

# مادختساب FTD ىلج AnyConnect VPN نيوكت Cisco ISE مادختساب RADIUS مداخك Server 2012 Root CA

## المحتويات

[المحتويات](#)

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[التكوين](#)

[تصدير شهادة المرجع المصدق الجذر من خادم Windows](#)

[ثبتت "شهادة المرجع المصدق الجذر" على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows/Mac](#)

[إنشاء CSR على FTD، والحصول على CSR الموقع من Windows Server Root CA، وثبتت تلك الشهادة](#)

[الموقعة على FTD](#)

[تنزيل صورة AnyConnect + محرر ملف تعريف AnyConnect وإنشاء ملف تعريف xml.](#)

[تكوين AnyConnect VPN على FTD \(إستخدام شهادة CA الجذر\)](#)

[تكوين قاعدة FTD NAT لإعفاء حركة مرور VPN من NAT لأنه سيتم فك تشفيرها على أي حال وإنشاء نهج/قواعد](#)

[التحكم في الوصول](#)

[إضافة FTD كجهاز شبكة وتكوين مجموعة النهج على Cisco ISE \(إستخدام سر RADIUS المشترك\)](#)

[تنزيل AnyConnect VPN Client وتثبته والاتصال ب FTD باستخدام AnyConnect VPN Client على أجهزة](#)

[الكمبيوتر الشخصية التي تعمل بنظام التشغيل Windows/Mac](#)

[التحقق من الصحة](#)

[نظام \(FTD\) Firepower Threat Defense](#)

[Cisco ISE](#)

[عمل AnyConnect VPN](#)

[استكشاف الأخطاء وإصلاحها](#)

[DNS](#)

[قوة الشهادة \(لتوافق المستعرض\)](#)

[الاتصال وتكوين جدار الحماية](#)

## المحتويات

### المقدمة

يصف هذا المستند كيفية تكوين AnyConnect VPN (الشبكة الخاصة الظاهرية) على جدار حماية (دفاع تهديد جدار الحماية من FTD) باستخدام Cisco ISE (محرك خدمات الهوية) كخادم RADIUS. إننا نستخدم Windows Server 2012 كمرجع مصدق جذري (مرجع مصدق) بحيث يتم تأمين الاتصال عبر VPN بواسطة الشهادات، أي أن كمبيوتر الموظف سيضمن شهادة FTD لأن شهادة FTD VPN تم توقيعها بواسطة Windows Server 2012 المرجع المصدق الجذر

## المتطلبات الأساسية

### المتطلبات

يجب نشر ما يلي وتشغيله في شبكتك:

- يتم نشر مركز إدارة Firepower وجدار حماية الحماية ضد تهديد Firepower مع إمكانية الاتصال الأساسية
  - نشر Cisco ISE وتشغيله في شبكتك
  - تم نشر Windows Server (مع Active Directory) وانضمام أجهزة الكمبيوتر الخاصة بالموظفين في Windows/Mac إلى مجال AD (Active Directory)
- في المثال التالي، سيقوم الموظفون بفتح "عميل AnyConnect" على جهاز الكمبيوتر الخاص بهم الذي يعمل بنظام التشغيل Windows/Mac، وسيقومون بالاتصال بأمان بالواجهة الخارجية ل FTD عبر الشبكة الخاصة الظاهرية (VPN) باستخدام بيانات الاعتماد الخاصة بهم. سيقوم FTD بالتحقق من اسم المستخدم وكلمة المرور مقابل Cisco ISE (الذي سيتم التحقق من صحته مع Windows Server Active Directory للتحقق من اسم المستخدم وكلمة المرور والمجموعة، أي يمكن فقط للمستخدمين في مجموعة 'AD' Employees إجراء VPN في شبكة الشركة.

### المكونات المستخدمة

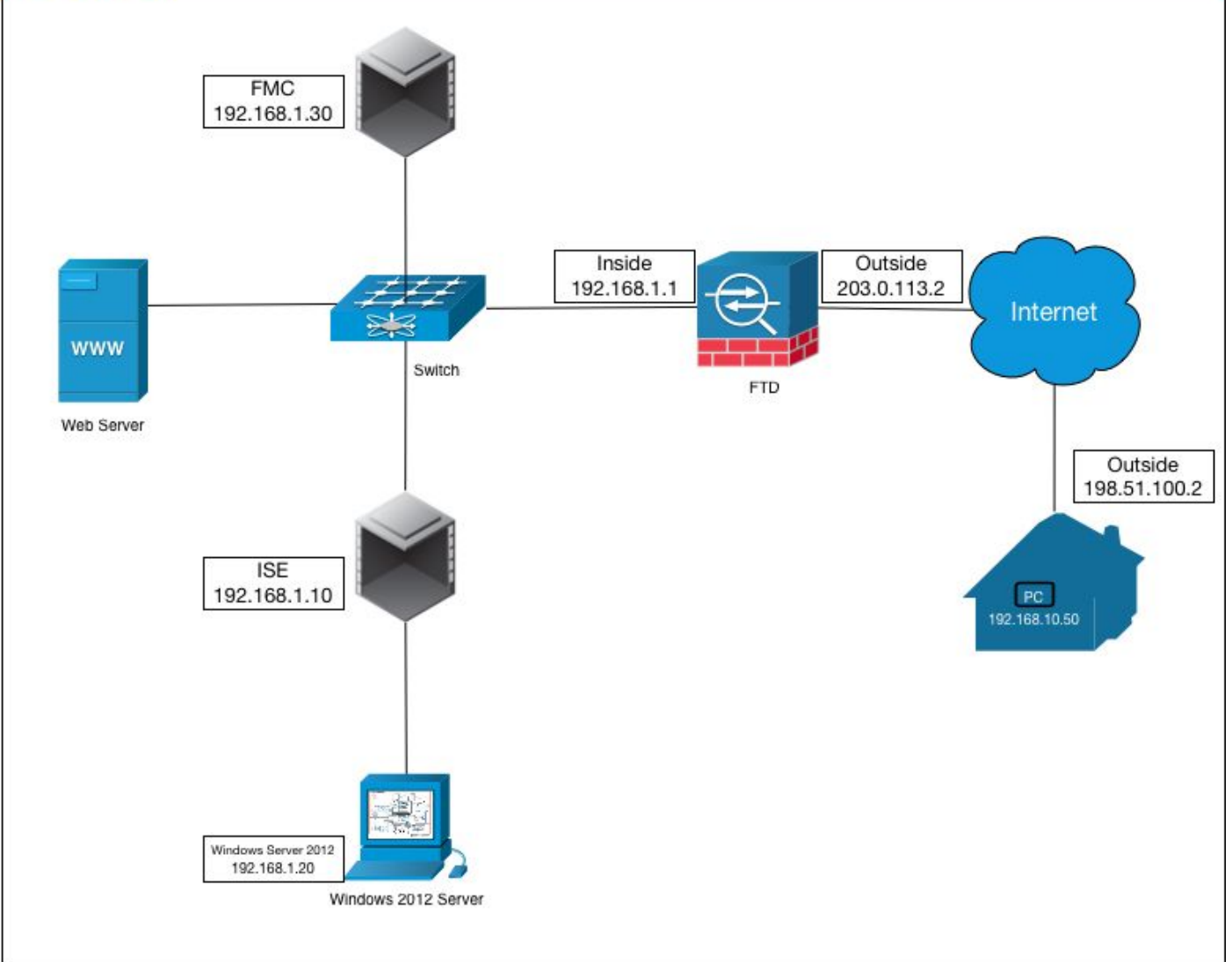
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- مركز إدارة Firepower والحماية ضد التهديد Firepower 6.2.3
- Cisco Identity Services Engine، الإصدار 2.4
- Cisco AnyConnect Secure Mobility Client الذي يعمل 4.6.03049
- Windows Server 2012 R2 الذي يقوم بتشغيل خدمة Active Directory وخدمات الشهادات (هذا هو المرجع المصدق الجذر الخاص بنا لجميع الشهادات)
- Windows 7 و Windows 10 وأجهزة الكمبيوتر Mac

## التكوين

### الرسم التخطيطي للشبكة

## Topology



في حالة الاستخدام هذه، سيقوم جهاز الكمبيوتر الشخصي Windows/Mac الخاص بالموظف الذي يقوم بتشغيل عميل AnyConnect VPN بالاتصال بعنوان IP العام الخارجي الخاص بجدار حماية FTD، وستقوم Cisco ISE بشكل ديناميكي بتمكينها من وصول محدود أو كامل إلى موارد معينة داخلية أو عبر الإنترنت (قابلة للتكوين) بمجرد إتصالها عبر شبكة VPN وفقا لمجموعة AD التي تكون عضوا فيها في Active Directory

اسم المضيف/FQDN	عنوان IP العام	عنوان IP الخاص	عنوان IP ل AnyConnect
	198.51.100.2	10.0.0.1	192.168.10.50

- 192.168.1.1 203.0.113.2 ciscofp3.cisco.com

- 192.168.1.30 -

- 192.168.1.10 - ciscoise.cisco.com

- 192.168.1.20 - ciscodc.cisco.com

- x.192,168,1 -

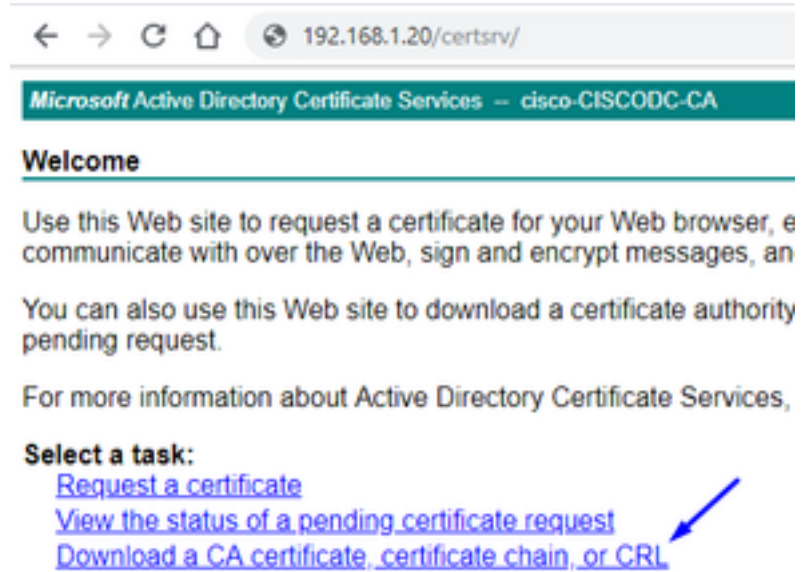
## التكوين

### تصدير شهادة المرجع المصدق الجذر من خادم Windows

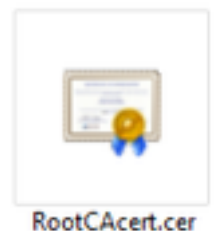
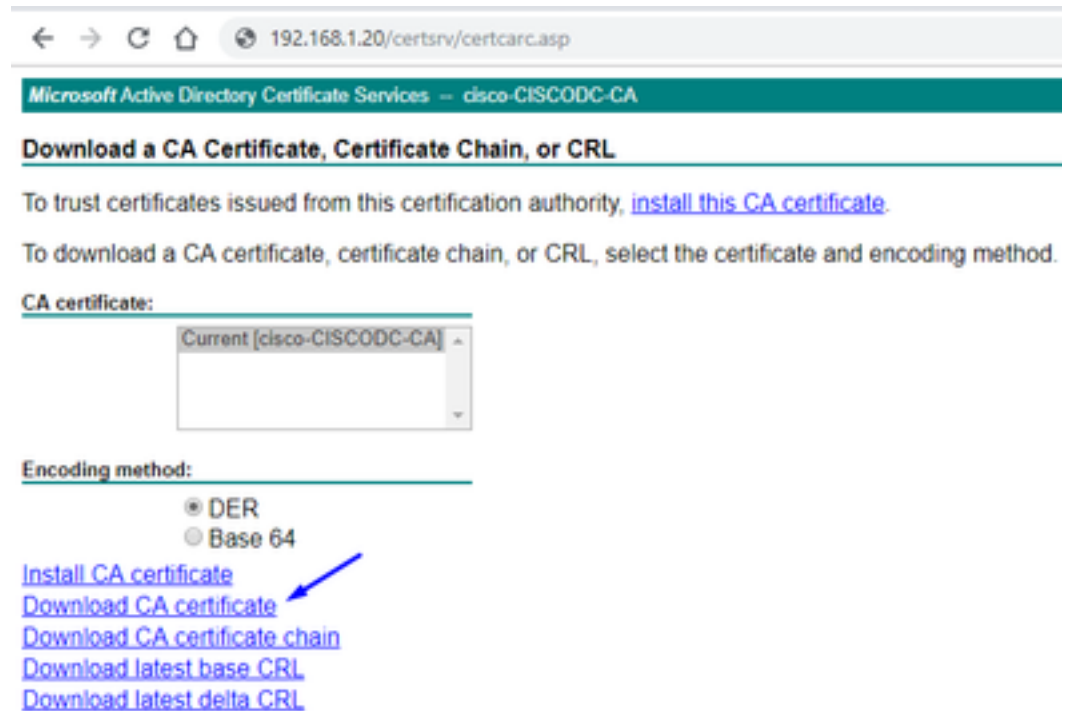
في هذا المستند، سنستخدم Microsoft Windows Server 2012 كمرجع مصدق جذري خاص بنا للشهادات. يثق الكمبيوتر العميل في هذا المرجع المصدق (CA) الجذري للاتصال بشكل آمن بـ FTD عبر الشبكة الخاصة الظاهرية (VPN) (انظر الخطوات التالية). سيضمن ذلك إمكانية الاتصال بشكل آمن ببرنامج الإرسال فائق السرعة (FTD) عبر الإنترنت والوصول إلى الموارد الداخلية من المنزل. سيثق الكمبيوتر الخاص بهم في الاتصال الموجود في المستعرض

انتقل إلى <http://192.168.1.20/certsrv> واتبع الخطوات التالية لتنزيل شهادة المرجع المصدق الجذر ل Windows Server:

انقر على تنزيل شهادة CA أو سلسلة الشهادات أو CRL



انقر فوق تنزيل الشهادة ثم أعد تسميتها إلى 'RootCAcert3.cer'



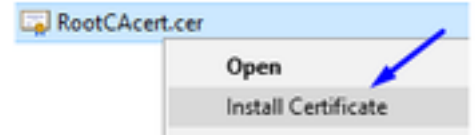
تثبيت "شهادة المرجع المصدق الجذر" على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows/Mac

