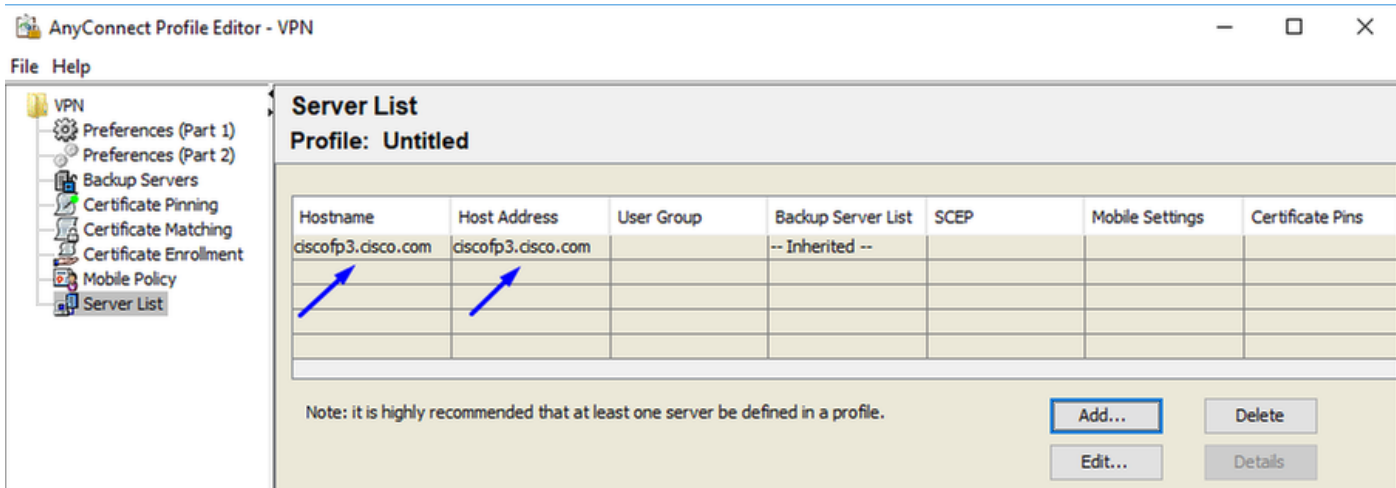
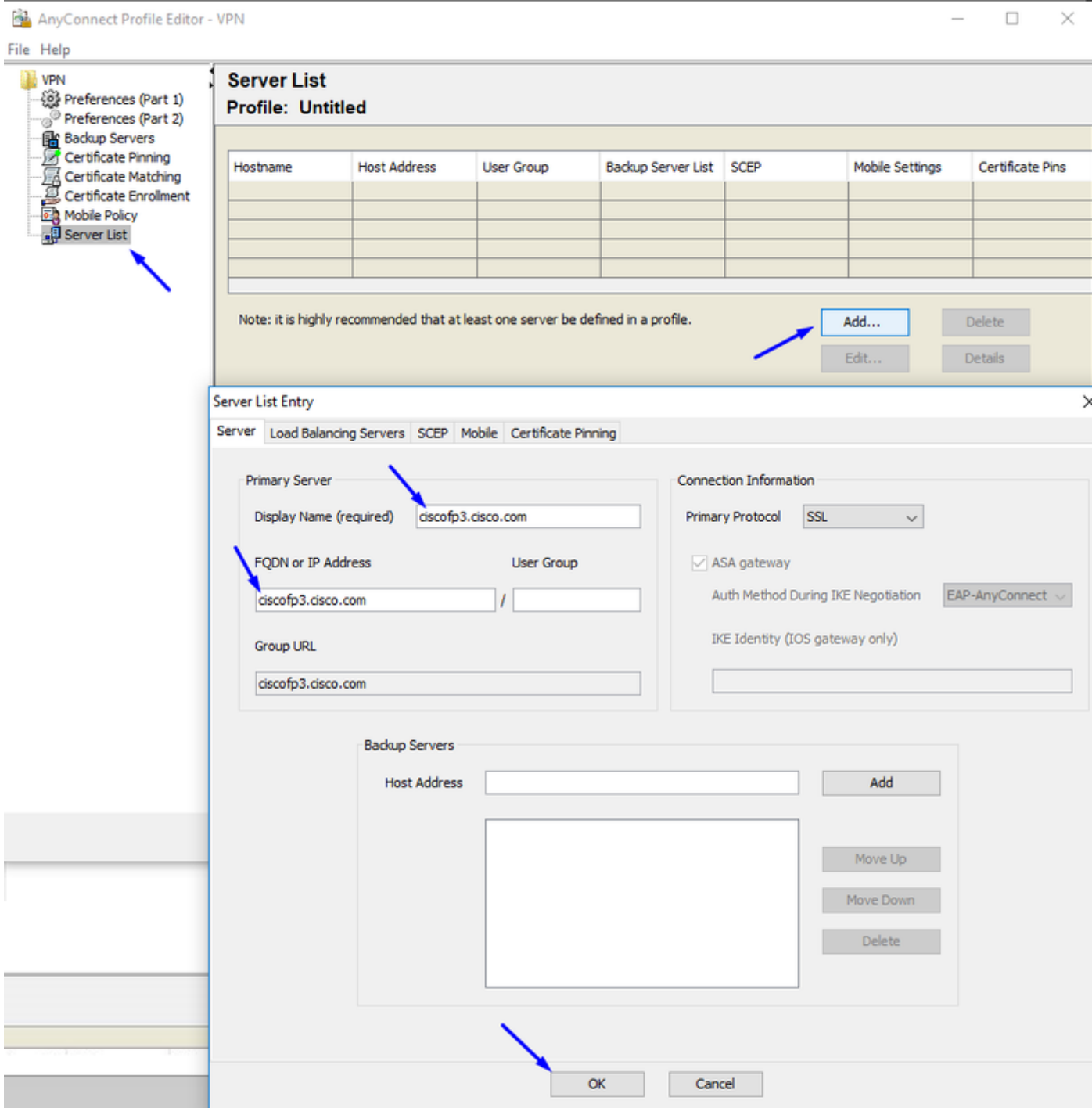
Profile Editor (Windows) 20-SEP-2018 7.74 MB
tools-anyconnect-win-4.6.03049-profileeditor-k9.msi

Abra o editor do perfil de AnyConnect

A lista de servidor do clique > o clique **adicionam...**

Datilografe um **nome do indicador** e o **FQDN** do IP address da interface externa do seu FTD.

Você deve ver entradas na lista de servidor



APROVAÇÃO e arquivo > salvaguarda do clique como...

VPNprofile.xml

Transfira imagens de Windows e do Mac .package de [aqui](#)

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		

Vá aos objetos > ao Gerenciamento do objeto > ao VPN > ao arquivo > ao clique de AnyConnect adicionam o arquivo de AnyConnect

Edit AnyConnect File ? x

Name: *

File Name: *

File Type: * ▾

Description:

Add AnyConnect File ? x

Name: *

File Name: *

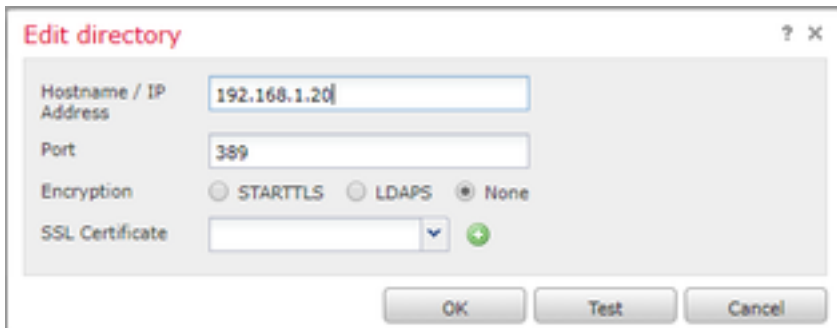
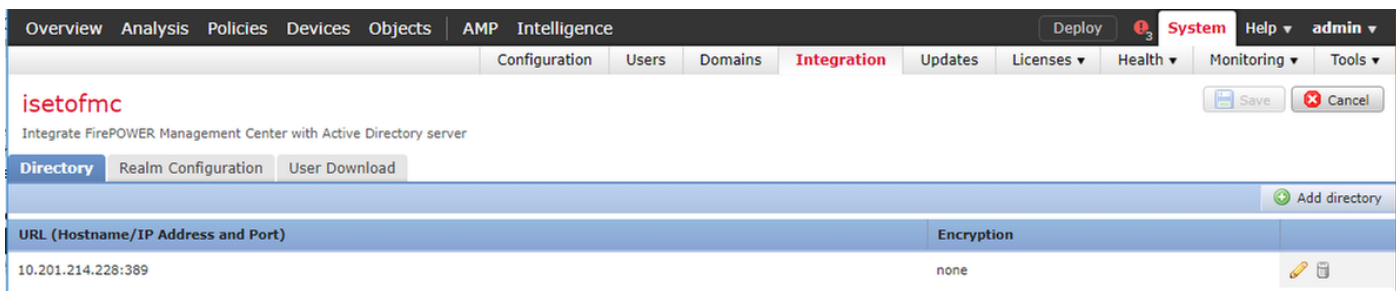
File Type: * ▾

Description:

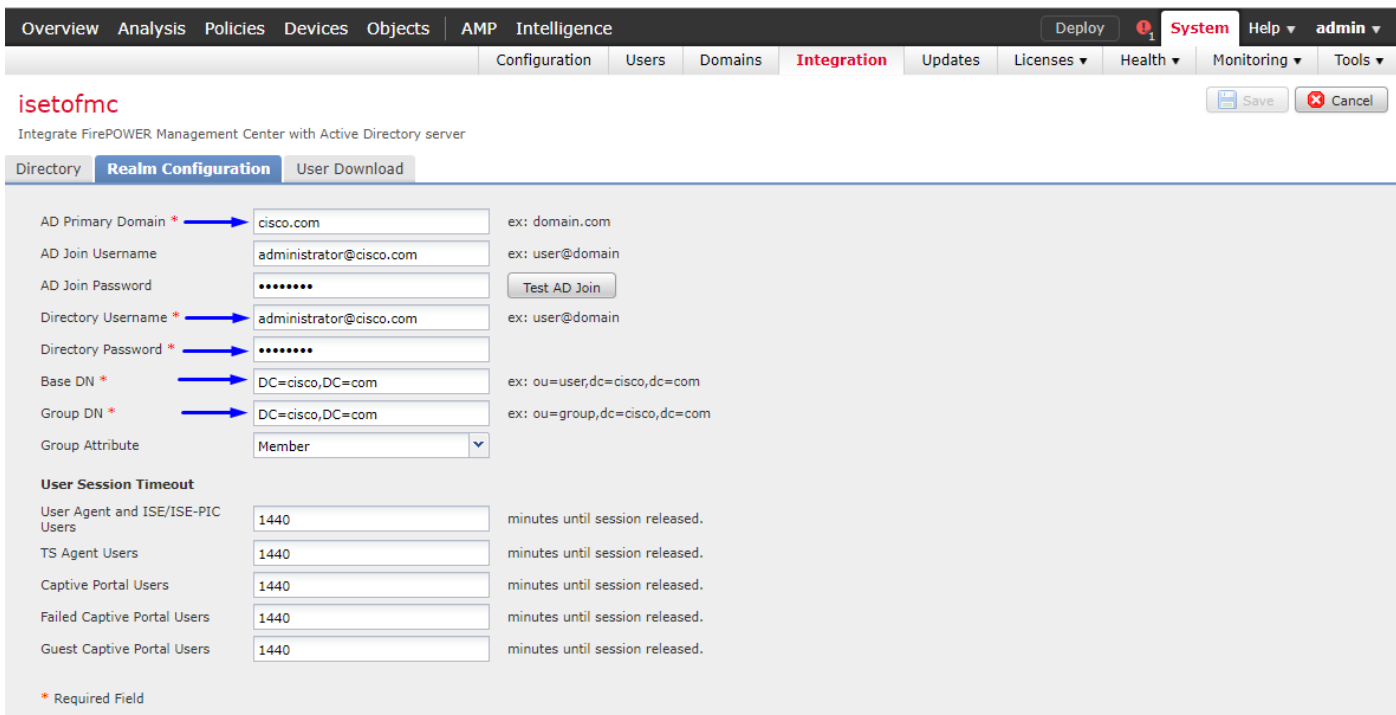
Configurar Anyconnect VPN em FTD (use o certificado CA raiz)

Entre ao centro de gerenciamento de FirePOWER

O sistema do clique > a integração > os reinos > o reino novo do clique >> a tabela de diretório do clique > o clique adicionam o diretório



Guia de configuração do reino do clique - configurar a informação do seu controlador de domínio aqui



Nota: No exemplo acima, um username AD com do “privilégios Admin domínio” no server de Windows AD é usado. Se você quer configurar um usuário com permissões mais específicas, mais mínimas para que o FMC se junte a seu domínio do diretório ativo para sua configuração do reino, você pode ver as etapas [aqui](#)

Aba da **transferência do usuário** do clique - certifique-se que transferência do usuário sucede

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

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

isetofmc
Integrate FirePOWER Management Center with Active Directory server

Directory Realm Configuration **User Download**

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

Available Groups Search by name

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

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

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

Os dispositivos do clique > o VPN > o Acesso remoto > o clique adicionam

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

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

Add

Name	Status	Last Modified
No configuration available Add a new configuration		

Datilografe um nome, descrição, e o clique adiciona para selecionar o dispositivo FTD em que você quer configurar Anyconnect VPN

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

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

Remote Access VPN Policy Wizard

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

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

Name: FTDAnyConnectVPN
Description: AnyConnect VPN configuration for this FTD

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices: Available Devices Selected Devices

10.201.214.134

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

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

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

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

Clique adiciona para o Authentication Server e escolhe o grupo de servidor Radius - este será seu

Cisco Identity Services Engine PSN (a política presta serviços de manutenção ao nó)

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 & Certify 5 Summary

Remote User AnyConnect Client Internet VPN Device (Outside/Inside) Corporate Resources AAA

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

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

Authentication Method:

Authentication Server* (Realm or RADIUS)

Authorization Server:

Accounting Server:

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* ⓘ

Back Next Cancel

Datilografe um **nome** para o servidor Radius
Selecione seu **reino** configurado acima
O clique **adiciona**

Add RADIUS Server Group

Name*

Description:

Group Accounting Mode:

Retry Interval:* (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update
Interval:* (1-120) hours

Enable dynamic authorization
Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

Save Cancel

Datilografe a informação seguinte para seu nó de Cisco ISE:

IP address/hostname: O IP address de Cisco ISE PSN (nó do serviço da política) - isto é onde os

pedidos de autenticação irão

Chave: cisco123

Confirme a chave: cisco123

Cuidado: o acima é sua chave secreta compartilhada RAIO - nós usaremos esta chave em uma etapa mais atrasada

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: Quando o utilizador final tenta conectar ao FTD através de AnyConnect VPN, o username + a senha que datilografa estarão enviados como um pedido de autenticação a este FTD. O FTD enviará esse pedido ao nó de Cisco ISE PSN para a autenticação (Cisco ISE verificará então o diretório ativo de Windows para ver se há esse nome de usuário e senha, e reforça o controle de acesso/acesso de rede segundo a circunstância que nós temos configurado atualmente em 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

Salvaguarda do clique

O clique edita para o conjunto de endereços 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:* FTDAAnyConnectVPN
This name is configured as a connection alias, it can be used to connect to the VPN gateway

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

Authentication Method: AAA Only

Authentication Server:* CiscoISE (Realm or RADIUS)

Authorization Server: Use same authentication server (RADIUS)

Accounting Server: (RADIUS)

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

Use AAA Server (RADIUS only)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: [] []

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.