**الطريقة 1:** قم بتثبيت الشهادة على كافة أجهزة الكمبيوتر الخاصة بالموظفين من خلال دفعها عبر نهج مجموعة خوادم Windows (مثالي لأي شيء يزيد عن 10 من مستخدمي شبكات VPN):

[كيفية استخدام Windows Server لتوزيع الشهادات على أجهزة الكمبيوتر العملية باستخدام نهج المجموعة](#)

**الطريقة 2:** قم بتثبيت الشهادة على جميع أجهزة الكمبيوتر الخاصة بالموظفين بتثبيتها بشكل فردي على كل جهاز كمبيوتر (مثالي لاختبار مستخدم شبكة VPN واحد):

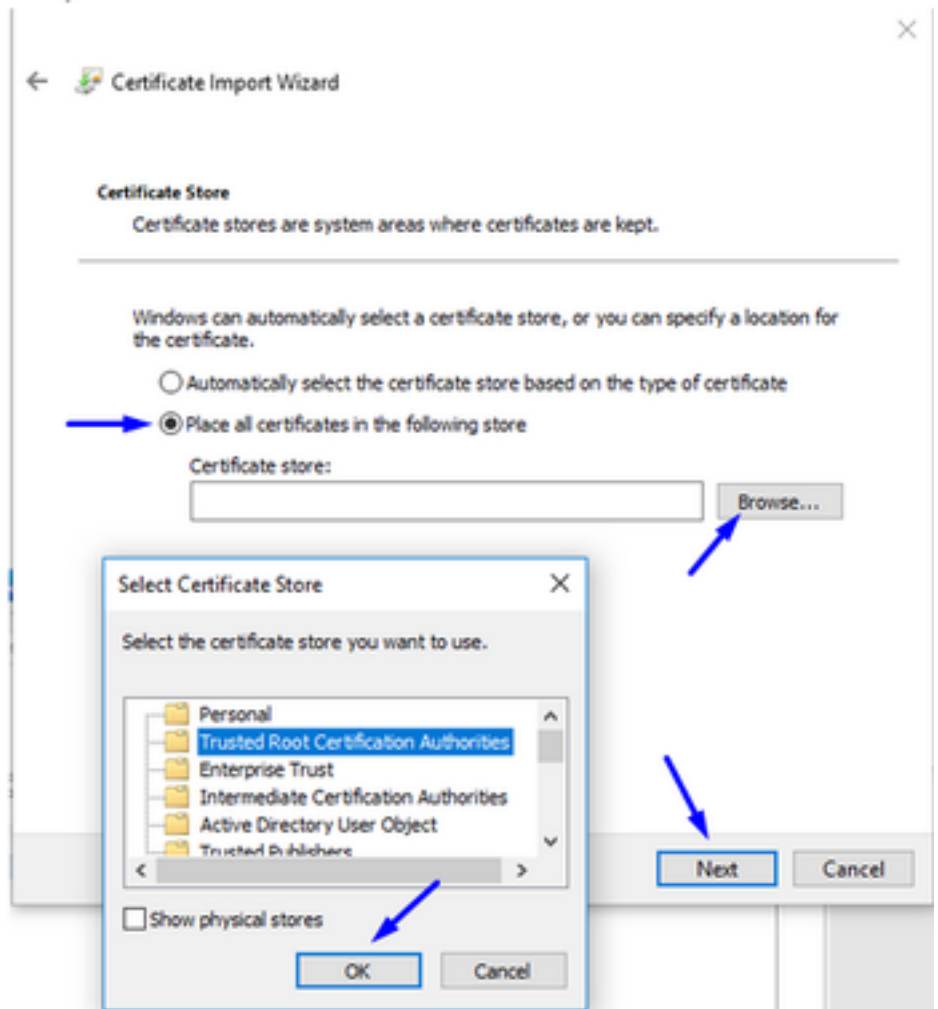
انقر بزر الماوس الأيمن على الشهادة الموجودة على الكمبيوتر الشخصي لموظفك في Windows/Mac وانقر فوق **تثبيت الشهادة**



تحديد 'المستخدم الحالي'

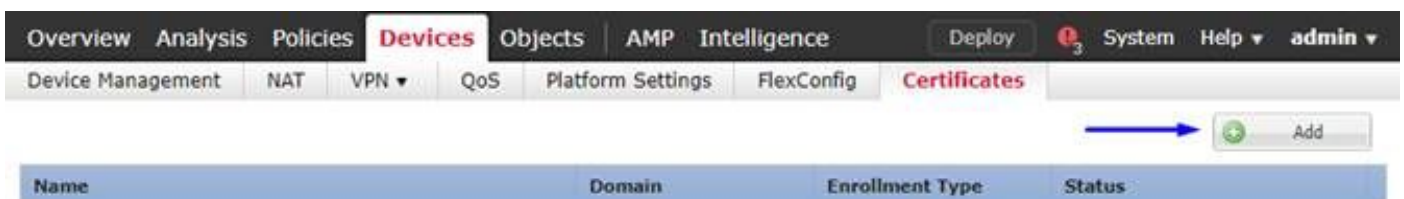


حدد وضع كل الشهادات في المتجر التالي وحدد مراجع التصديق الجذر الموثوقة، وانقر موافق، وانقر التالي، وانقر نهاية



إنشاء CSR على FTD، والحصول على CSR الموقع من Windows Server Root CA، وتثبيت تلك الشهادة  
الموقعة على FTD

انتقل إلى الكائنات < إدارة الكائنات < PKI < التسجيل لـ Cert، انقر فوق إضافة تسجيل Cert




انقر فوق الزر إضافة تسجيل الثقة



**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\*:  

حدد نوع التسجيل < يدوي  
كما يظهر في الصورة أدناه، نحن بحاجة إلى لصق شهادة المرجع المصدق الجذر هنا:

**Add Cert Enrollment** ? X

Name\*:

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

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

Allow Overrides:

فيما يلي كيفية تنزيل شهادة المرجع المصدق الجذر وعرضها بتنسيق نصي ولصقها في المربع أعلاه:

انتقل إلى <http://192.168.1.20/certsrv>

انقر على تنزيل شهادة CA أو سلسلة الشهادات أو 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](#)

انقر على زر أساس 64 < تنزيل شهادة المرجع المصدق

← → ↻ 🏠 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.

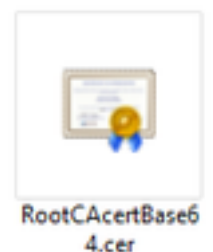
CA certificate:

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](#)



افتح ملف RootCAcertBase64.cer في Notepad

قم بنسخ محتويات cer. (شهادة مرجع مصدق جذري) ولصقها من Windows AD Server هنا:

## Add Cert Enrollment



Name:\*

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:\*  

```
-----BEGIN CERTIFICATE-----
MIIBKjCCARAgAwIBAgIQDzR0KCRWEERAAaVZMhQWCVYTDVK0PBAQDRgDGMFA8QAI0UEW
EB/wQFMAMBAf8wHQYD
VR0OBBYEF0lpC7y9musCkmDJaKVus9bJUoMiMBAGCSsGAQQBg
jcVAQQDAgEBMCMG
CSsGAQQBgjcVAgQWBBQXIqPq2/dCT41fyYZHPxKhGEYNnzANBg
kqhkiG9w0BAQsF
AAOCAQEAOTa5S8Zw7RfarjTGm7HHJHZsA2p9CHdsvB/I35nYeqc
OnxyeTWFN7by6
C43uyBfTWTpU3Ljr1mCgEo72qJErJOoU/Y4y7ADAKJF8RtUIb4H
Zq13XNW7Tu9X
DbZCTeYL7INbzZxPyfcuZWIBk5I8uHRvqq2YkBdx6YUYJocNTshH
WwZIXYvQPwwc
yjHrFjm0/YIIQIJMhyIVULXXxWGP7diLIEQ67aHsdz+UZq9JofvYa
heHBjzbiF
zvN2WwFXQs3mFMUxkrjEyzNIDws6vrm6ZhajvOupzmeC6YqByK
QIEAggjevemL7Zd
8DufTZQ4E4VQ9Kp4hrSdzuHSggDTuw==
-----END CERTIFICATE-----
```

Allow Overrides:

انقر على علامة تبويب **معلومات الشهادات** << اكتب معلومات الشهادة الخاصة بك

ملاحظة:

يجب أن يكون حقل FQDN المخصص هو FTD الخاص بك

يجب أن يكون حقل الاسم الشائع هو FTD الخاص بك

## Add Cert Enrollment

? X

Name:\*

Description:

CA Information Certificate Parameters Key Revocation

Include FQDN:

Custom FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides:

Save Cancel

تلميح: يمكنك الحصول على FTD الخاص بك من خلال كتابة الأمر التالي من واجهة سطر الأوامر (CLI) الخاصة ب  
:FTD

```
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
```

انقر فوق علامة التبويب مفتاح واكتب أي اسم مفتاح

**Add Cert Enrollment** ? X

Name:\* FTDVPNServerCert

Description: FTD AnyConnect VPN Server Certificate

CA Information Certificate Parameters **Key** Revocation

Key Type:  RSA  ECDSA

Key Name:\* CiscoTACRSAkey

Key Size: 2048

**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

لقطة حفظ

حدد FTDVPNServerCert الذي أنشأناه أعلاه للتو وانقر فوق إضافة

**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\*: FTDVPNServerCert

**Cert Enrollment Details:**

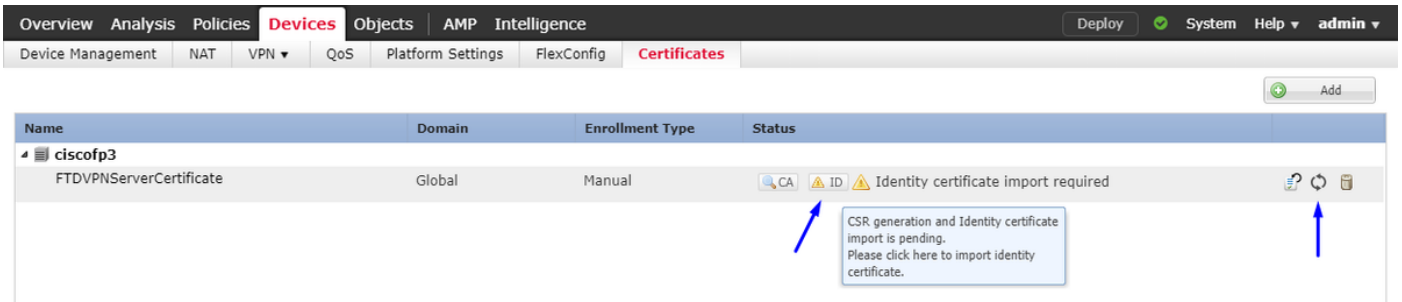
Name: FTDVPNServerCert

Enrollment Type: Manual

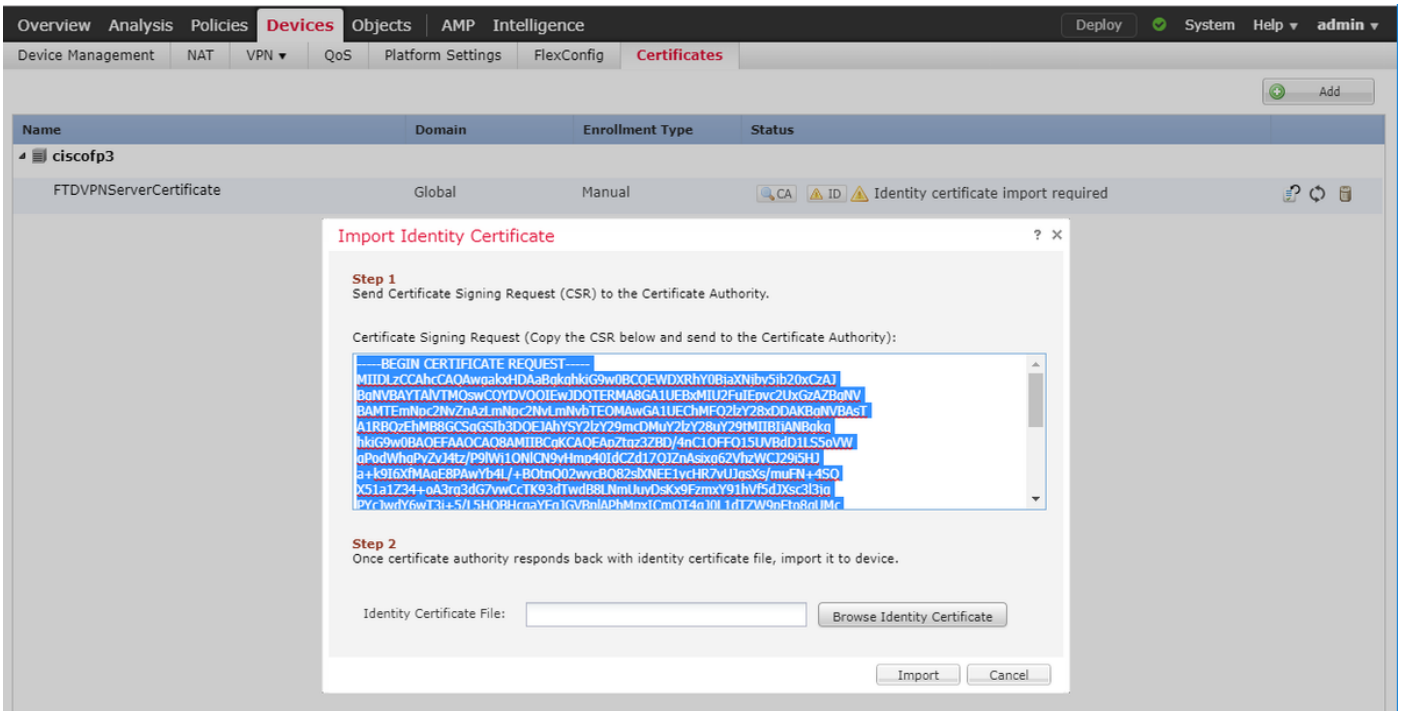
SCEP URL: NA

Add Cancel

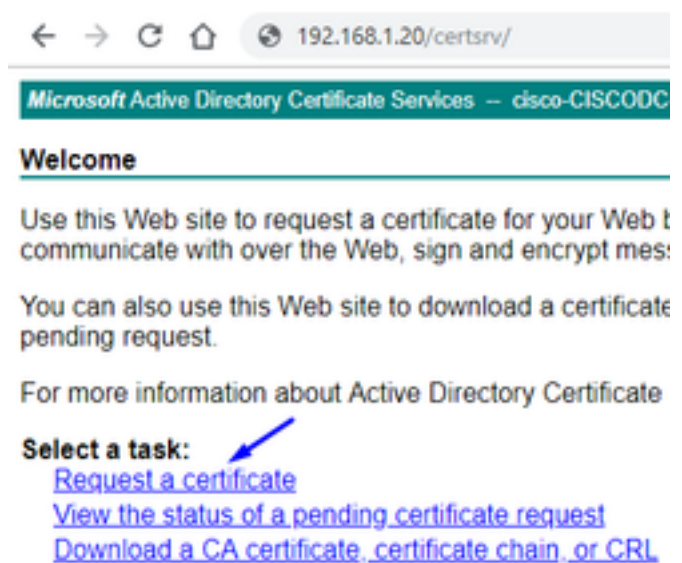
تلميح: انتظر حوالي 10-30 ثانية حتى يتحقق FMC + FTD من شهادة CA الجذر وثبيتها (انقر فوق رمز التحديث إذا لم تظهر)



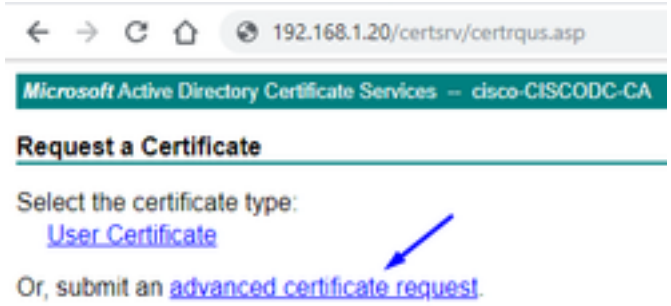
قم بنسخ هذه CSR ولصقها، وأخذها إلى المرجع المصدق الجذر ل Windows Server الخاص بك:



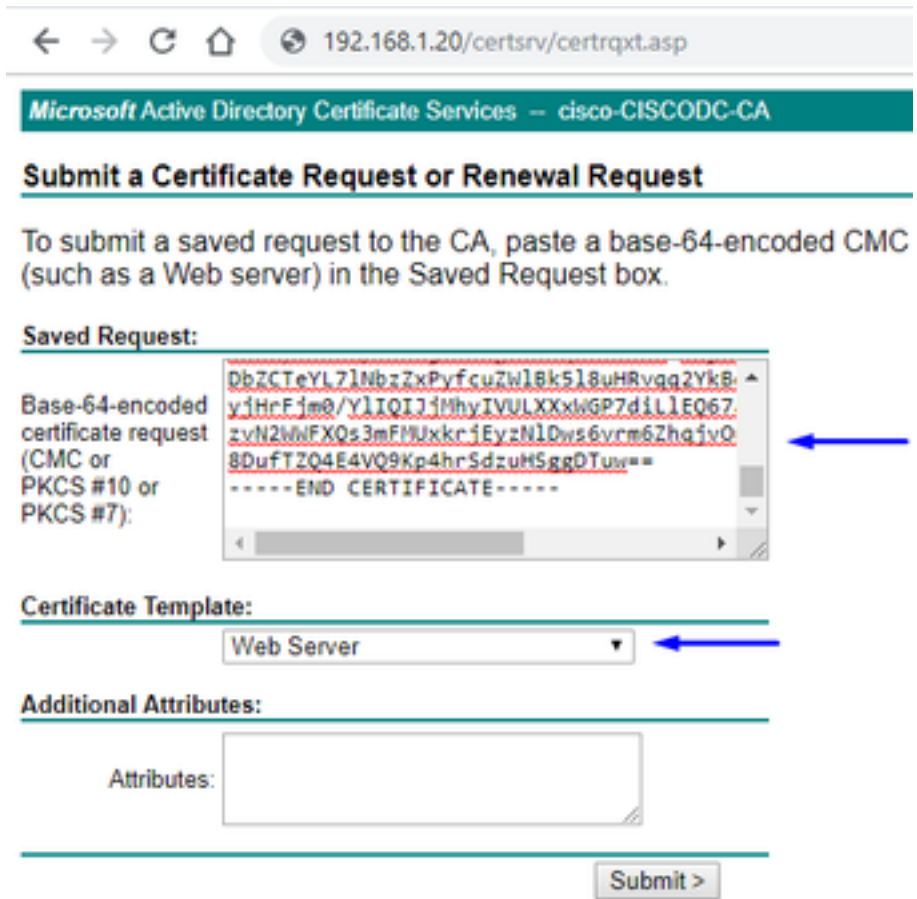
انتقل إلى <http://192.168.1.20/certsrv>



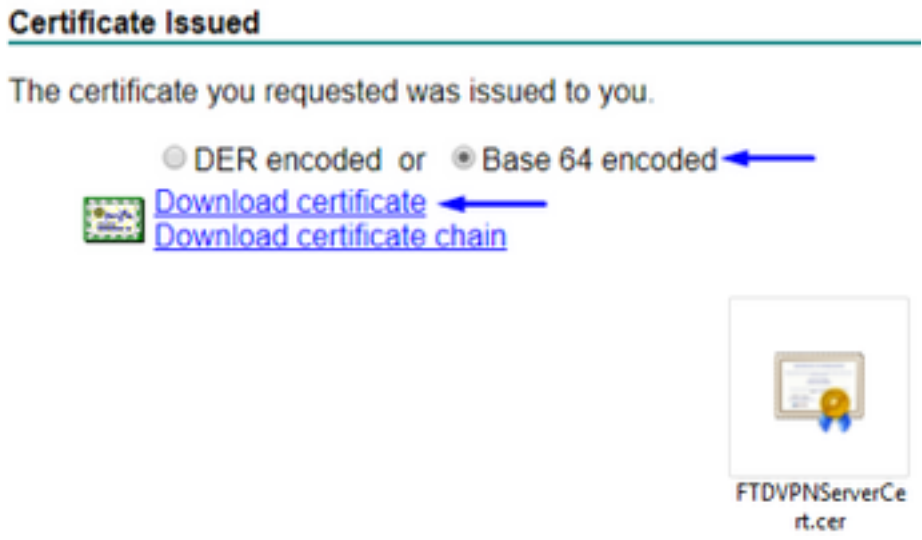
انقر على طلب شهادة متقدمة



الصق طلب توقيع الشهادة (CSR) في الحقل أدناه وحدد خادم الويب كقالب الشهادة

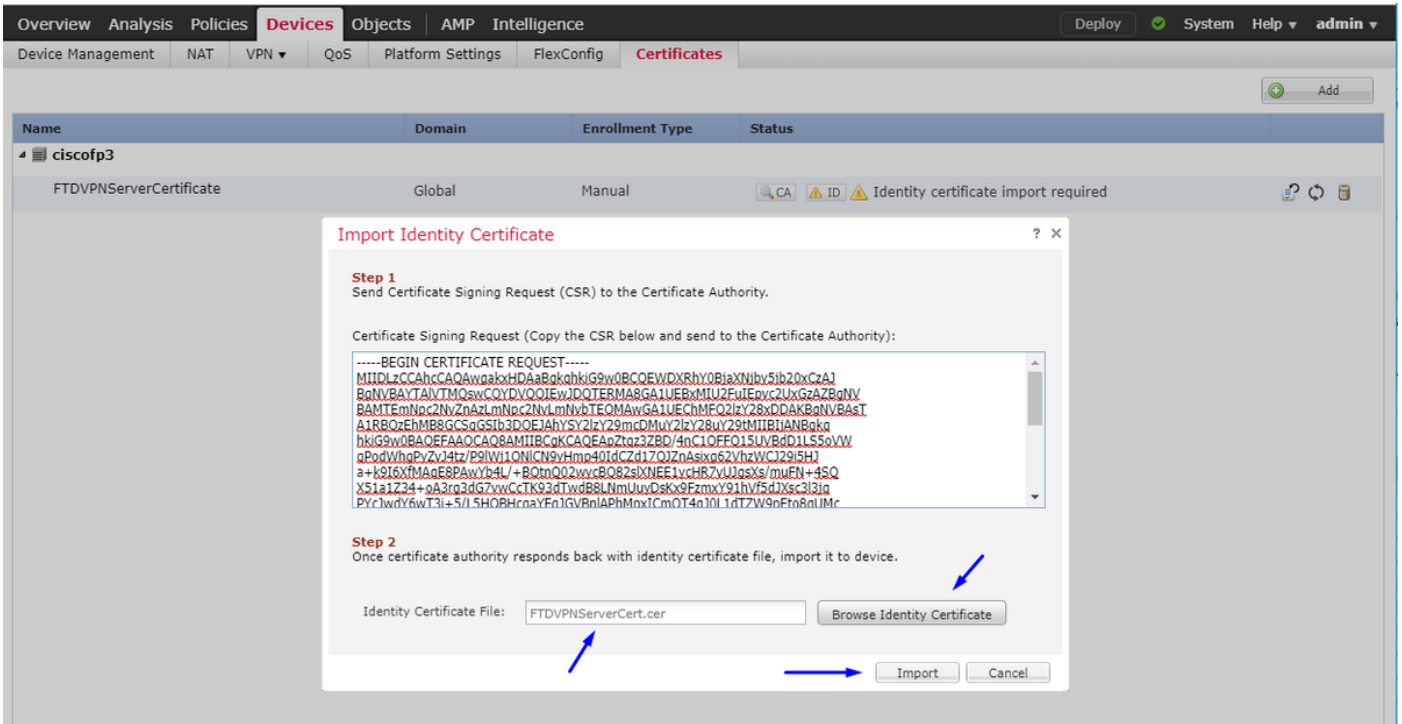


انقر على إرسال  
طققت base 64 برمز زر وطققة تنزيل شهادة

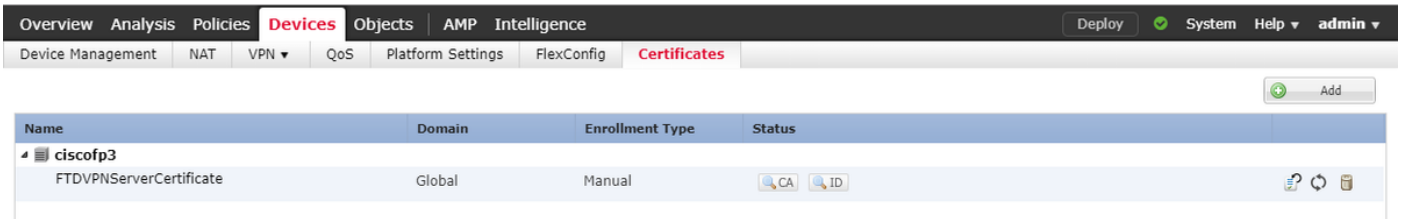




## انقر على إستمراض شهادة الهوية وحدد الشهادة التي قمنا بتزيلها للتو



تم تثبيت "شهادة خادم VPN ل FTD" (الموقعة من قبل Windows Server Root CA) بنجاح



## تنزيل صورة AnyConnect + محرر ملف تعريف AnyConnect وإنشاء ملف تعريف .xml

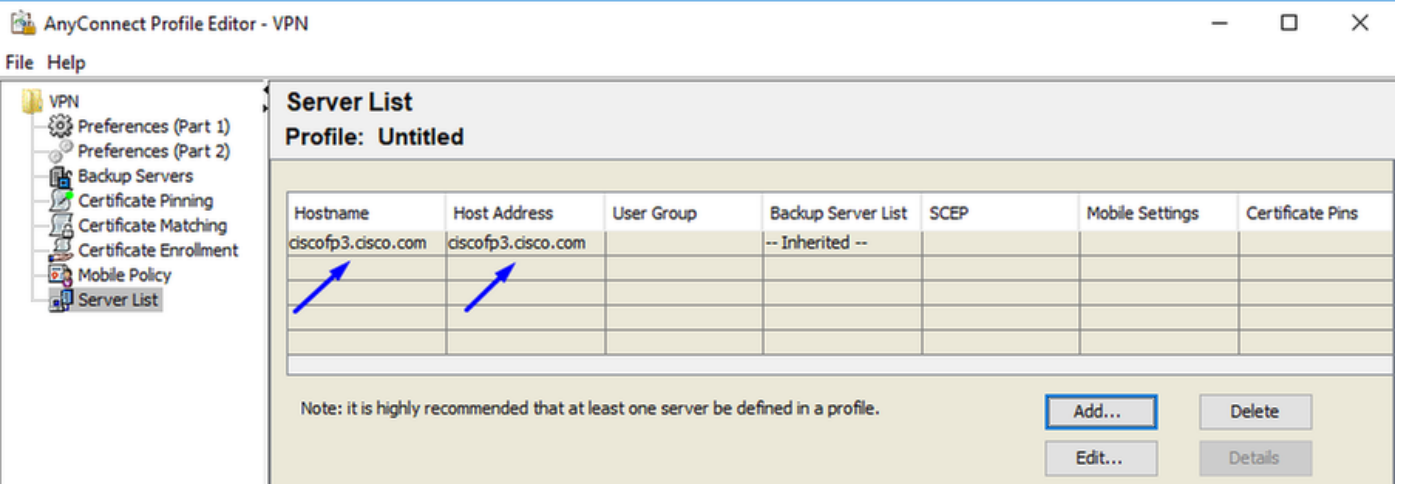
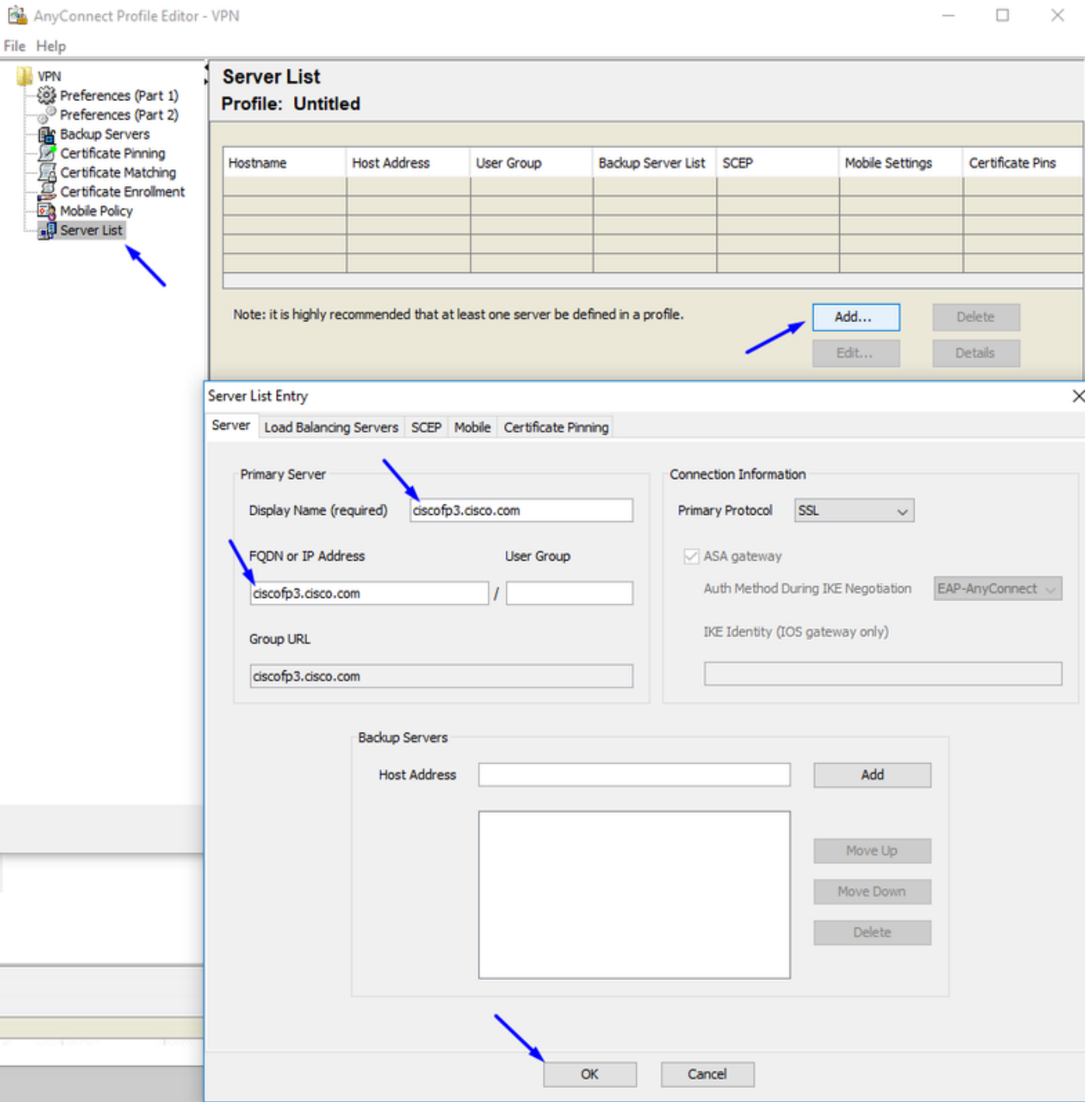
تنزيل [محرر ملف تعريف AnyConnect من Cisco](#) وتثبيته