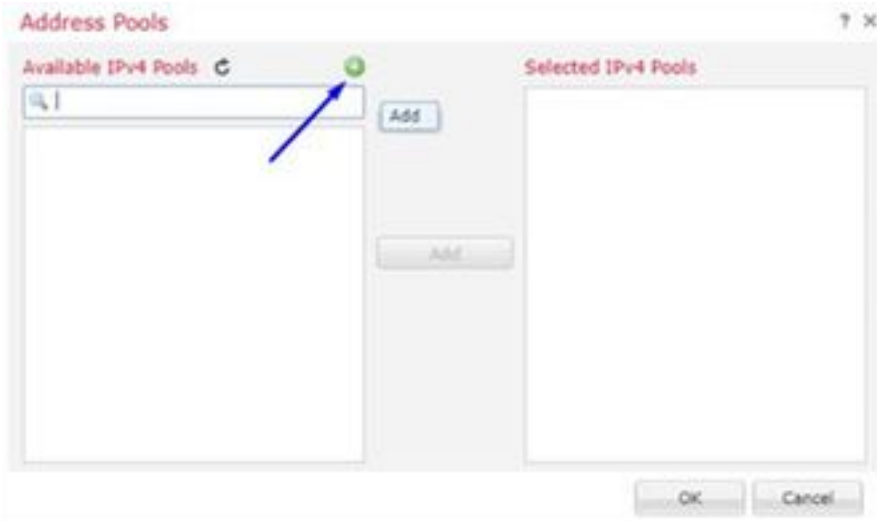
Group Policy:* DfGpPolicy Edit Group Policy

Back Next Cancel

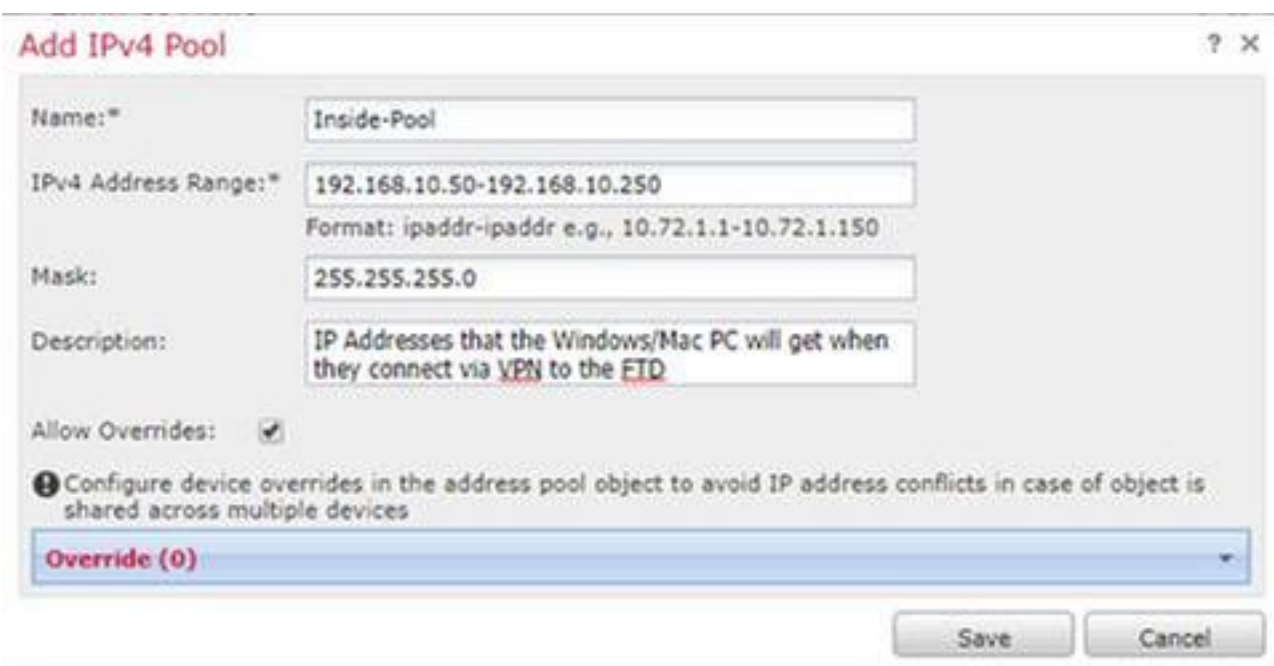
Last login on Wednesday, 2018-10-10 at 10:30:14 AM from 10.152.21.157