فتح محرر ملف تعريف AnyConnect  
 طقطقت نادل قائمة <طقطقة يضيف..

اكتب اسم العرض و FQDN من عنوان IP الخاص بالواجهة الخارجية ل FTD الخاص بك. يجب أن ترى الإدخالات في قائمة الخوادم





انقر فوق موافق وملف < حفظ باسم...

تنزيل صور Windows و Mac .pkg من [هنا](#)

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		

انتقل إلى الكائنات < إدارة الكائن < VPN < ملف AnyConnect < انقر إضافة ملف AnyConnect

**Edit AnyConnect File** ? x

Name:\* AnyConnect\_Windows\_4.6.03049

File Name:\* anyconnect-win-4.6.03049-webdeploy-k9.pk

File Type:\* AnyConnect Client Image

Description: Cisco AnyConnect Image for Windows PCs

**Add AnyConnect File** ? x

Name:\* AnyConnect\_Mac\_4.6.03049

File Name:\* anyconnect-macos-4.6.03049-webdeploy-k9

File Type:\* AnyConnect Client Image

Description: Cisco AnyConnect Image for Mac PCs

تكوين AnyConnect VPN على FTD (إستخدام شهادة CA الجذر)

تسجيل الدخول إلى مركز إدارة FirePOWER  
 انقر فوق نظام < تكامل < Realms < انقر فوق عالم جديد < انقر فوق علامة التبويب Directory < انقر فوق  
 إضافة دليل

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

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

isetofmc Save Cancel

Integrate FirePOWER Management Center with Active Directory server

Directory Realm Configuration User Download Add directory

URL (Hostname/IP Address and Port)	Encryption
10.201.214.228:389	none

**Edit directory** ? X

Hostname / IP Address: 192.168.1.20

Port: 389

Encryption:  STARTTLS  LDAPS  None

SSL Certificate:  +

OK Test Cancel

انقر فوق علامة التبويب تكوين النطاق - قم بتكوين معلومات وحدة التحكم بالمجال الخاصة بك هنا

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

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

isetofmc Save Cancel

Integrate FirePOWER Management Center with Active Directory server

Directory **Realm Configuration** User Download

AD Primary Domain \*  ex: domain.com

AD Join Username  ex: user@domain

AD Join Password  Test AD Join

Directory Username \*  ex: user@domain

Directory Password \*

Base DN \*  ex: ou=user,dc=cisco,dc=com

Group DN \*  ex: ou=group,dc=cisco,dc=com

Group Attribute

**User Session Timeout**

User Agent and ISE/ISE-PIC Users  minutes until session released.

TS Agent Users  minutes until session released.

Captive Portal Users  minutes until session released.

Failed Captive Portal Users  minutes until session released.

Guest Captive Portal Users  minutes until session released.

\* Required Field

ملاحظة: في المثال أعلاه، يتم استخدام اسم مستخدم AD مع امتيازات "مسؤول المجال" في Windows AD Server. إذا كنت ترغب في تكوين مستخدم بمزيد من التحديد، الحد الأدنى من الأذونات ل FMC للانضمام إلى مجال Active Directory الخاص بك لتكوين المجال، يمكنك رؤية الخطوات [هنا](#)

انقر فوق علامة التبويب تنزيل المستخدم - تأكد من نجاح تنزيل المستخدم

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

قطعة أداة VPN وصول عن بعد <قطعة يضيف

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

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

Name Status Last Modified

No configuration available Add a new configuration

Add

اكتب اسم، وصف، وانقر فوق إضافة لتحديد جهاز FTD الذي تريد تكوين VPN AnyConnect عليه

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.

انقر على إضافة لخدم المصادقة واختر مجموعة خوادم RADIUS - وستكون هذه هي العقدة PSN الخاصة بمحرك خدمات الهوية من Cisco

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

**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:

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:

Buttons: Back Next Cancel

اكتب اسم لخدم RADIUS  
 حدد النطاق الذي تم تكوينه أعلاه  
 قطعة يضيف

**Add RADIUS Server Group** ? X

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

Buttons: Save Cancel

اكتب المعلومات التالية لعقدة Cisco ISE الخاصة بك:  
 عنوان IP/اسم المضيف: عنوان IP الخاص ب Cisco ISE PSN (عقدة خدمة السياسة) - هذا هو المكان الذي  
 ستذهب إليه طلبات المصادقة  
 المفتاح: Cisco123

تحذير: أعلاه هو مفتاح سر RADIUS المشترك - سنستخدم هذا المفتاح في خطوة لاحقة

**Edit RADIUS Server**
? X

IP Address/Hostname: *	<input type="text" value="192.168.1.10"/>	
<small>Configure DNS at Threat Defense Platform Settings to resolve hostname</small>		
Authentication Port: *	<input type="text" value="1812"/>	(1-65535)
Key: *	<input type="password" value="*****"/>	
Confirm Key: *	<input type="password" value="*****"/>	
Accounting Port:	<input type="text" value="1813"/>	(1-65535)
Timeout:	<input type="text" value="10"/>	(1-300) Seconds
Connect using:	<input checked="" type="radio"/> Routing <input type="radio"/> Specific Interface <span style="font-size: 0.8em;">i</span>	
	<input type="text"/> <span style="float: right;">v +</span>	
Redirect ACL:	<input type="text"/> <span style="float: right;">v +</span>	

ملاحظة: عندما يحاول المستخدم النهائي الاتصال ب FTD عبر AnyConnect VPN، سيتم إرسال اسم المستخدم + كلمة المرور التي يكتبها كطلب مصادقة إلى FTD. هذا. سيقوم FTD بإعادة توجيه هذا الطلب إلى عقدة Cisco ISE PSN للمصادقة (سيقوم Cisco ISE بعد ذلك بالتحقق من Windows Active Directory لمعرفة اسم المستخدم وكلمة المرور تلك، وفرض التحكم في الوصول/الوصول إلى الشبكة استنادا إلى الحالة التي قمنا بتكوينها حاليا في 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

طقطقة حفظ  
طقطقة يحرر ل IPv4 عنوان بركة

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:** DftGrpPolicy (Edit Group Policy)

Back Next Cancel

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

How-To Cisco

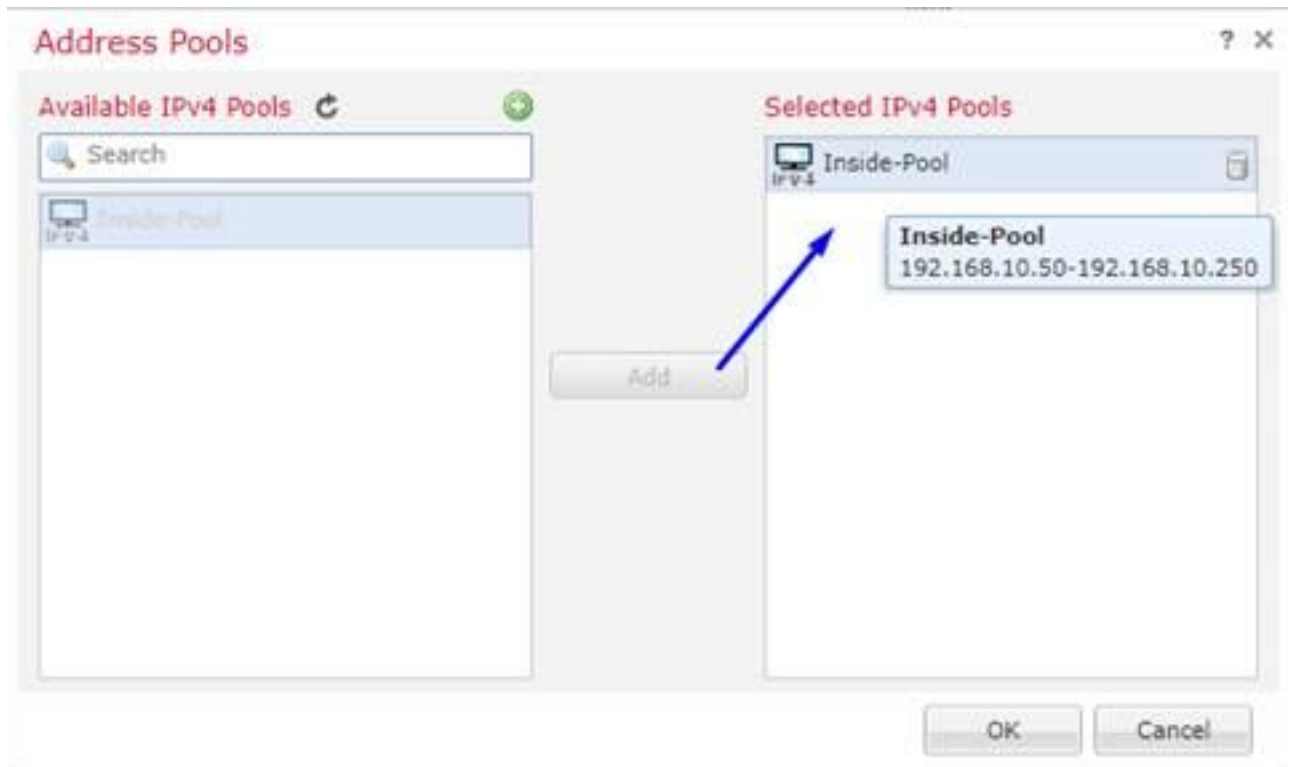
طقطقة يضيف



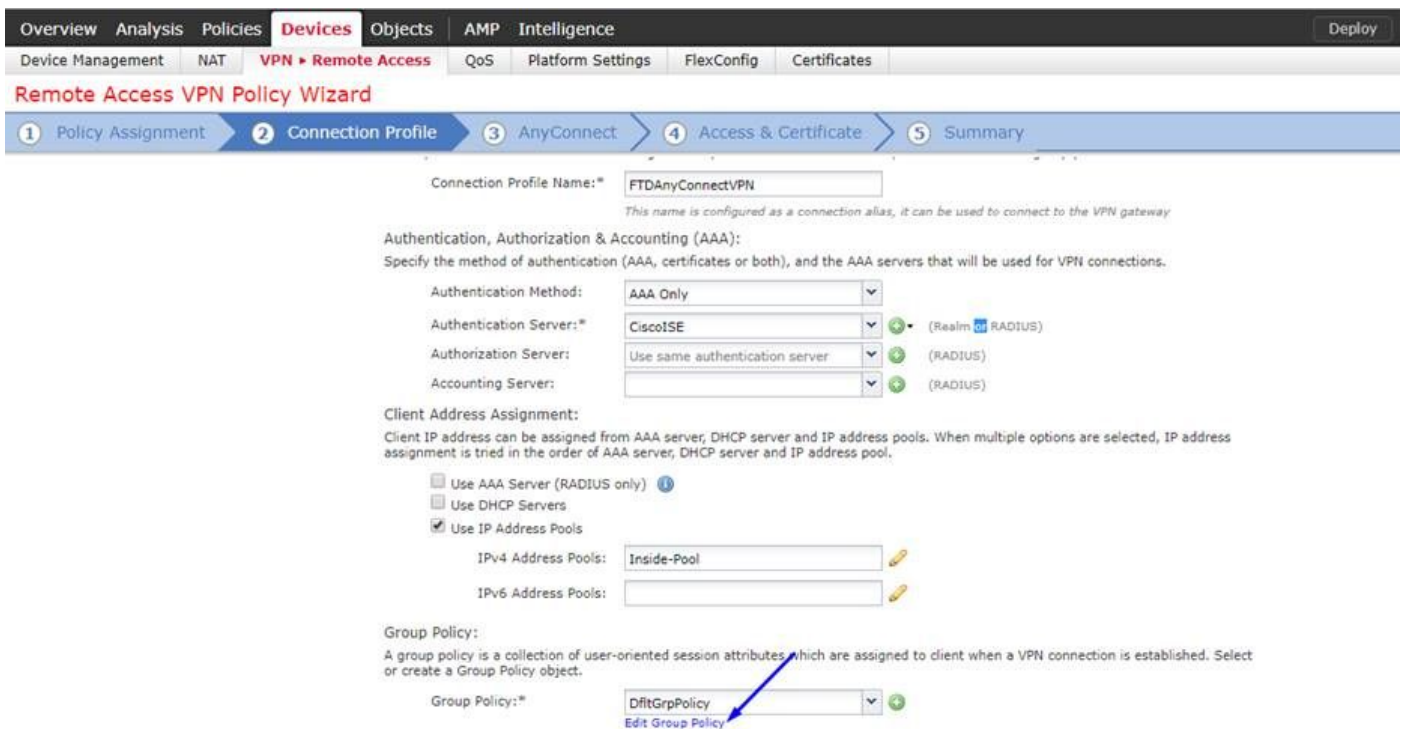
اكتب اسم، ونطاق عنوان IPv4، وقناع الشبكة الفرعية

حدد تجمع عناوين IP وانقر فوق موافق





انقر فوق تحرير نهج المجموعة



انقر على علامة تبويب AnyConnect < توصيفات > انقر على إضافة

## Edit Group Policy

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](#).

اكتب اسم وانقر إستعراض.. وحدد ملف VPNprofile.xml من الخطوة 4 أعلاه

Overview Analysis Policies Devices Objects AMP Intelligence

Device Management NAT VPN Remote Access QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Edit Group Policy

Name:\* DfitGrpPolicy

Description:

General AnyConnect Advanced

Profiles

SSL Settings

Connection Settings

AnyConnect XML Profile

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

طقطقة حفظ وطقطقة بعد ذلك

حدد خانات الاختيار لملف AnyConnect Windows/Mac من الخطوة 4 أعلاه

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

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

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

Download AnyConnect Client packages from [Cisco Software Download Center](#). Show Re-order buttons

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyConnect_Mac_4.603049	anyconnect-macos-4.6.03049-webdeploy-k9...	Mac OS
<input checked="" type="checkbox"/>	AnyConnect_Windows_4.6.03049	anyconnect-win-4.6.03049-webdeploy-k9.pkg	Windows

Back Next Cancel

طقطقت بعد ذلك  
حدد مجموعة الواجهة/منطقة الأمان كخارج الشبكة  
حدد تسجيل الشهادة كشهادة خاصة بك قمنا بإجرائها في الخطوة 3 أعلاه

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

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

**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

راجع التكوين الخاص بك وانقر فوق التالي

**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

تكوين قاعدة NAT FTD لإعفاء حركة مرور VPN من NAT لأنه سيتم فك تشفيرها على أي حال وإنشاء نهج/قواعد التحكم في الوصول

خلقت قاعدة nat ساكن إستاتيكي أن يتأكد ال VPN حركة مرور لا يحصل FTD (FTD NAT d) بالفعل يفك تشفير AnyConnect ربط بما أن هم يأتون إلى القارن خارجي، لذلك هو كما لو أن pc يكون بالفعل خلف القارن داخلي، وأنهم لديهم بالفعل عنوان IP خاص - نحن بعد بحاجة إلى تكوين قاعدة NAT-Exempt (nat-لا) لحركة مرور VPN تلك):

انتقل إلى الكائنات < انقر فوق إضافة شبكة < انقر فوق إضافة كائن

### Edit Network Objects

Name:

Description:

Network:

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:

Example_Company_NAT_Policy											
NAT policy											
Rules											
Filter by Device											
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
1		Static	Inside	Outside	inside-subnet	outside-subnet-anyconnect-pool		inside-subnet	outside-subnet-anyconnect-pool		<input type="checkbox"/> Dns: false <input type="checkbox"/> route-lookup <input type="checkbox"/> no-proxy-arp
▼ Auto NAT Rules											
#		Dynamic	Inside	Outside	inside-subnet			Interface			<input type="checkbox"/> Dns: false
▼ NAT Rules After											

وبالإضافة إلى ذلك، يجب أن تسمح لحركة مرور البيانات بالتدفق بعد دخول شبكات VPN الخاصة بالمستخدم. لديك خيارين لهذا:

أ. قم بإنشاء قواعد السماح أو الرفض للسماح لمستخدمي شبكات VPN أو رفضها بالوصول إلى موارد معينة

ب. قم بتمكين "سياسة التحكم بالوصول الالتفافي لحركة المرور التي تم فك تشفيرها" - وهذا يسمح لأي شخص قادر على الاتصال ب FT D بنجاح عبر قوائم التحكم في الوصول (ACL) الخاصة بالشبكة الخاصة الظاهرية (VPN) الالتفافية والوصول إلى أي شيء خلف FT D دون المرور على قواعد "السماح أو الرفض" في نهج التحكم في الوصول

تمكين نهج التحكم في الوصول الالتفافي لحركة المرور التي تم فك تشفيرها ضمن: الأجهزة < VPN < الوصول عن بعد < ملف تعريف VPN < واجهات الوصول:

#### 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.

ملاحظة: إذا لم تقم بتمكين هذا الخيار، فستحتاج إلى الانتقال إلى السياسات < نهج التحكم في الوصول وإنشاء قواعد السماح لمستخدمي الشبكة الخاصة الظاهرية (VPN) للتمكن من الوصول إلى الأشياء الموجودة داخل المنطقة أو المنطقة الإدارية الخاصة (DMZ)

انقر فوق Deployment في أعلى يمين مركز إدارة FirePOWER

إضافة FT D كجهاز شبكة وتكوين مجموعة النهج على Cisco ISE (إستخدام سر RADIUS المشترك)

قم بتسجيل الدخول إلى Cisco Identity Services Engine (محرك خدمات الهوية من Cisco) وانقر فوق إدارة < أجهزة الشبكة < انقر إضافة



Network Devices

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

اكتب اسم، واكتب عنوان IP الخاص ب FTD، واكتب سر RADIUS المشترك من الخطوات أعلاه  
 تحذير: يجب أن يكون هذا هو الواجهة/عنوان IP الذي يمكن أن يصل إلى FTD (إلى خادم RADIUS Cisco ISE) أي  
 واجهة FTD التي يمكن ل Cisco ISE الوصول إلى FTD منها

Network Devices List > FTDVPN

Network Devices

\* Name: FTDVPN

Description:

IP Address: \* IP: 192.168.1.1 / 32

\* Device Profile: AlcatelWired

Model Name:

Software Version:

\* Network Device Group

Location: All Locations [Set To Default]

IPSEC: No [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

\* Shared Secret: cisco123 [Hide]

Use Second Shared Secret:  [i]

CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings [i]

DTLS Required:  [i]

Shared Secret: radius/dtls [i]

CoA Port: 2083 [Set To Default]

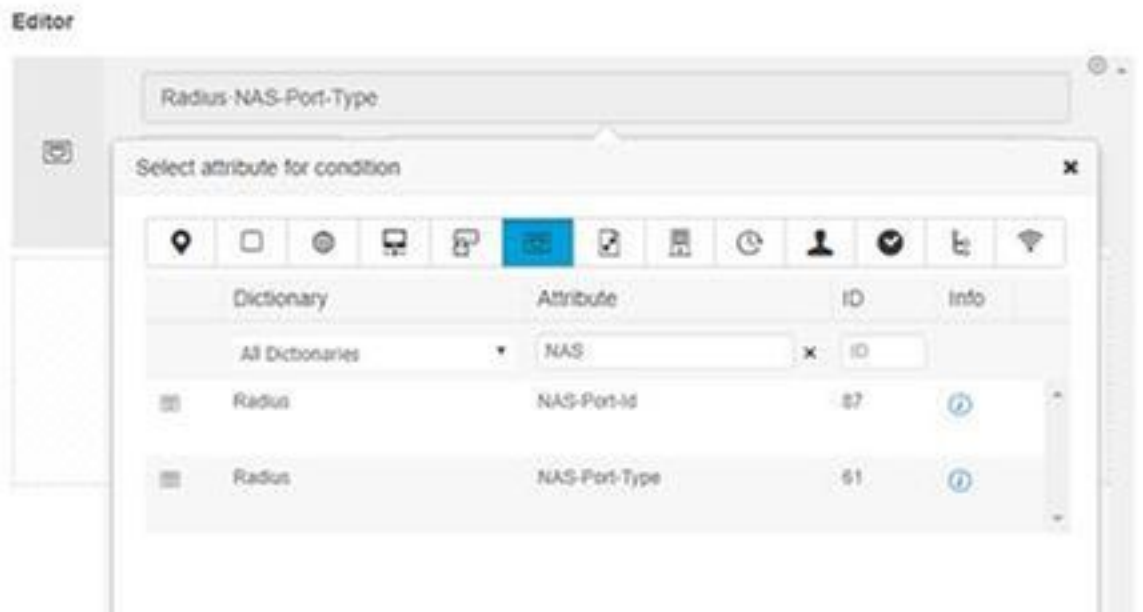
انقر فوق سياسة <مجموعة السياسات> إنشاء مجموعة سياسات لأي طلبات مصادقة تأتي من النوع التالي:

## RADIUS-NAS-Port-type يساوي الافتراضي

وهذا يعني أنه إذا طلب أي من RADIUS أن يأتي إلى ISE الذي يبدو كاتصالات VPN، فسوف يؤثر على مجموعة النهج هذه

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	GuestSSID		Airspace Airspace-Wan-Id EQUALS 1	Default Network Access	181		
✔	EmployeeSSID		Airspace Airspace-Wan-Id EQUALS 2	Default Network Access	686		
✔	VPN Users		Radius-NAS-Port-Type EQUALS Virtual	Default Network Access			
✔	Default	Default policy set		Default Network Access	1380		

هنا حيث أنت تستطيع وجدت أن شرط في cisco ISE:



تحرير مجموعة النهج التي قمت بإنشائها أعلاه  
أضف قاعدة أعلى قاعدة الحظر الافتراضية لمنح الأشخاص ملف تعريف تخويل السماح بالوصول " فقط إذا كانوا في مجموعة Active Directory التي تسمى الموظفين:

Policy Sets → VPN Users

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

Authentication Policy (2)

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

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

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

Reset Save

ما يلي هو شكل قاعدتك بمجرد اكتمالها

Policy Sets → VPN Users

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

Authentication Policy (2)

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

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

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

Reset Save


تنزيل AnyConnect VPN Client وتثبيته والاتصال ب FTD باستخدام AnyConnect VPN Client على أجهزة الكمبيوتر الشخصية التي تعمل بنظام التشغيل Windows/Mac

افتح المستعرض الخاص بك على كمبيوتر Windows/Mac للموظف، وانتقل إلى العنوان الخارجي الخاص ب FTD في المستعرض الخاص بك