How-To Cisco

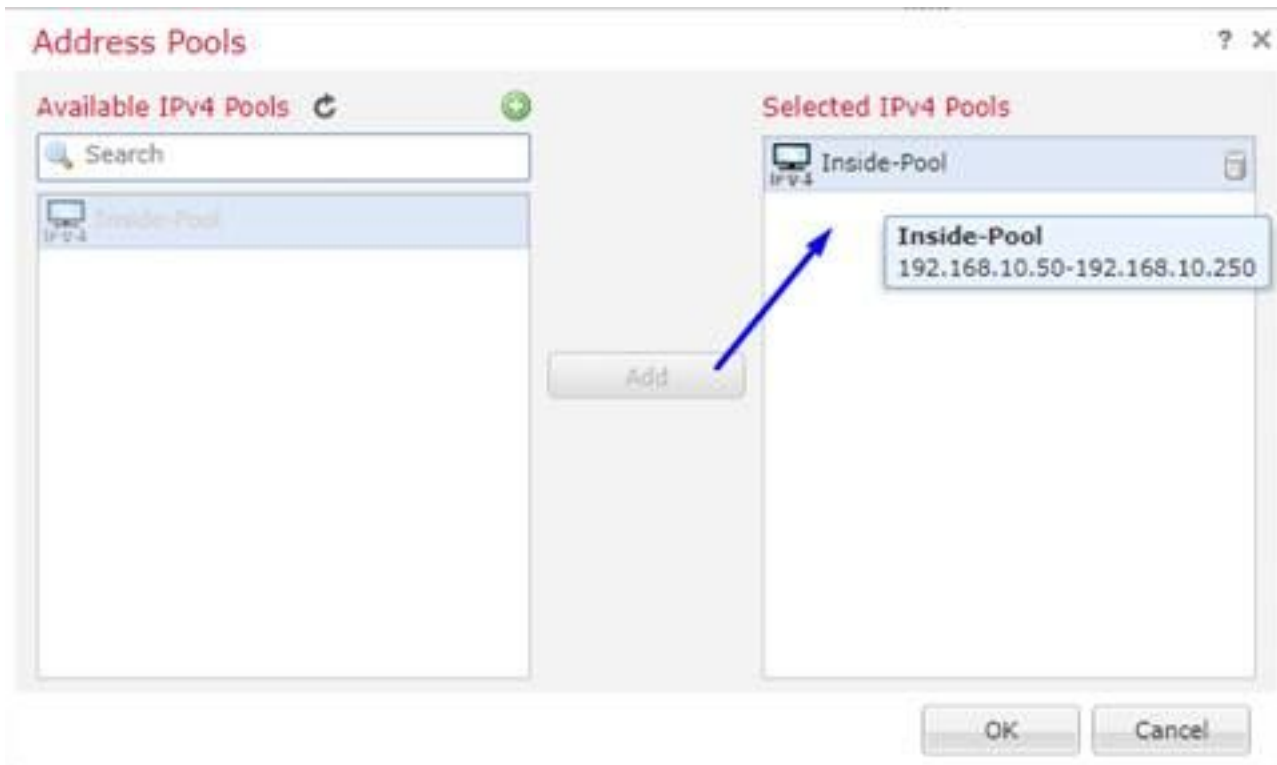
O clique adiciona



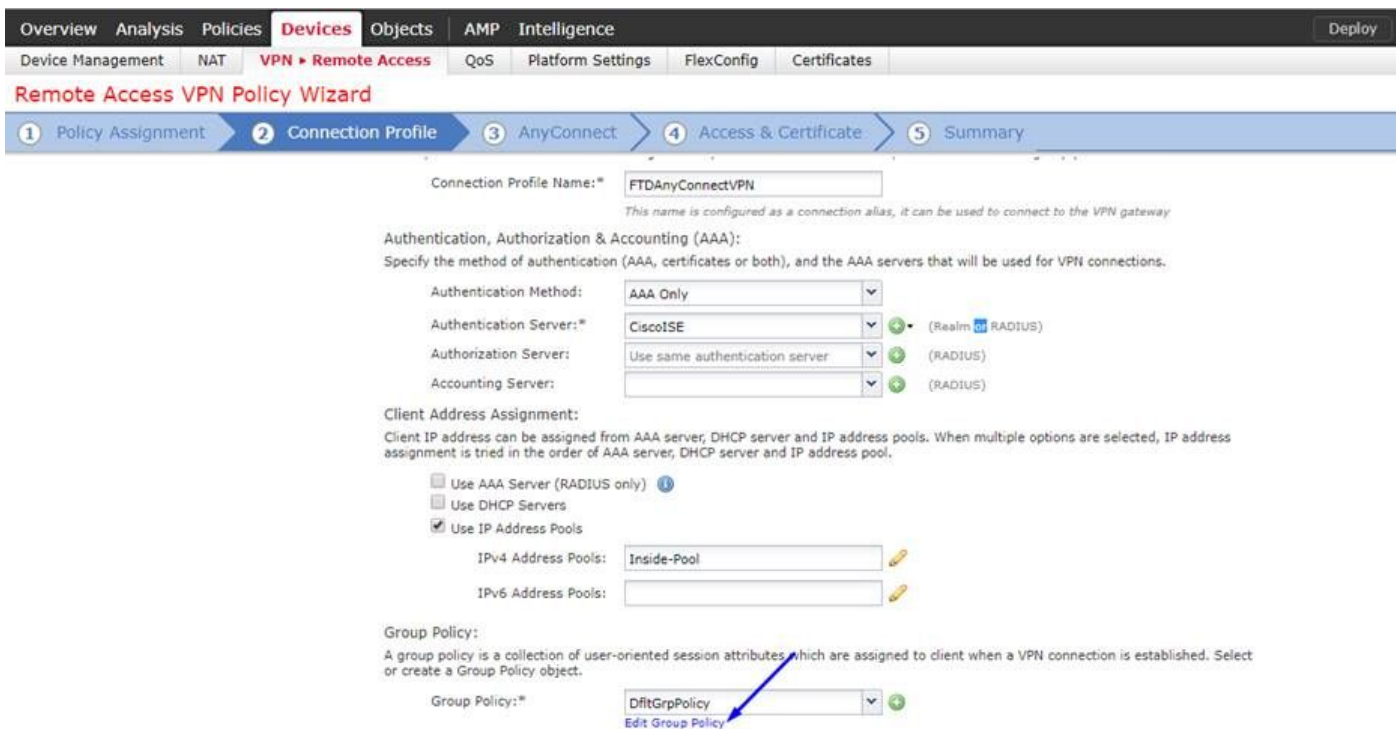
Datilografe um nome, uma escala de endereço IPv4, e uma máscara de sub-rede



Selecione seu pool do IP address e clique a **aprovação**



O clique edita a política do grupo



A aba > os perfis > o clique de Anyconnect do clique adicionam

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.

Datilografe um **nome** e o clique **consulta...** e seleciona seu arquivo VPNprofile.xml de etapa 4 acima

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 File

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

Salv guarda do clique e clique em seguida

Selecione as caixas de seleção para seu arquivo de AnyConnect Windows/Mac de etapa 4 acima

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_4.6.03049	anyconnect-macos-4.6.03049-webdeploy-k9...	Mac OS
<input checked="" type="checkbox"/>	AnyConnect_Windows_4.6.03049	anyconnect-win-4.6.03049-webdeploy-k9.pkg	Windows

Back Next Cancel

Clique em seguida

Selecione a zona do grupo de interface/Segurança como a parte externa

Selecione o certificado de registro como seu certificado que nós fizemos em etapa 3 acima

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

Reveja sua configuração e clique-a em seguida

Remote Access VPN Policy Configuration

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

Name: FTDAnyConnectVPN

Device Targets: 10.201.214.134

Connection Profile: FTDAnyConnectVPN

Connection Alias: FTDAnyConnectVPN

AAA:

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

Address Assignment:

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

Group Policy: DfltGrpPolicy

AnyConnect Images: AnyConnect_Windows_4.6.03049

Interface Objects: Outside

Device Certificates: FTDVPNServerCert

Additional Configuration Requirements

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

- Access Control Policy Update**
An *Access Control* rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a *NAT rule* to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or 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

Configurar a regra FTD NAT para isentar o tráfego VPN do NAT desde que será decifrado de qualquer maneira e para criar a política do controle de acesso/regras

Crie uma **regra** do NAT estático para certificar-se que o tráfego VPN não obtém NAT'd (FTD já decifra os pacotes de AnyConnect enquanto vêm à interface externa, assim que é como se esse PC é já atrás da interface interna, e *já* têm um endereço IP privado - nós ainda precisamos de configurar uma regra (Nenhum-NAT) NAT-isenta para esse tráfego VPN):
Vá aos **objetos** > ao clique **adicionam a rede** > o clique **adicionam o 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

Name:

Description:

Network:

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

Allow Overrides:

Save Cancel

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Example_Company_NAT_Policy

Rules

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

Adicionalmente, você deve permitir que o tráfego de dados flua após o usuário VPN dentro. Você tem duas escolhas para este:

- Crie permitem ou negam as regras para permitir que ou negar os usuários VPN alcancem determinados recursos
- Permita do “a política do controle de acesso desvio para o tráfego decifrado” - isto deixa qualquer um que pode conectar com sucesso ao FTD através do desvio ACL VPN e do acesso que qualquer coisa atrás do FTD sem ir completamente permite ou nega regras na política do controle de acesso

Permita a política do controle de acesso do desvio para o tráfego decifrado abaixo: **Dispositivos > VPN > Acesso remoto > perfil > interfaces de acesso VPN:**

Access Control for VPN Traffic

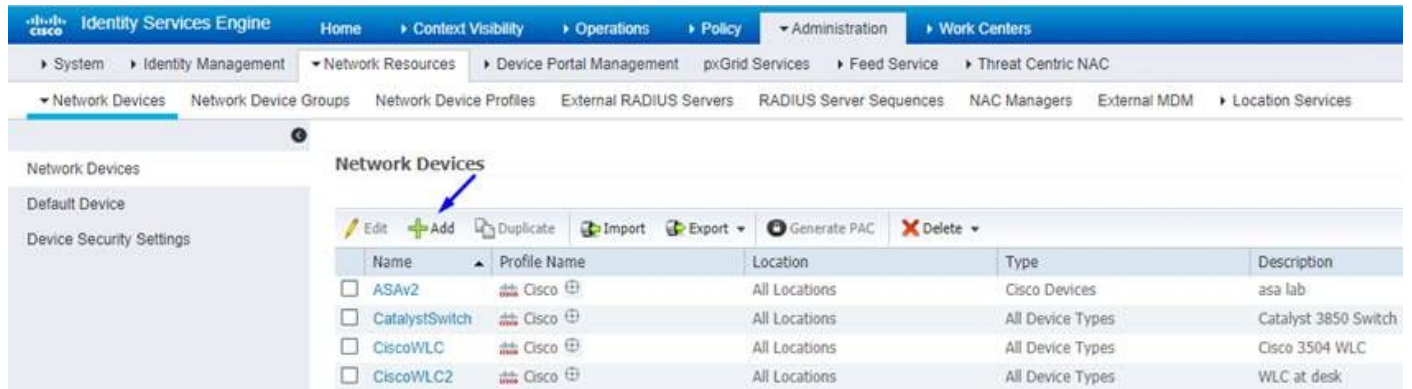
- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Nota: Se você não permite esta opção, você precisará de ir às **políticas > à política do controle de acesso** e para criar permita que as regras para que os usuários VPN possam alcançar atrás as coisas internas ou o dmz