← → ↻ <https://cisconf3.cisco.com>

اكتب اسم مستخدم وكلمة مرور Active Directory





### Logon

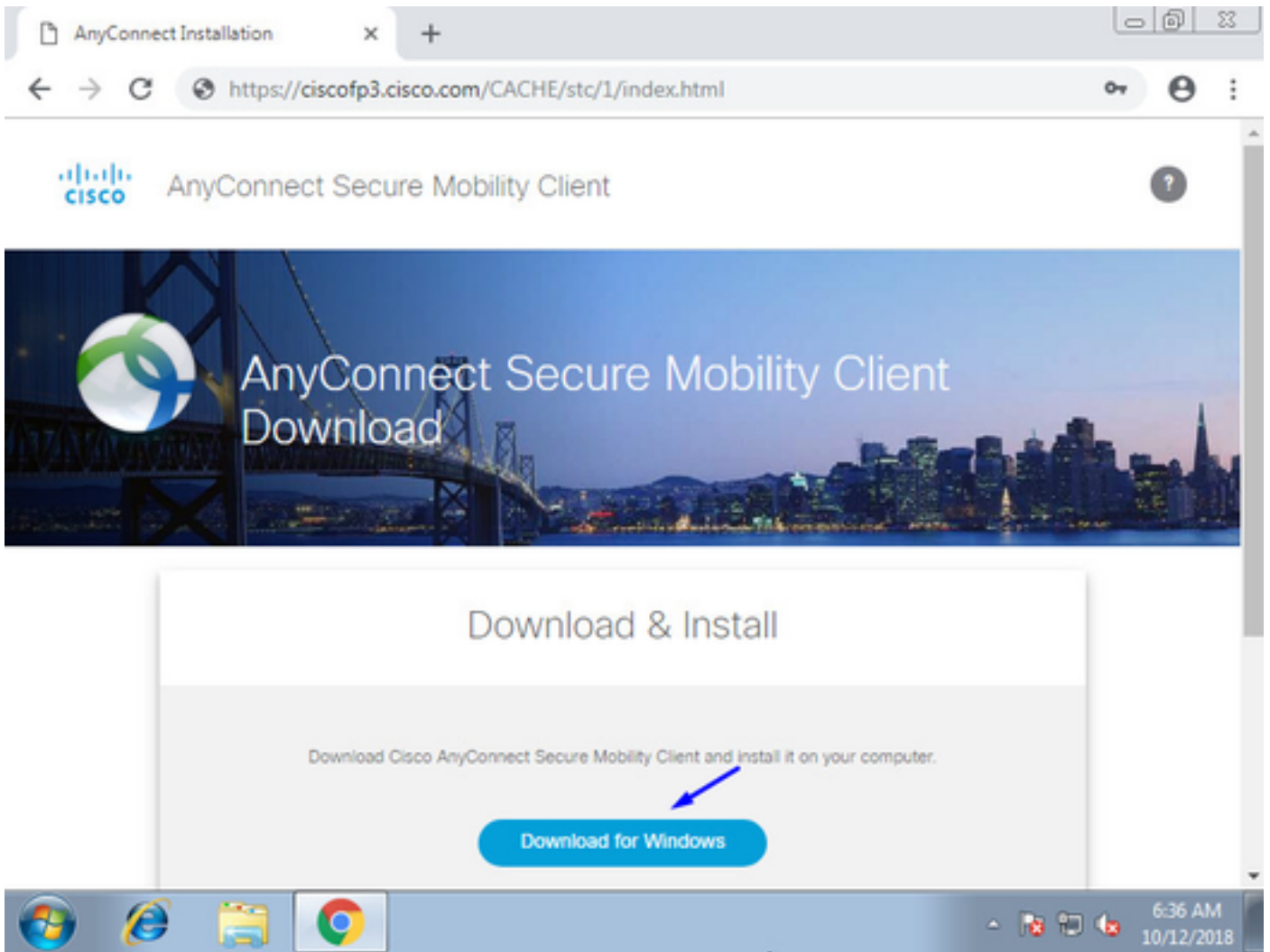
Group

Username

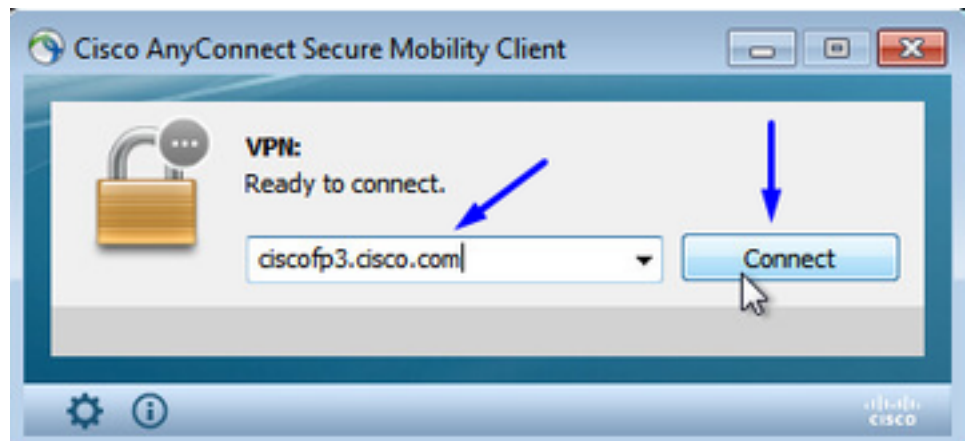
Password



انقر فوق تنزيل

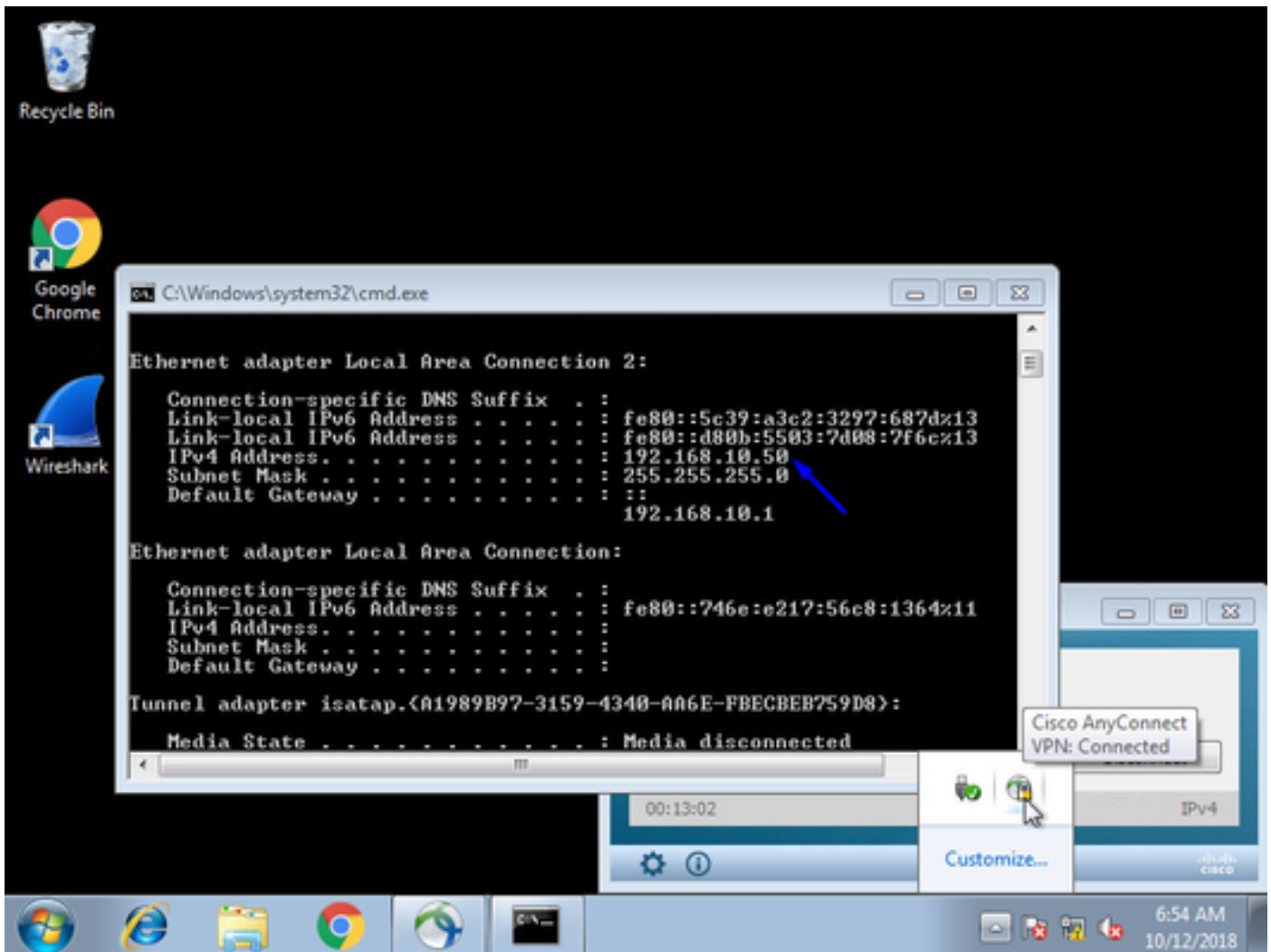


تثبيت AnyConnect VPN Secure Mobility Client وتشغيله على كمبيوتر Windows/Mac



اكتب اسم مستخدم وكلمة مرور Active Directory عند طلبها

سيتم منحك عنوان IP من تجمع عناوين IP الذي تم إنشاؤه أعلاه في الخطوة 5 وبوابة افتراضية من 1. في هذه الشبكة الفرعية



## التحقق من الصحة

نظام Firepower Threat Defense (FTD)

إظهار الأوامر

تحقق من على FTD أن المستخدم النهائي متصل بشبكة 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 : FTDAAnyConnectVPN  
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

بمجرد الانتقال إلى جهاز الكمبيوتر الذي يعمل بنظام التشغيل Windows 7 والنقر فوق "قطع الاتصال" على عميل Cisco AnyConnect، ستحصل على:

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

## التقاط

كيف يبدو التقاط العمل على الواجهة الخارجية عند الضغط على اتصال على عميل AnyConnect

مثال:

سيكون عنوان IP العام الخاص بالمستخدم النهائي هو عنوان IP العام الخاص بالموجه الخاص به في المنزل على سبيل المثال

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

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

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

عرض الحزم التي جاءت إلى الواجهة الخارجية ل FTD من كمبيوتر المستخدم النهائي للتأكد من وصولها إلى واجهة FTD الخارجية:

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

ack 2933935593 win 32768 . :198.51.100.2.55928 < 203.0.113.2.443 17:05:56.810398 :20  
F 2933935593:2933935593(0) ack :203.0.113.2.443 < 198.51.100.2.55928 17:05:56.810428 :21  
430677898 win 64240  
ack 2933935594 win 32768 . :198.51.100.2.55928 < 203.0.113.2.443 17:05:56.810489 :22  
FP 430677898:430677898(0) ack :198.51.100.2.55928 < 203.0.113.2.443 17:05:56.810627 :23  
2933935594 win 32768  
ack 430677899 win 64240 . :203.0.113.2.443 < 198.51.100.2.55928 17:05:56.811008 :24  
S 2614357960:2614357960(0) win :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.250566 :25  
<8192 <mss 1460,nop,wscale 8,nop,nop,sackOK  
S 3940915253:3940915253(0) ack :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.250963 :26  
<2614357961 win 32768 <mss 1460  
ack 3940915254 win 64240 . :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.251406 :27  
P 2614357961:2614358126(165) ack :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.252062 :28  
3940915254 win 64240  
ack 2614358126 win 32768 . :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.252138 :29  
P 3940915254:3940915431(177) ack :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.252458 :30  
2614358126 win 32768  
P 2614358126:2614358217(91) ack :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.253450 :31  
3940915431 win 64063  
ack 2614358217 win 32768 . :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.253679 :32  
P 2614358217:2614358526(309) ack :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.255235 :33  
3940915431 win 64063  
ack 2614358526 win 32768 . :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.255357 :34  
P 2614358526:2614359555(1029) :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.255388 :35  
ack 3940915431 win 64063  
ack 2614359555 win 32768 . :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.255495 :36  
P 3940915431:3940915740(309) ack :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.400110 :37  
2614359555 win 32768  
P 3940915740:3940917069(1329) :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.400186 :38  
ack 2614359555 win 32768  
ack 3940917069 win 64240 . :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.400675 :39  
P 3940917069:3940918529(1460) :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.400736 :40  
ack 2614359555 win 32768  
P 3940918529:3940919979(1450) :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.400751 :41  
ack 2614359555 win 32768  
ack 3940919979 win 64240 . :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.401544 :42  
P 3940919979:3940921439(1460) :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.401605 :43  
ack 2614359555 win 32768  
P 3940921439:3940922899(1460) :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.401666 :44  
ack 2614359555 win 32768  
P 3940922899:3940923306(407) ack :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.401727 :45  
2614359555 win 32768  
P 3940923306:3940923375(69) ack :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.401743 :46  
2614359555 win 32768  
ack 3940923375 win 64240 . :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.402185 :47  
P 2614359555:2614359624(69) ack :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.402475 :48  
3940923375 win 64240  
ack 2614359624 win 32768 . :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.402597 :49  
F 2614359624:2614359624(0) ack :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.402628 :50  
3940923375 win 64240  
ack 2614359625 win 32768 . :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.402673 :51  
FP 3940923375:3940923375(0) ack :198.51.100.2.56228 < 203.0.113.2.443 17:05:59.402765 :52  
2614359625 win 32768  
ack 3940923376 win 64240 . :203.0.113.2.443 < 198.51.100.2.56228 17:05:59.413384 :53  
S 1903869753:1903869753(0) win :203.0.113.2.443 < 198.51.100.2.56280 17:05:59.555665 :54  
<8192 <mss 1460,nop,wscale 8,nop,nop,sackOK  
S 2583094766:2583094766(0) ack :198.51.100.2.56280 < 203.0.113.2.443 17:05:59.556154 :55  
<1903869754 win 32768 <mss 1460  
ack 2583094767 win 64240 . :203.0.113.2.443 < 198.51.100.2.56280 17:05:59.556627 :56  
P 1903869754:1903869906(152) ack :203.0.113.2.443 < 198.51.100.2.56280 17:05:59.560502 :57  
2583094767 win 64240  
ack 1903869906 win 32768 . :198.51.100.2.56280 < 203.0.113.2.443 17:05:59.560578 :58  
P 2583094767:2583096227(1460) :198.51.100.2.56280 < 203.0.113.2.443 17:05:59.563996 :59  
ack 1903869906 win 32768

```

ack 2583096227 win 64240 . :203.0.113.2.443 < 198.51.100.2.56280      17:05:59.780034 :60
P 2583096227:2583097673(1446) :198.51.100.2.56280 < 203.0.113.2.443    17:05:59.780141 :61
ack 2583097673 win 62794 . :203.0.113.2.443 < 198.51.100.2.56280      17:05:59.998376 :62
P 1903869906:1903870032(126) ack :203.0.113.2.443 < 198.51.100.2.56280  17:06:14.809253 :63
ack 1903869906 win 32768      17:06:14.809970 :64
P 2583097673:2583097724(51) ack :198.51.100.2.56280 < 203.0.113.2.443    1903870032 win 32768
17:06:14.815768 :65
ack 1903870032:1903870968(936) ack :203.0.113.2.443 < 198.51.100.2.56280  2583097724 win 64240
17:06:14.815860 :66
ack 1903870968 win 32768 . :198.51.100.2.56280 < 203.0.113.2.443    17:06:14.816913 :67
P 2583097724:2583099184(1460) :198.51.100.2.56280 < 203.0.113.2.443    ack 1903870968 win 32768
17:06:14.816928 :68
ack 1903870968 win 32768      17:06:14.816959 :69
P 2583099184:2583099306(122) ack :198.51.100.2.56280 < 203.0.113.2.443    1903870968 win 32768
17:06:14.816974 :70
ack 1903870968 win 32768      17:06:14.816989 :71
P 2583099306:2583100766(1460) :198.51.100.2.56280 < 203.0.113.2.443    ack 1903870968 win 32768
17:06:14.817554 :72
ack 1903870968 win 32768      17:06:14.817615 :73
P 2583100766:2583100888(122) ack :198.51.100.2.56280 < 203.0.113.2.443    1903870968 win 32768
17:06:14.817630 :74
ack 1903870968 win 32768      17:06:14.817630 :75
P 2583100888:2583102142(1254) :198.51.100.2.56280 < 203.0.113.2.443    1903870968 win 32768
17:06:14.817645 :76
ack 2583102142 win 64240 . :203.0.113.2.443 < 198.51.100.2.56280      17:06:14.817645 :77
P 2583102142:2583103602(1460) :198.51.100.2.56280 < 203.0.113.2.443    1903870968 win 32768
17:06:14.817660 :78
ack 1903870968 win 32768      17:06:14.818088 :79
P 2583103602:2583103930(328) ack :198.51.100.2.56280 < 203.0.113.2.443    17:06:14.818530 :80
ack 1903870968 win 32768      17:06:18.215122 :81
P 2583103930:2583104052(122) ack :198.51.100.2.56280 < 203.0.113.2.443    17:06:18.215610 :82
ack 1903870968 win 32768      17:06:18.215671 :83
P 2583104052:2583105512(1460) :198.51.100.2.56280 < 203.0.113.2.443    ack 2583105738 win 64014
17:06:18.215763 :84
ack 2583105512 win 64240 . :203.0.113.2.443 < 198.51.100.2.56280      17:06:18.247011 :85
ack 2583105738 win 64014 . :203.0.113.2.443 < 198.51.100.2.56280      17:06:18.247728 :86
udp 99 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.249285 :87
udp 48 :198.51.100.2.58944 < 203.0.113.2.443      17:06:18.272309 :88
P 1903870968:1903872025(1057) :203.0.113.2.443 < 198.51.100.2.56280      17:06:18.277680 :89
ack 1903872025 win 32768 . :198.51.100.2.56280 < 203.0.113.2.443    17:06:18.334501 :90
udp 119 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.381541 :91
udp 188 :198.51.100.2.58944 < 203.0.113.2.443      17:06:18.443565 :92
udp 93 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.786702 :93
udp 93 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.786870 :94
udp 93 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.786931 :95
udp 221 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.952755 :96
udp 109 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.968272 :97
udp 109 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.973902 :98
udp 109 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.973994 :99
udp 109 :203.0.113.2.443 < 198.51.100.2.58944      17:06:18.989267 :100

```

عرض تفاصيل ما يحدث لتلك الحزمة الواردة من المستخدم النهائي داخل جدار الحماية

packets captured 2943

006b.f1e7.6c5e 000c.294f.ac84 0x0800 Length: 66 17:05:56.580994 :1  
S [tcp sum ok] 2933933902:2933933902(0) win 8192 <mss :203.0.113.2.443 < 198.51.100.2.55928  
(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

packet shown 1
ciscofp3#

```

انسخ الالتقاط إلى disk0: الخاص ب FTD. ويمكنك بعد ذلك تنزيله عبر SCP أو FTP أو TFTP

FirePOWER Management Center >> System >> Health Monitor >> Health Monitor >> Health Monitor >> Advanced Troubleshooting (أومن واجهة مستخدم الويب الخاصة ب >> Health Monitor >> Health Monitor >> Advanced Troubleshooting (أستكشف الأخطاء وإصلاحها المتقدمة) < انقر فوق علامة التبويب (تنزيل ملف) Download File)

```
ciscofp3# copy /pcap capture:capin disk0:/capin.pcap
<Source capture name [capin]? <hit Enter
<Destination filename [capin.pcap]? <hit Enter
!!!!!!!!!!!!!!!
packets copied in 0.0 secs 207
```

```
ciscofp3# dir
/:Directory of disk0
rwx 198 05:13:44 Apr 01 2018 lina_phase1.log- 122
drwx 4096 21:42:20 Jun 30 2018 log 49
drwx 4096 21:42:36 Jun 30 2018 coredumpinfo 53
drwx 4096 14:59:51 Oct 10 2018 csm 110
rwx 21074 01:26:44 Oct 10 2018 backup-config.cfg- 123
rwx 21074 01:26:44 Oct 10 2018 startup-config- 124
rwx 20354 01:26:44 Oct 10 2018 modified-config.cfg- 125
rwx 60124 17:06:22 Oct 10 2018 capin.pcap- 160
```

```
/: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
(bytes copied in 21.800 secs (5411 bytes/sec 113645
ciscofp3#
```

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

تحقق من تكوين قاعدة NAT بشكل صحيح:

```
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-po ol 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: ALLOW  
:Config
```

```
:Additional Information  
found next-hop 192.168.1.30 using egress ifc inside
```

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

ciscofp3#

## التقاط الكمبيوتر الشخصي الخاص بالموظفين الخاص بالكمبيوتر الشخصي بنجاح الاتصال ب FTD من خلال AnyConnect VPN

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

يمكنك أيضا رؤية نفق DTLS بشكل فيما بعد في هذا الالتقاط نفسه

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 (00:6b:f1:e7:6c:5e), Dst: Vmware_4f:ac:84 (00:0c:29:4f:ac:84)
> Internet Protocol Version 4, Src: , Dst:
> User Datagram Protocol, Src Port: 58944, Dst Port: 443
> Datagram Transport Layer Security
  > DTLS 1.0 (OpenSSL pre 0.9.8f) Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: DTLS 1.0 (OpenSSL pre 0.9.8f) (0x0100)
    Epoch: 0
    Sequence Number: 0
    Length: 86
    > Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
        Length: 74
        Message Sequence: 0
        Fragment Offset: 0
        Fragment Length: 74
  
```

التقاط المأخوذ على الواجهة الخارجية ل FTD الذي يظهر أن جهاز كمبيوتر AnyConnect يتصل بنجاح بشبكة VPN

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	12:05:56.580994		55928		443	TCP	66	55928 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	12:05:56.581375		443		55928	TCP	58	443 → 55928 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
3	12:05:56.581757		55928		443	TCP	54	55928 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	12:05:56.582382		55928		443	TLSv1.2	187	Client Hello
5	12:05:56.582458		443		55928	TCP	54	443 → 55928 [ACK] Seq=1 Ack=134 Win=32768 Len=0
6	12:05:56.582733		443		55928	TLSv1.2	1514	Server Hello
7	12:05:56.790211		55928		443	TCP	54	55928 → 443 [ACK] Seq=134 Ack=1461 Win=64240 Len=0
8	12:05:56.790349		443		55928	TLSv1.2	1159	Certificate, Server Hello Done
9	12:05:56.791691		55928		443	TLSv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	12:05:56.794911		443		55928	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
11	12:05:56.797077		55928		443	TLSv1.2	363	Application Data
12	12:05:56.797169		443		55928	TCP	54	443 → 55928 [ACK] Seq=2657 Ack=801 Win=32768 Len=0
13	12:05:56.797199		55928		443	TLSv1.2	875	Application Data
14	12:05:56.797276		443		55928	TCP	54	443 → 55928 [ACK] Seq=2657 Ack=1622 Win=32768 Len=0
15	12:05:56.798634		443		55928	TLSv1.2	363	Application Data
16	12:05:56.798786		443		55928	TLSv1.2	811	Application Data

```

> Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: Vmware_4f:ac:84 (00:0c:29:4f:ac:84), Dst: Cisco_e7:6c:5e (00:6b:f1:e7:6c:5e)
> Internet Protocol Version 4, Src: , Dst:
> Transmission Control Protocol, Src Port: 443, Dst Port: 55928, Seq: 1, Ack: 134, Len: 1460
  Source Port: 443
  Destination Port: 55928
  [Stream index: 0]
  [TCP Segment Len: 1460]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 1461 (relative sequence number)]
  Acknowledgment number: 134 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window size value: 32768
  [Calculated window size: 32768]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0x3693 [unverified]
  
```

```

00c0 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 51 31 15 ..*H....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....c...
0100 31 1d 30 1b 06 03 55 04 03 13 14 63 6f 68 61 64 1-0...U....
0110 6c 65 79 33 2d 43 4f 52 42 44 43 33 2d 43 41 30 6c 65 79 33 2d 43 4f 52 42 44 43 33 2d 43 41 30 ...18101 00245002
0120 1e 07 0d 31 38 31 30 31 30 30 32 34 35 30 30 5a ...201009 02450020
0130 17 0d 32 30 31 30 30 39 30 32 34 35 30 30 5a 30 ...1805...*H....
0140 61 b3 31 26 30 24 06 09 2a 86 48 86 f7 0d 01 09 ... f p3...
0150 02 13 7f 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 ...: 0...
0160 6c 65 79 33 2e 6c 6f 63 61 6c 31 0b 30 09 06 03 U...US1-0...U...
0170 55 04 06 13 02 55 53 31 0b 30 09 06 03 55 04 08 ...CA1-0...U...S
0180 13 02 43 41 31 11 30 0f 06 03 55 04 07 13 08 53 an Jose1-0...U...
0190 61 6e 20 4a 6f 73 65 31 0e 30 0c 06 03 55 04 0a ...Cisco1-0...U...
01a0 13 05 43 69 73 63 6f 31 0c 30 0a 06 03 55 04 0b ...TAC1 0...U...
01b0 13 03 54 41 43 31 20 30 1e 06 03 55 04 03 13 17 ...f p3...
01c0 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 6c 65 79 3,local1-0...*H...
01d0 33 2e 6c 6f 63 61 6c 31 1c 30 1a 06 09 2a 86 48 ..... tac@cis
01e0 86 f7 0d 01 09 01 16 0d 74 61 63 40 63 69 73 63 o.com0...0...*H...
01f0 6f 2e 63 6f 6d 30 82 01 22 30 0d 06 09 2a 86 48 .....0...
0200 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 .....0...
  
```

ملاحظة: يمكنك الاطلاع على شهادة خادم FTD VPN في الحزمة 'Server Hello' أثناء إتصالنا بالواجهة الخارجية ل

FTD من خلال VPN. سيق كميوتر الموظف بهذه الشهادة لأن كميوتر الموظف يحتوي على شهادة CA الجذر عليها، وتم توقيع شهادة خادم VPN ل FTD من قبل المرجع المصدق الجذر نفسه.

التقط على FTD من FTD يسأل نادل RADIUS إذا كان username + كلمة صحيح (Cisco ISE)

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

```

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

كما يمكنك أن ترى أعلاه، يحصل اتصال الشبكة الخاصة الظاهرية (VPN) الخاص بنا على قبول الوصول، كما يتصل عميل AnyConnect VPN بنجاح ب FTD عبر الشبكة الخاصة الظاهرية (VPN)

التقاط (CLI) من FTD يسأل Cisco ISE إذا كان اسم المستخدم + كلمة المرور صحيحين (أي تأكد من أن طلبات RADIUS تنتقل بنجاح بين FTD و ISE وتحقق من الواجهة التي سترکہا)

```

[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
udp 659 :192.168.1.10.1812 < 192.168.1.1.3238 01:23:52.264512 :37
udp 159 :192.168.1.1.3238 < 192.168.1.10.1812 01:23:52.310210 :38
udp 659 :192.168.1.10.1812 < 192.168.1.1.3238 01:23:52.311064 :39
udp 20 :192.168.1.1.3238 < 192.168.1.10.1812 01:23:52.326734 :40
udp 714 :192.168.1.10.1813 < 192.168.1.1.19500 01:23:52.737663 :82
udp 20 :192.168.1.1.19500 < 192.168.1.10.1813 01:23:52.744483 :85
  
```

أدناه يظهر خادم RADIUS Cisco ISE أن المصادقة ناجحة. انقر فوق العدسة المكبرة للاطلاع على تفاصيل المصادقة الناجحة

Time	Source	Destination	Protocol	Info
Oct 11, 2018 06:10:08.808 PM	jsmith	00:0C:29:37:EF:BF	Workstation	VPN Users >> Default
Oct 11, 2018 06:10:08.808 PM	jsmith	00:0C:29:37:EF:BF	FTDVPN	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

التقط على محول AnyConnect الخاص بالكمبيوتر الموظف الخاص بالموظف المتوجه إلى موقع ويب داخلي عبر HTTPS (على سبيل المثال، أثناء وجوده بنجاح في VPN d):

The image shows a Wireshark capture of network traffic on a local area connection. The filter is set to 'tcp.port == 443'. The capture shows a series of packets from source IP 192.168.10.50 to destination IP 192.168.10.50. The traffic includes a SYN packet (seq=0), a SYN-ACK packet (seq=0, ack=63576), and several TLSv1.2 packets for Client Hello, Key Exchange, Change Cipher Spec, and Application Data. The final packet is a TCP ACK (seq=4583, ack=13).

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=63576
51	1.547675	192.168.10.50	192.168.10.50	TCP	54	63576 → 443 [ACK] Seq=1 Ack=1 Win=0
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 Key Exchange
54	1.550909	192.168.10.50	192.168.10.50	TLSv1.2	372	Client Key Exchange, Change Cipher Spec
58	1.562066	192.168.10.50	192.168.10.50	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake
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=4583
67	1.667423	192.168.10.50	192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=4583 Ack=13

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

تصحيح الأخطاء

debug radius all

debug webVPN AnyConnect 255



قم بتشغيل الأمر "debug radius all" على CLI (واجهة سطر الأوامر (CLI) التشخيصية لدعم النظام (FTD) واضغط على "Connect" على جهاز كمبيوتر Windows/Mac على عميل 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
...fb 19 19 df f6 b1 c7 3e 34 fc 88 ce | .....>4 93 02 10 01
....2d 55 01 08 6a 73 6d 69 74 68 02 12 a0 83 | u8-U..jsmith 38 75
.....c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 05 06 | ...r...$.c
1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...198.51.100.2 00 50 00 00
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
....2e 32 31 34 2e 32 35 31 1a 23 00 00 09 | 51.100.2# 31 30
1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device 01
.,.2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win
6d 64 6d 2d 74 6c 76 3d 64 65 76 | ...&mdm-tlv=dev 26 01 09 00 00
2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29 65 63 69
.....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
6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c 62 75 70
...2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u 34 01 09 00
2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon 72 65 73
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
.f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6 66 74
2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P 31
6b 20 31 1a 40 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm 63 61
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
6c 20 50 6c 61 | ware Virtual Pla 61 75 74 72 69 56 20 65 72 61 77
6f 72 6d 1a 5b 00 00 09 01 55 6d 64 6d | tform.[.....Umdm 66 74
=2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid
3693C6407C925251 | 31 35 32 35 32 39 43 37 30 34 36 43 33 39 36 33
FF72B6493BDD8731 | 31 33 37 38 44 44 42 33 39 34 36 42 32 37 46 46
8ABFC90C621542C3 | 33 43 32 34 35 31 32 36 43 30 39 43 46 42 41 38
8FAF878EF49614A1 | 31 41 34 31 36 39 34 46 45 38 37 38 46 41 46 38
1a 31 00 00 09 01 2b 61 75 | .....1.....+au 00 00 00 06 04
2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0 74 69 64
ac9d68a000050005 | 35 30 30 30 35 30 30 30 30 61 38 36 64 39 63 61
1a 23 00 00 09 01 1d 69 | bbelf91.#.....i 31 39 66 31 65 62 62
3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1 70
```

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

```
.....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
2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2 30 31
Radius: Type = 31 (0x1F) Calling-Station-Id
(Radius: Length = 16 (0x10)
= (Radius: Value (String
2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2 30 31
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
2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2 30 31
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
3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e 63 61
2d 62 66 | f-bf 66
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
-6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c 62 75
2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf 39 32
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
6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect 65 67 61
6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030 69 57 20
49 | 39 34
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
2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service 36
6b 20 31 | Pack 1 63 61 50 20
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
.3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc 65 70 79
4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual 56 20
6c 61 74 66 6f 72 6d | Platform 50
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
3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925 64 69
251FF72B6493BDD8 | 38 44 44 42 33 39 34 36 42 32 37 46 46 31 35 32
7318ABFC90C62154 | 34 35 31 32 36 43 30 39 43 46 42 41 38 31 33 37
2C38FAF878EF4961 | 31 36 39 34 46 45 38 37 38 46 41 46 38 33 43 32
4A1 | 31 41 34
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
2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id 74 69 64 75 61
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
05bbelf91 | 31 39 66 31 65 62 62 35 30
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
.3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192 70 69
2e 32 31 34 2e 32 35 31 | 168.10.50 31 30 32
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
6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN 41 44 54 46
      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
6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true 63
      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
      'key 'cisco123
      sip 192.168.1.10
      type 1