ClickDeployin o direita superior do centro de gerenciamento de FirePOWER

Adicionar FTD como o dispositivo de rede e configurar o grupo da política em Cisco ISE (o segredo compartilhado RAIO do uso)

Entre ao Cisco Identity Services Engine e a **administração** > os **dispositivos de rede** > o clique do **adicionam**



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 existing devices and an 'Add' button 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

Datilografe um **nome**, datilografe o **IP address** de seu FTD, e datilografe seu **segredo compartilhado RAIO** das etapas acima

Cuidado: Este deve ser a relação/IP address para fora que o FTD pode alcançar seu Cisco ISE (servidor Radius) isto é a relação FTD que seu Cisco ISE pode alcançar o FTD sobre

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

A política do clique > a política ajustada > criam uma política ajustada para todos os pedidos de autenticação que entrarem do seguinte tipo:

O Raio-NAS-porta-tipo IGUALA virtual

Isto significa se alguma requisição RADIUS que entrar o ISE que olha como conexões de VPN, ela baterá este grupo da política

Identity Services Engine Administration Work Centers License Warning

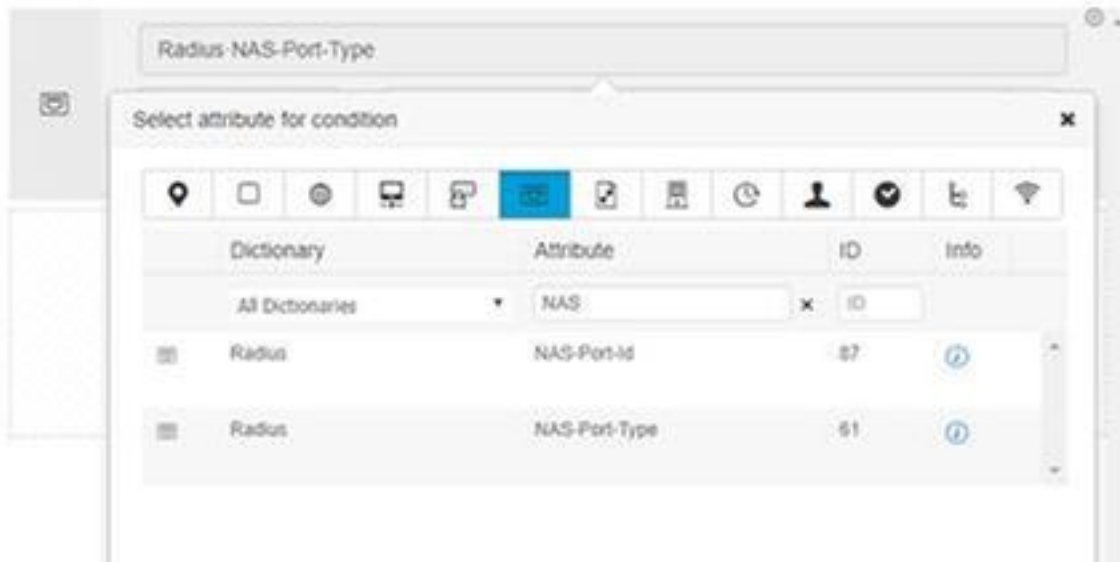
Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

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

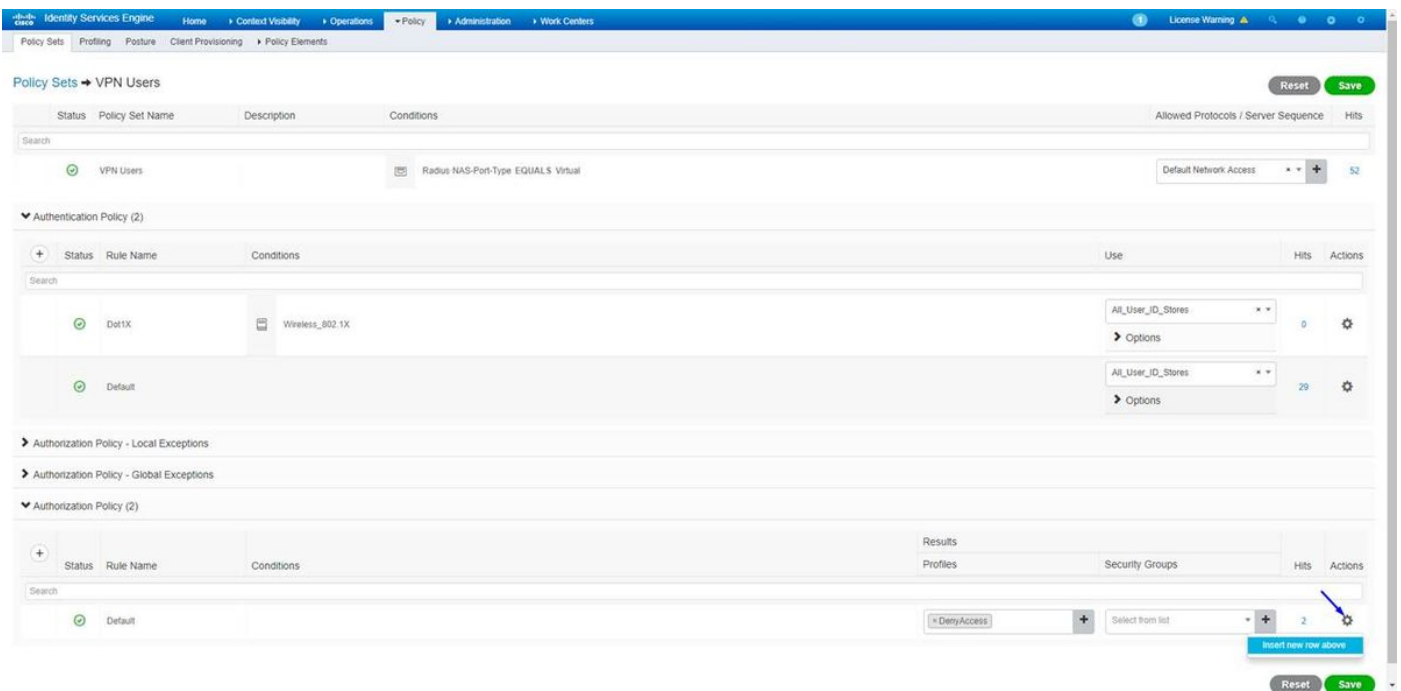
É aqui onde você pode encontrar essa condição em Cisco ISE:

Editor



Edite a **política ajustam-no** criado acima

Adicionar uma regra acima da regra de bloqueio de padrão dar da “o perfil da autorização do **acesso licença**” dos povos somente se estão no grupo do diretório ativo chamado “**empregados**”:



Éabaixo como sua regra olhará uma vez completa


The screenshot displays the Cisco ISE Policy Sets configuration interface. The main table shows the 'VPN Users' policy set with a condition of 'Radius-NAS-Port-Type EQUALS Virtual'. Below this, there are two sections for 'Authentication Policy (2)'. The first section shows rules for 'Dot1X' and 'Default'. The second section, 'Authorization Policy - Local Exceptions', shows a rule named 'Allow FTD VPN connections if AD Group VPNUsers' with the condition 'ciscodc:ExternalGroups EQUALS cisco.com/Users/Employees'. This rule has two actions: 'PermitAccess' and 'DenyAccess'. Two blue arrows point to the condition and the 'PermitAccess' action.

A transferência, instala e conecta ao FTD usando o cliente VPN de AnyConnect no empregado Windows/PCes do Mac

Abra seu navegador no empregado Windows/PC do Mac, e vá ao endereço exterior de seu FTD em seu navegador

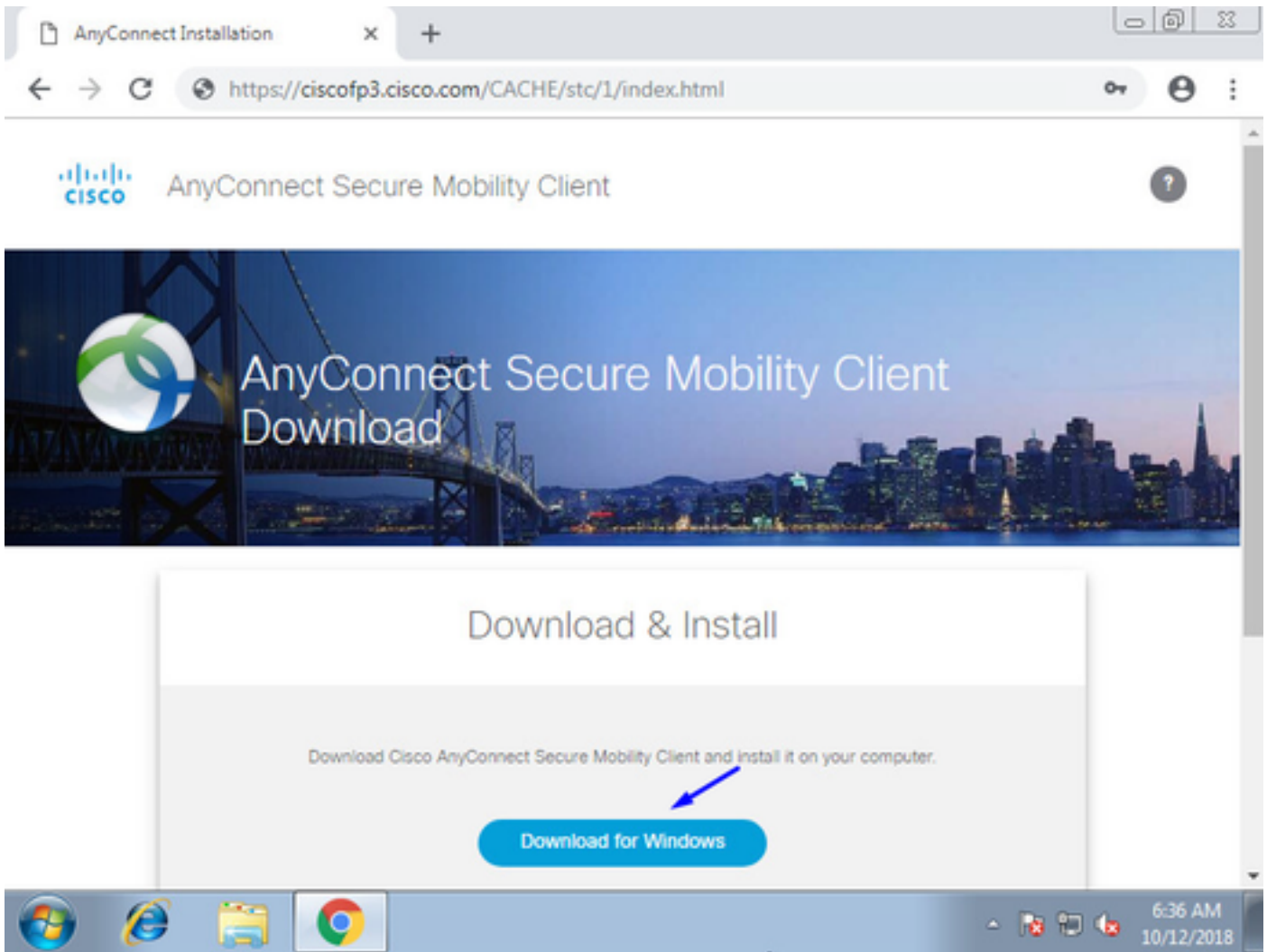
← → ↻ <https://cisconfp3.cisco.com>

Datilografe seu nome de usuário e senha do diretório ativo

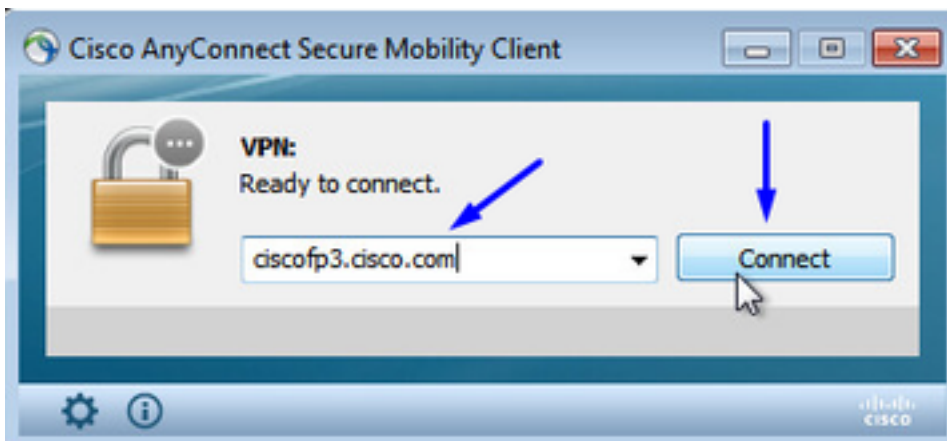


The screenshot shows a web browser window with a 'Logon' form. The form has a title bar with a key icon and the text 'Logon'. Below the title bar, there are three input fields: 'Group' with a dropdown menu showing 'FTDAnyConnectVPN', 'Username' with the text 'smith', and 'Password' with a masked password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

Clique a **transferência**

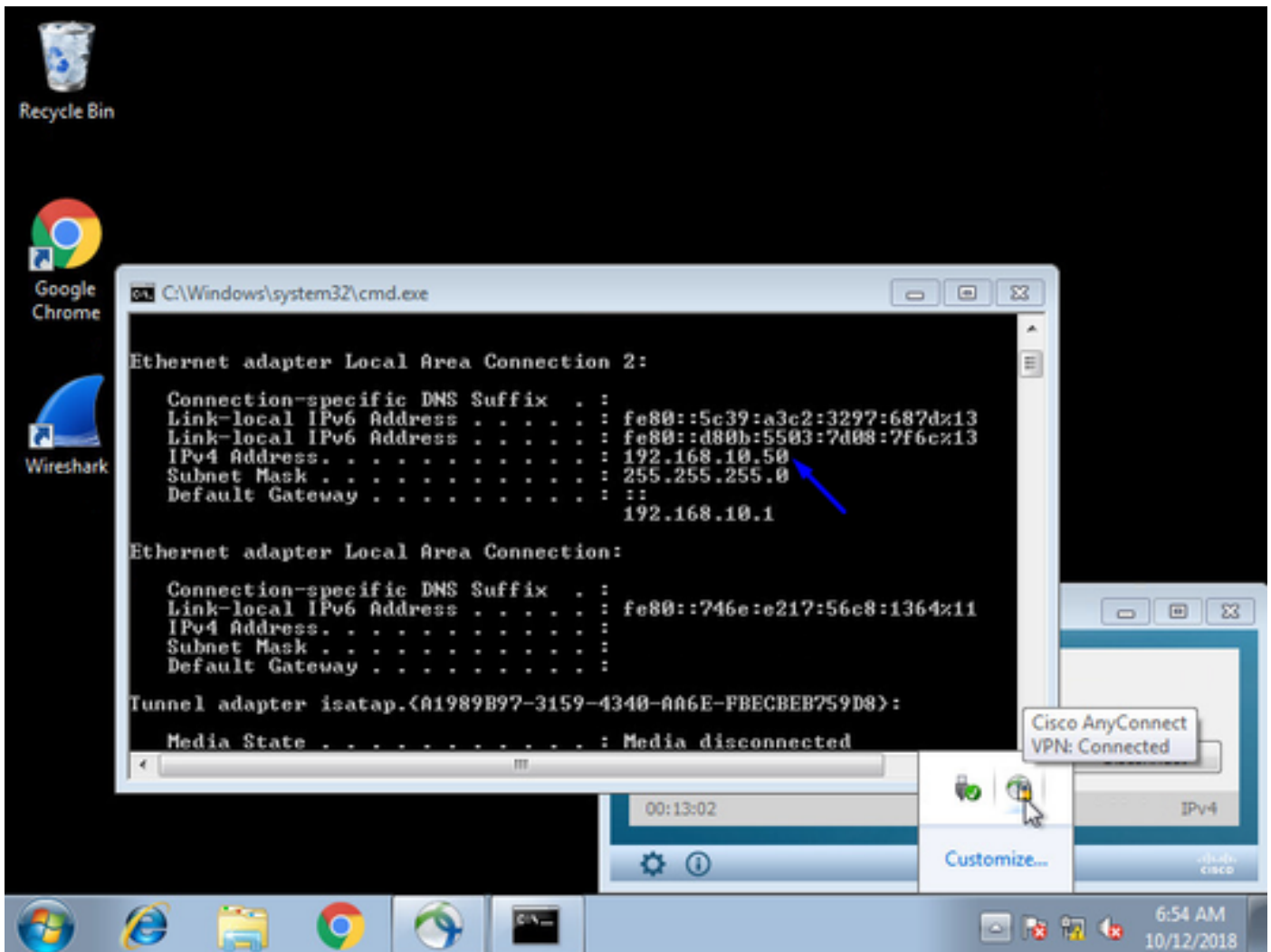


Instale e execute o cliente seguro da mobilidade de AnyConnect VPN no PC de Windows/Mac



Datilografe seu nome de usuário e senha do diretório ativo quando alertado

Você será dado um IP address do pool do IP address criado acima na etapa 5 e em um gateway padrão do .1 nessa sub-rede



Verificar

FTD

Comandos show

Verifique em FTD que o utilizador final está conectado a 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

Uma vez que você vai no PC de Windows 7 e clica a “disconexão” no cliente de Cisco AnyConnect, você obterá:

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

Captações

Como uma captação de trabalho olha como na interface externa quando você bater conecta no cliente de AnyConnect

Exemplo:

O IP do público do utilizador final será o IP do público de seu roteador em casa por exemplo

```
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
```

Veja os pacotes que vieram à interface externa do FTD do PC do utilizador final se certificar que chegam em nossa relação 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
```

Veja os detalhes do que acontece a esse pacote que vem dentro do utilizador final dentro do 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 a captação ao disco 0: de seu FTD. Você pode então transferi-lo através do SCP, do FTP, ou do TFTP

(ou da Web de centro de gerenciamento de FirePOWER UI >> sistema >> saúde >> Troubleshooting avançado do monitor de funcionamento >> do clique >> aba do arquivo da transferência do clique)

```
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 regra NAT está configurado corretamente:

```
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 no PC do empregado do PC que conecta com sucesso ao FTD através de AnyConnect VPN

anyconnectinitiation.pcapng

File Edit View Go Analyze Statistics Telephony Wireless Tools Help

ip.addr ==

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

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

Você pode igualmente ver o túnel DTL formar mais tarde nesta mesma captação

capin.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
76	12:06:14.817645		443		56280	TCP	1514	443 → 56280 [PSH, ACK] Seq=9286 Ack=1215 Win=32768 Len=1460 [TCP segment of a reassembled PDU]
77	12:06:14.817645		443		56280	TLSv1.2	176	Application Data
78	12:06:14.817660		443		56280	TLSv1.2	158	Application Data
79	12:06:14.818088		56280		443	TCP	54	56280 → 443 [ACK] Seq=1215 Ack=10746 Win=64240 Len=0
80	12:06:14.818530		56280		443	TCP	54	56280 → 443 [ACK] Seq=1215 Ack=10972 Win=64014 Len=0
81	12:06:18.215122		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	141	Client Hello
82	12:06:18.215610		443		58944	DTLS 1.0 (OpenSSL pre 0.9.8f)	90	Hello Verify Request
83	12:06:18.215671		56280		443	TLSv1.2	1111	Application Data
84	12:06:18.215763		443		56280	TCP	54	443 → 56280 [ACK] Seq=10972 Ack=2272 Win=32768 Len=0
85	12:06:18.247011		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	161	Client Hello
86	12:06:18.247728		443		58944	DTLS 1.0 (OpenSSL pre 0.9.8f)	230	Server Hello, Change Cipher Spec, Encrypted Handshake Message
87	12:06:18.249285		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Change Cipher Spec, Encrypted Handshake Message
88	12:06:18.272309		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
89	12:06:18.277680		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
90	12:06:18.334501		58944		443	DTLS 1.0 (OpenSSL pre 0.9.8f)	263	Application Data

> Frame 81: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)
 > Ethernet II, Src: Cisco_e7:6c:5e (00:16:b1:e7:6c:5e), Dst: Vmware_4f:ac:84 (00:0c:29:4f:ac:84)
 > Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
 > User Datagram Protocol, Src Port: 58944, Dst Port: 443
 > Datagram Transport Layer Security
 > DTLS 1.0 (OpenSSL pre 0.9.8f) Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: DTLS 1.0 (OpenSSL pre 0.9.8f) (0x0100)
 Epoch: 0
 Sequence Number: 0
 Length: 86
 > Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 74
 Message Sequence: 0
 Fragment Offset: 0
 Fragment Length: 74

A captação tomada na interface externa do FTD que mostra o PC de AnyConnect conecta com sucesso ao 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 (00:0b:f1:e7:6c:5e)

> Internet Protocol Version 4, Src: , Dst:

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

Source Port: 443

Destination Port: 55928

[Stream index: 0]

[TCP Segment Len: 1460]

Sequence number: 1 (relative sequence number)

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

Acknowledgment number: 134 (relative ack number)

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

> Flags: 0x018 (PSH, ACK)

Window size value: 32768

[Calculated window size: 32768]

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

Checksum: 0x3693 [unverified]

```

00c0 99 2a 86 48 86 f7 0d 01 01 0b 05 00 30 51 31 15 ..*H...001
00d0 30 13 06 0a 09 92 26 89 93 f2 2c 64 01 19 16 05 0...&...d...
00e0 6c 6f 63 61 6c 31 19 30 17 06 0a 09 92 26 89 93 local1-0...&...
00f0 f2 2c 64 01 19 16 09 63 6f 68 61 64 6c 65 79 33 ..,d....
0100 31 1d 30 1b 06 03 55 04 03 13 14 63 6f 68 61 64 1-0...U...
0110 6c 65 79 33 2d 43 4f 52 42 44 43 33 2d 43 41 30 ...18101 0024500Z
0120 1e 17 0d 31 38 31 30 31 30 32 34 35 30 30 5a ...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 92 13 17 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 ...US1...U...
0160 6c 65 79 33 2e 6c 6f 63 61 6c 31 0b 30 09 06 03 ...CA1-0...U...S
0170 55 04 06 13 02 55 53 11 0b 30 09 06 03 55 04 08 an Jose1...U...
0180 13 02 43 41 31 11 30 0f 06 03 55 04 07 13 08 53 ...Cisco1...U...
0190 61 6e 20 4a 6f 73 65 31 0e 30 0c 06 03 55 04 0a ...TAC1 0...U...
01a0 13 05 43 69 73 63 6f 31 0c 30 0a 06 03 55 04 0b ...rfp3.
01b0 13 03 54 41 43 31 20 30 1e 06 03 55 04 03 13 17 3.local1-0...*H
01c0 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 6c 65 79 .....tac@cisc
01d0 33 2e 6c 6f 63 61 6c 31 1c 30 1a 06 09 2a 86 48 o.com0...0...*H
01e0 86 f7 0d 01 09 01 16 0d 74 61 63 40 63 69 73 63 .....
01f0 6f 2e 63 6f 6d 30 82 01 22 30 0d 06 09 2a 86 48 .....
0200 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 .....0...

```

capin.pcap

Nota: você pode ver o certificado de servidor de VPN FTD no pacote dos “servidores hello enquanto nós conectamos à interface externa do FTD através do VPN. O PC do empregado confiará este certificado porque o PC do empregado tem o certificado CA raiz nele, e o certificado de servidor de VPN FTD foi assinado por essa mesma CA raiz.

Capture tomado no FTD do FTD que pede o servidor Radius se o username + a senha estão corretos (Cisco o ISE)

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets, with packet 2 selected. The packet list shows:

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

The details pane for packet 2 shows the following structure:

- 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)

The raw data pane shows the hex and ASCII representation of the RADIUS message. A blue arrow points to the ASCII string `jsmith (ReauthSe` in the hex dump.

Como você pode ver acima, nossa conexão de VPN obtém uma aceitação de acesso, e nosso cliente VPN de AnyConnect conecta com sucesso ao FTD através do VPN

A capturação (CLI) de FTD que pede Cisco ISE se o username + a senha são válidos (isto é certifica-se que as requisições RADIUS estão indo com sucesso entre FTD e ISE e se verifica para fora do que relação é que saem)

```

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

```

Abaixo do servidor Radius de Cisco ISE mostra essa autenticação bem sucedida. Clique a lupa para ver os detalhes da autenticação bem sucedida

Time	Source	Destination	Protocol	Length	Info
Oct 11, 2018 06:10:08.808 PM	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

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 no adaptador de AnyConnect do PC do empregado do PC do empregado que vai a um Web site interno através de HTTPS (isto é quando for com sucesso VPN'd dentro):

*Local Area Connection 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

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

Frame 49: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)

Internet Protocol Version 4, Src: 192.168.10.50, Dst: 192.168.10.50

Transmission Control Protocol, Src Port: 63576, Dst Port: 443, Seq: 0, Len: 0

Source Port: 63576

Destination Port: 443

```

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
    
```

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

Debugs

debugar o raio todo

debugar o anyconnect 255 do webvpn

Seja executado "debugam o raio todo o" comando em FTD CLI diagnóstico (apoio diagnóstico-CLI do >system) e batem o " conectar " no PC de Windows/Mac no 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 | bbe1f91.#.....i  
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
```

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

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 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 | 05bbe1f91
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 | be1f91
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 | 050005bbe1f91:co
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408
34 2f 31 39 33 31 36 38 32 | 4/1931682
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 32 (0x20)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 26 (0x1A)
Radius: Value (String) =
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f 72 | profile-name=Wor
6b 73 74 61 74 69 6f 6e | kstation
rad_procpkt: ACCEPT
Got AV-Pair with value profile-name=Workstation
RADIUS_ACCESS_ACCEPT: normal termination
radius mkreq: 0x16
alloc_rip 0x00002ace10874b80
new request 0x16 --> 17 (0x00002ace10874b80)
got user 'jsmith'
got password
add_req 0x00002ace10874b80 session 0x16 id 17
RADIUS_DELETE
remove_req 0x00002ace10875428 session 0x15 id 16
free_rip 0x00002ace10875428
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

```

RADIUS packet decode (authentication request)

```

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

```

```

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

```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 17 (0x11)

Radius: Length = 659 (0x0293)

Radius: Vector: C6FC11C10EC481AC09A785A883C1E488

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

Radius: Length = 8 (0x08)

Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith

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

Radius: Length = 18 (0x12)

Radius: Value (String) =

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

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

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5000

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

Radius: Length = 16 (0x10)

Radius: Value (String) =

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

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

Radius: Length = 16 (0x10)

Radius: Value (String) =

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

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

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

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

Radius: Length = 16 (0x10)

Radius: Value (String) =

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

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

Radius: Length = 35 (0x23)

Radius: Vendor ID = 9 (0x00000009)

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

Radius: Length = 29 (0x1D)

Radius: Value (String) =

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

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

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

Radius: Length = 44 (0x2C)

Radius: Vendor ID = 9 (0x00000009)

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

Radius: Length = 38 (0x26)

Radius: Value (String) =

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

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

66 2d 62 66 | f-bf

Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 51 (0x33)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 45 (0x2D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 58 (0x3A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 52 (0x34)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030
34 39 | 49
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 63 (0x3F)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 57 (0x39)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service
20 50 61 63 6b 20 31 | Pack 1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 49 (0x31)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 43 (0x2B)
Radius: Value (String) =
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
30 35 62 62 65 31 66 39 31 | 05bbe1f91
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 | 050005bbe1f91: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 | 05bbe1f91
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#

```

Seja executado 'debugam o comando do anyconnect 255' do webvpn em FTD CLI diagnóstico

(apoio diagnóstico-CLI do >system) e batem o " conectar " no PC de Windows/Mac no 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, 0x00002acdff1d6440, 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) & 0xffff0(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) & 0xffff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 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 > operações > RAI0 > logs vivos > detalhes do clique de cada autenticação

Verifique em Cisco ISE seu início de uma sessão VPN e o resultado "PermitAccess" ACL é dado
Vive o jsmith da mostra dos logs autenticado a FTD através do VPN com sucesso

Overview

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

Authentication Details

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

Steps

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

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

Other Attributes

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

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

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

Ciente VPN de AnyConnect

Pacote do DARDO

[Como recolher o pacote do DARDO para AnyConnect](#)

Troubleshooting

DNS

Verifique que Cisco ISE, FTD, Windows Server 2012, e PCs de Windows/Mac pode toda a resolução para a frente e o reverso (verificação DNS em todos os dispositivos)

PC Windows

Lance um comando prompt, e certifique-se que você pode executar um “nslookup” no hostname do 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, 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
```

> **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(cdtp) - 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, 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) & 0xffff0(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) & 0xffff0(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
```

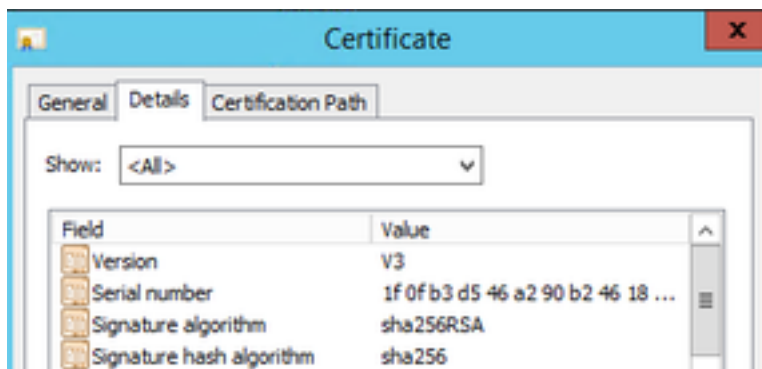
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false

Windows Server 2012

Lance um comando prompt, e certifique-se que você pode executar um “nslookup” no hostname/FQDN do FTD

Certificate a força (para a compatibilidade do navegador)

Verifique Windows Server 2012 Certificados dos sinais como SHA256 ou mais altamente. Fazer duplo clique seu certificado CA raiz em Windows e verifique da “os campos do algoritmo assinatura”



Se são SHA1, a maioria de navegadores mostrarão um aviso do navegador para aqueles Certificados. Para mudá-lo, você pode verificar aqui:

[Como promover a autoridade de certificação de Windows Server a SHA256](#)

Verifique que o certificado de servidor de VPN FTD tem os seguintes campos corretos (quando você conectar no navegador a FTD)

Common Name = <FTDFQDN>

Nome alternativo sujeito (SAN) = <FTDFQDN>

Exemplo:

Common Name: **ciscofp3.cisco.com**

Nome alternativo sujeito (SAN): **DNS Name=ciscofp3.cisco.com**

Conectividade e configuração de firewall

Verifique usando captações em FTD CLI e captações no PC do empregado usando Wireshark para verificar que os pacotes estão vindo sobre TCP+UDP 443 ao IP exterior do FTD. Verifique que aqueles pacotes são originado do endereço IP público do roteador home do empregado

```
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

...