```

(RADIUS packet decode (response

```

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

```

```

.....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
6f 6e 3a 30 61 | ReauthSession:0a 69 73 73 65 53 68 74 75 61 65 52

```

```
c9d68a000050005b | 62 35 30 30 30 35 30 30 30 30 61 38 36 64 39 63
                                belf91 | 31 39 66 31 65 62
                                Radius: Type = 25 (0x19) Class
                                (Radius: Length = 59 (0x3B)
                                = (Radius: Value (String
3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000 53 43 41 43
3a 63 6f | 050005bbelf91:co 31 39 66 31 65 62 62 35 30 30 30 35 30
6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408 69 62 72
                                2f 31 39 33 31 36 38 32 | 4/1931682 34
                                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
6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f 72 | profile-name=Wor 72 70
                                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
                                ..... | c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 93 02 11 01
                                c1 e4 88 01 08 6a 73 6d 69 74 68 02 12 79 41 | .....jsmith..yA 83
                                ...0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 05 06 | .q.8..I.<...e
                                1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...203.0.113 00 50 00 00
                                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
                                ...#. <2e 32 31 34 2e 32 35 31 1a 23 00 00 09 | ess 31 30
                                1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device 01
                                ..2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win
                                6d 64 6d 2d 74 6c 76 3d 64 65 76 | ...&mdm-tlv=dev 26 01 09 00 00
                                2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29 65 63 69
                                .....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
                                6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c 62 75 70
                                ..:2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf
                                6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u 34 01 09 00
                                2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon 72 65 73
                                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
                                .6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6 66 74
                                2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P 31
                                6b 20 31 1a 40 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm 63 61
                                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
                                6c 20 50 6c 61 | ware Virtual Pla 61 75 74 72 69 56 20 65 72 61 77
                                6f 72 6d 1a 5b 00 00 09 01 55 6d 64 6d | tform.[.....Umdm 66 74
```

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

```
.....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)
.0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 | yA.q.8..I.<...e 41 79
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)
2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2 30 31
Radius: Type = 31 (0x1F) Calling-Station-Id
(Radius: Length = 16 (0x10)
= (Radius: Value (String)
2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2 30 31
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)
2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2 30 31
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
3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e 63 61
2d 62 66 | f-bf 66
```

```
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
-6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c 62 75
2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf 39 32
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
6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect 65 67 61
6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030 69 57 20
49 | 39 34
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
2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service 36
6b 20 31 | Pack 1 63 61 50 20
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
.3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc 65 70 79
4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual 56 20
6c 61 74 66 6f 72 6d | Platform 50
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
3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925 64 69
251FF72B6493BDD8 | 38 44 44 42 33 39 34 36 42 32 37 46 46 31 35 32
7318ABFC90C62154 | 34 35 31 32 36 43 30 39 43 46 42 41 38 31 33 37
2C38FAF878EF4961 | 31 36 39 34 46 45 38 37 38 46 41 46 38 33 43 32
4A1 | 31 41 34
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
2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id 74 69 64 75 61
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
05bbelf91 | 31 39 66 31 65 62 62 35 30
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
.3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192 70 69
2e 32 31 34 2e 32 35 31 | 168.10.50 31 30 32
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
6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAAnyConnectVPN 41 44 54 46
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
4f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true 63
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
;...}...{c3 44 44 7d a6 07 0d 7b 92 f2 3b | .....DD 15 14 00 11 03
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  
..ca be a0 6e 46 71 af 5c 65 82 77 c7 b5 | .....nFq.\e.w 02 12 04  
....d7 01 08 6a 73 6d 69 74 68 05 06 00 00 | Pxa...jsmith 61 78 50  
.....P | 06 08 01 00 00 00 06 07 02 00 00 06 06 00 50  
c0 a8 0a 32 19 3b 43 41 43 53 3a 30 61 63 39 64 | ...2.;CACS:0ac9d  
68a000050005bbe1 | 31 65 62 62 35 30 30 30 35 30 30 30 61 38 36  
3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32 31 39 66  
.2f 31 39 33 31 36 38 32 1e | 2344084/1931682 34 38 30 34 34 33 32  
.2e 32 30 31 2e 32 31 34 2e 31 35 31 1f | .203.0.113.2 30 31 10  
)2e 32 30 31 2e 32 31 34 2e 32 35 31 28 | .198.51.100.2 30 31 10  
2c 0a 43 31 46 | .....).C1F 00 00 00 00 06 29 01 00 00 00 06  
....=.....2d 06 00 00 00 01 3d 06 00 00 00 | 00005- 35 30 30 30 30  
2e 32 30 31 2e 32 31 34 2e 32 35 | .B.203.0.113.2 30 31 10 42 05  
1a 18 00 00 0c 04 92 12 46 54 44 41 6e 79 43 | .....FTDAnyC 31  
.....6f 6e 6e 65 63 74 56 50 4e 1a 0c 00 00 0c 04 96 | onnectVPN  
..... | 1a 0c 00 00 0c 04 97 06 00 00 00 02 00 00 00 06  
.#..... | 1a 0c 00 00 0c 04 98 06 00 00 00 03 1a 23 00 01  
1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | .....mdm-tlv=dev 01 09 00 00  
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e | ice-platform=win 65 63 69  
=1a 2c 00 00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d | ,.....&mdm-tlv  
2d 6d 61 63 3d 30 30 2d 30 63 | device-mac=00-0c 65 63 69 76 65 64  
..2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 31 00 00 | -29-37-ef-bf.1  
2b 61 75 64 69 74 2d 73 65 73 73 69 6f | ...+audit-sessio 01 09 00  
6e 2d 69 64 3d 30 61 63 39 64 36 38 61 30 30 30 | n-id=0ac9d68a000  
.1a 33 00 | 050005bbe1f91.3 31 39 66 31 65 62 62 35 30 30 30 35 30  
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....-mdm-tlv=dev 01 09 00 00  
2d 70 75 62 6c 69 63 2d 6d 61 63 3d 30 | ice-public-mac=0 65 63 69  
2d 30 63 2d 32 39 2d 33 37 2d 65 66 2d 62 66 | 0-0c-29-37-ef-bf 30  
=1a 3a 00 00 00 09 01 34 6d 64 6d 2d 74 6c 76 3d | :.....4mdm-tlv  
2d 75 73 65 72 2d 61 67 65 6e 74 3d 41 6e | ac-user-agent=An 63 61  
6f 6e 6e 65 63 74 20 57 69 6e 64 6f 77 73 | yConnect Windows 43 79  
....?.2e 36 2e 30 33 30 34 39 1a 3f 00 00 00 09 | 4.6.03049 34 20  
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | .9mdm-tlv=device 39 01  
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  
.....@.6b 20 31 1a 40 00 00 00 09 01 | ce Pack 1 63 61 50 20 65 63  
-3a 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | :mdm-tlv=device  
3d 56 4d 77 61 72 65 2c 20 49 6e 63 | type=VMware, Inc 65 70 79 74  
2e 20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c | . VMware Virtual  
.....].6c 61 74 66 6f 72 6d 1a 5b 00 00 00 09 01 | Platform 50 20  
-6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | Umdm-tlv=device 55  
3d 33 36 39 33 43 36 34 30 37 43 39 32 | uid=3693C6407C92 64 69 75  
5251FF72B6493BDD | 44 44 42 33 39 34 36 42 32 37 46 46 31 35 32 35  
87318ABFC90C6215 | 35 31 32 36 43 30 39 43 46 42 41 38 31 33 37 38  
42C38FAF878EF496 | 36 39 34 46 45 38 37 38 46 41 46 38 33 43 32 34  
.....14A1 | 00 00 00 00 06 04 31 41 34 31

.....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)
3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000 53 43 41 43
3a 63 6f | 050005bbe1f91:co 31 39 66 31 65 62 62 35 30 30 30 35 30
6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408 69 62 72
2f 31 39 33 31 36 38 32 | 4/1931682 34
Radius: Type = 30 (0x1E) Called-Station-Id
(Radius: Length = 16 (0x10)
= (Radius: Value (String)
2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2 30 31
Radius: Type = 31 (0x1F) Calling-Station-Id
(Radius: Length = 16 (0x10)
= (Radius: Value (String)
2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2 30 31
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)
C1F00005 | 35 30 30 30 30 46 31 43
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)
2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2 30 31
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)
6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAAnyConnectVPN 41 44 54 46
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
3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e 63 61
    2d 62 66 | f-bf 66
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
2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id 74 69 64 75 61
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
    05bbelf91 | 31 39 66 31 65 62 62 35 30
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
-6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c 62 75
    2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf 39 32
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
6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect 65 67 61
    6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030 69 57 20
    49 | 39 34
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
2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service 36
    6b 20 31 | Pack 1 63 61 50 20

```

```

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
.3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc 65 70 79
 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual 56 20
      6c 61 74 66 6f 72 6d | Platform 50
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
3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925 64 69
251FF72B6493BDD8 | 38 44 44 42 33 39 34 36 42 32 37 46 46 31 35 32
7318ABFC90C62154 | 34 35 31 32 36 43 30 39 43 46 42 41 38 31 33 37
2C38FAF878EF4961 | 31 36 39 34 46 45 38 37 38 46 41 46 38 33 43 32
      4A1 | 31 41 34
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
.e5 fd b1 6d fb ee 58 f0 89 79 73 8e | .....m..X..ys 14 00 12 05
      ... | dc a7 20 90

```

```

.....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#

```

قم بتشغيل الأمر 'debug webVPN AnyConnect 255' على CLI (واجهة سطر الأوامر (CLI) التشخيصية لدعم

# النظام (FTD) (واجهة سطر الأوامر (CLI)) واضغط على 'Connect' على جهاز كمبيوتر Windows/Mac على عميل 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-
'input: 'X-DTLS-Accept-Encoding: lzs...
'Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs
'input: 'X-DTLS-Header-Pad-Length: 0...
'input: 'X-CSTP-Accept-Encoding: lzs,deflate...
'Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate
'.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) & 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(dtlshdr) - 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**

[انقر تفاصيل كل مصادقة < Cisco ISE > Operations > RADIUS > Live Log](#)

دقت على cisco ISE ك VPN login و ال ACL نتيجة 'PermitAccess' قدمت  
تظهر السجلات المباشرة jsmith التي تمت مصادقتها إلى FTD عبر VPN بنجاح

### Overview

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

### Authentication Details

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

### Steps

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

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

**Other Attributes**

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

CPMSessionID	00000000000070005bbc08c3
ISEPolicySetName	VPN Users
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
DTLSSupport	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

عمل AnyConnect VPN

حزمة DART

[كيفية تحميل حزمة AnyConnect J DART](#)

## استكشاف الأخطاء وإصلاحها

DNS

تحقق من أنه يمكن لأجهزة الكمبيوتر الشخصي Cisco ISE و FTD و Windows Server 2012 و Windows/Mac حل كل المشكلات للأمام والعكس (تحقق من DNS على جميع الأجهزة)

كمبيوتر Windows قم بتشغيل موجه أوامر، وتأكد من إمكانية تنفيذ 'nslookup' على اسم المضيف الخاص ب FTD

واجهة سطر الأوامر في FTD

show network<

```
nslookup 192.168.1.10 <
Server: 192.168.1.10
Address: 192.168.1.10#53
in-addr.arpa name = ciscoise.cisco.com.10.1.168.192
وجهة سطر الأوامر ISE:
```

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

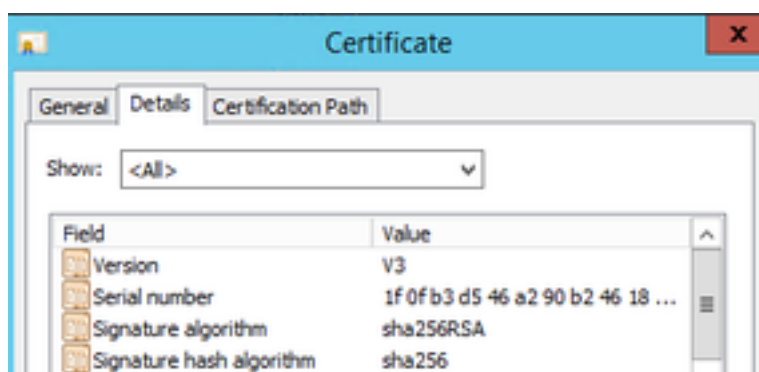
:QUESTION SECTION ;;
in-addr.arpa. IN PTR.20.1.168.192;

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

نظام التشغيل Windows Server 2012  
قم بتشغيل موجه أوامر، وتأكد من إمكانية تنفيذ 'nslookup' على hostname/FQDN الخاص ب FTD

### قوة الشهادة (لتوافق المستعرض)

تحقق من توقيع Windows Server 2012 على شهادات SHA256 أو أعلى. انقر شهادة المرجع المصدق الجذر نقرا مزدوجا في Windows وتحقق من حقول 'خوارزمية التوقيع'



إذا كانت SHA1، فستظهر معظم المستعرضات تحذير المستعرض لهذه الشهادات. لتغييره، يمكنك التحقق من هنا:

[كيفية ترقية مرجع مصادقة خادم Windows إلى SHA256](#)

تحقق من أن شهادة خادم FTD VPN تحتوي على الحقول التالية الصحيحة (عند التوصيل في المستعرض ب FTD)

الاسم الشائع = <ftdfqdn>

الاسم البديل للموضوع (SAN) = <FTDFQDN>

مثال:

الاسم الشائع: ciscofp3.cisco.com

اسم الموضوع البديل (SAN): اسم DNS=ciscofp3.cisco.com

## الاتصال وتكوين جدار الحماية

تحقق من استخدام التقاط على واجهة سطر الأوامر (CLI) ل FTD والتقاط على كمبيوتر الموظف باستخدام Wireshark للتحقق من وصول الحزم عبر 443 TCP+UDP إلى IP الخارجي من FTD. تحقق من أن هذه الحزم يتم الحصول عليها من عنوان IP العام الخاص بالموجه الرئيسي للموظف

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

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

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

```
ciscofp3# show cap capin
```

```
packets captured 2375
```

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

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

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

```
...
```

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل