

FTD: ىلج AnyConnect VPN ليمع نيوكت NAT و HAIRpin ءانثتسا

تايوتحمل

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتل](#)

[SSL ةءاهش ءاريتسا 1. ةوطخل](#)

[RADIUS مءاخ نيوكت 2. ةوطخل](#)

[IP عمجت ءاشنا 3. ةوطخل](#)

[XML فيرعت فلم ءاشنا 4. ةوطخل](#)

[AnyConnect XML فيرعت فلم ليءمجت 5. ةوطخل](#)

[AnyConnect روص ليءمجت 6. ةوطخل](#)

[Remote Access VPN ءلعم 7. ةوطخل](#)

[NAT و HairPin ءافء](#)

[NAT ءانثتسا نيوكت 1. ةوطخل](#)

[رءشل سوبء نيوكت 2. ةوطخل](#)

[ءحصلا نم ققءتلا](#)

[ءءالص او ءاطءأل ءاشكتسا](#)

ةمدقملا

ىلج Cisco (AnyConnect) ىلج ءعب نع لوصولل VPN لء نيوكت ةي فيءك ءنتسملا اءه فصى FMC ةطساوب ءتراءا مءت يءلا، 6.3 راءصل، (FTD) FirePOWER Threat Defense.

ةيساسأل تابلطتملا

تابلطتملا

ةيلاءل ءيضاوملاب ةفرعم ءيءل نوكت نأ Cisco يءصوت:

- ءءام ةقبط فرعمو ءعب نع لوصولل ةيساسأل (VPN) ةي رءاظلا ءصااءل ءكءشل (IKEv2) 2 راءصل ءنءرنءل ءءاءم لءاءتو (SSL) ءنمأل لءي ءصوتل
- RADIUS ةفرعمو ةيساسأل (AAA) ءبءءملا ءي ءو ءءل او ءءاءملا
- ةيساسأل FMC ةفرعم
- FTD لوكو ءورءب ةيساسأل ةفرعم

ةمدختسملا تانوكملا

ةيلاللا ةيداملا تانوكملا او جماربلا تارادصلا لىل دن تسملا اذه يف ةدراولا تامولعمل دن تست

- Cisco FMC، رادصلا 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

ىلع Cisco (AnyConnect) لىل دعب نع لوصولل VPN لىل نيوكت ءارجل دن تسملا اذه فصى FirePOWER (FMC) ةرادا زكرم ةطساوب رادملا، 6.3 رادصلا، FirePOWER (FTD) ديدته نع عافدلا

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دن تسملا اذه يف ةدراولا تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكت دن تسملا اذه يف ةمدختسملا ةزهجال عيمج تادب رمأ يال لم تحملا ريثاتلل كمهف نم دكاتف، ليغشتلا ديقتك بيش

ةيساسا تامولعمل

نيوكت لاثم نع ثحبت تنك اذا. FTD ةزهجال لىل نيوكتلا ةيطغت لىل دن تسملا اذه فدهى ASA، دن تسملا لىل ءوجرلا لىل جري، <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

دويقلا:

ةادا: ASA لىل رفوتى دعب نأ ريغ، FTD لىل دن ساي ال قمس اذه، ايلاح

- (FTD نم 6.5 رادصلا لىل رفوتىم) ءودزم AAA ءقداصم
- يكيما نيديلا لوصولل قسايس
- فبضملا صحف
- ISE Posture
- RADIUS COa
- VPN لىل نزاوم
- Cisco (CSCv92680) نم ءاطخال لىل حصت فرع 6.3 رادصلا، FirePOWER Device Manager لىل رفوتىم) ءيلحملا ءقداصملا
- Cisco (CSCvd64585) نم ءاطخال لىل حصت فرع، FlexConfig ربع ءرفوتىم) LDAP قمس ءطيرخ
- AnyConnect صي صخت
- ءي صلل AnyConnect جمارب
- AnyConnect بىرخت
- قىببنت لىل VPN ءكفبش
- SCEP لىل و
- WSA لىل مكف
- Cisco (CSCvq90789) نم ءاطخال لىل فرع) SAML SSO
- RA و L2L VPN ءنما زتملا ءيكيما نيديلا ريفشتلا ءطيرخ
- DART، (كذل لىل امو بيول نامأو Umbrella و SBL و AMP Enabler و Hostscan و NAM) AnyConnect تادحو رادصلا اذه لىل عيضا رتفا
- (KCD و RSA SDI) ءقداصم) TACACS، Kerberos
- ضرعتسملا لىل و

نيوكتلا

ةيلاللا تاوطخال لىل امك لىل جى، FMC يف Remote Access VPN ءلام لىل نم لاقنتلال

SSL ءداهش داريتسا 1. ءوطخال

ل طقف RSA لىل دن تسملا تاداهشلا معد مئى. AnyConnect نيوكت دن عىرورض تاداهشلا SSL و IPsec.

كذلك، IPsec، في عدم (ECDSA) يواضحي بالإنترنت لم يقرها عي قوتها في مزراخ تاداهش إلى دنست عدهاش مادتسإ دن XML في صوت وأ ديديج AnyConnect مزن رشن نكمي ال ECDSA.

فلم عم AnyConnect مزجل قبسمها رشنها كيلي بجي نكلو، IPsec، ل مادتسإ نكمي فرعم) ليمع لك يلع ايودي XML في رعت فلم تاتيديج عي مچ عفد بجي و XML في رعت (CSCtx42595) Cisco نم اطاخال جي حصت.

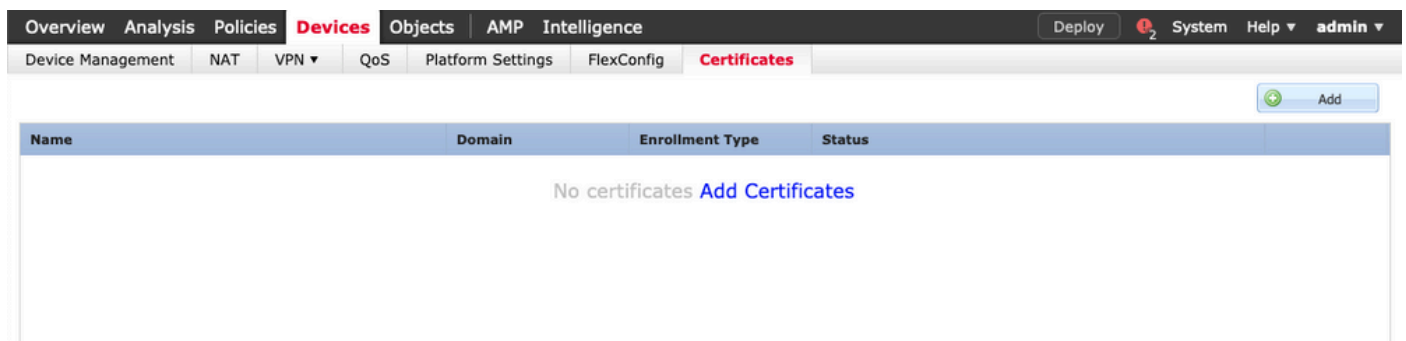
أو DNS مساب (CN) كرتشم مسا قحلم يلع عدهاشها يوتحت نا بجي، كذلك إلى عفاضها ب بيولا تاضرعتسم في "اهب قوتوم ريغ مداخ عدهاش" اطاخال بنجت ل IP ناووع.

عي قوت بلط عاشنا لبق (CA) قدصمها عجرمها عدهاش دوجو مزلي، FTD عزهجأ في: عطاالم (CSR) عدهاشها.

- عقي رط نم دصقي في (OpenSSL أو Windows Server لثم) يجراخ مداخ في CSR عاشنا مت اذا ايودي جي تافمها ليجست معددي ال FTD نأل ارظن، لشفها ايوديها ليجستها
- لثم PKCS12 فلتم بولسا مادتسإ بجي.

CSR، عاشنا مزلي، ايوديها ليجستها عقي رط مادتسإ فTD زاهج عدهاش يلع لوصحلل. عوهها عدهاش داري تسي م CA مادتسإ ه عي قوتو.

1. عروصلها في حضورم وه امك عفاضها دجو تاداهشها > عزهجالا إلى لقتنا.



2. عروصلها في حضورم وه امك ديديج عدهاش ليجست نئاك فضا أو زاهجالا دج.

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

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates** Add

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

Add New Certificate

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

Device*: FTD-Virtual

Cert Enrollment*: Select a certificate enrollment object

Add Cancel

Add Cert Enrollment

Name* Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL: * http://

Challenge Password:

Confirm Password:

Retry Period: 1 Minutes (Range 1-60)

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7cb bdcddd92

Allow Overrides

Save Cancel

3. (CSR عېقوت اهنم دصقې ېتلا ءداهشلا) CA ءداهش قصلو ېوډيالا لېجستلا عون ددح.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3tTUhYpfbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogklzou6
RqV66G9IE7Z2
xIVrSrJFqhrT795kMb8am8xhb4eXYXxUgJmODIPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/lJG2LgRDraOKt+jwbS7DGSK4mfZsZqhFdQP
LhBNFbyBvb9
dOjUkmdSvzQDRSqSo+HINEm3E8/q20wrtZp04MpAabyhr+hEpeP
VMrhvBOT8h
H8eMjSQjGhhHbuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDr
mwNgy5mTP9cHa
9Or3RlWRzEa11HE3mHC4Rj6DOnmgulfjx+TZRYczownSKILL7LcW1
DIBZclYmfaldC
W2cZuBR0yVDxQvq4#04ISEIBfOWFSd5rAD/bvk2n6xrJI1SLqABMJJ
uslu9KTGH1
bVKEYACKVvETw==
-----END CERTIFICATE-----
```

Allow Overrides

4. مقو FQDN ني مضا ل قحل "ص صخ م ال FQDN" دحو ة داهش ال تامل عم بيوبت ال ة مال ع دح . ة روص ال ي ة حصوص ال ة داهش ال لي صافات ة ئبعت ب

Add Cert Enrollment

Name* Anyconnect-certificate

Description

CA Information Certificate Parameters Key Revocation

Include FQDN: Use Device Hostname as FQDN

Include Device's IP Address:

Common Name (CN): vpn.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): MX

State (ST): Mexico

Country Code (C): MX

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

5. إلى عقب سنن لآب .محلل او مسال رايتخا كنكمي ،حاتفملا عون ددو ،حاتفم بيوبتلا ةمالع ددح . RSA ،يندا ابلطتم تياب 2048 دع ي .

6. ددح ،وتلل هؤاشنإ مت يذل TrustPoint ةقثلا ليحست نمض ددح م ث ،زاهل نم دكأت ،ظفح ددح . ةداهشلا رشنل ةفاضإ .

Add New Certificate



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

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: Anyconnect-certificate

Enrollment Type: Manual

SCEP URL: NA

Add

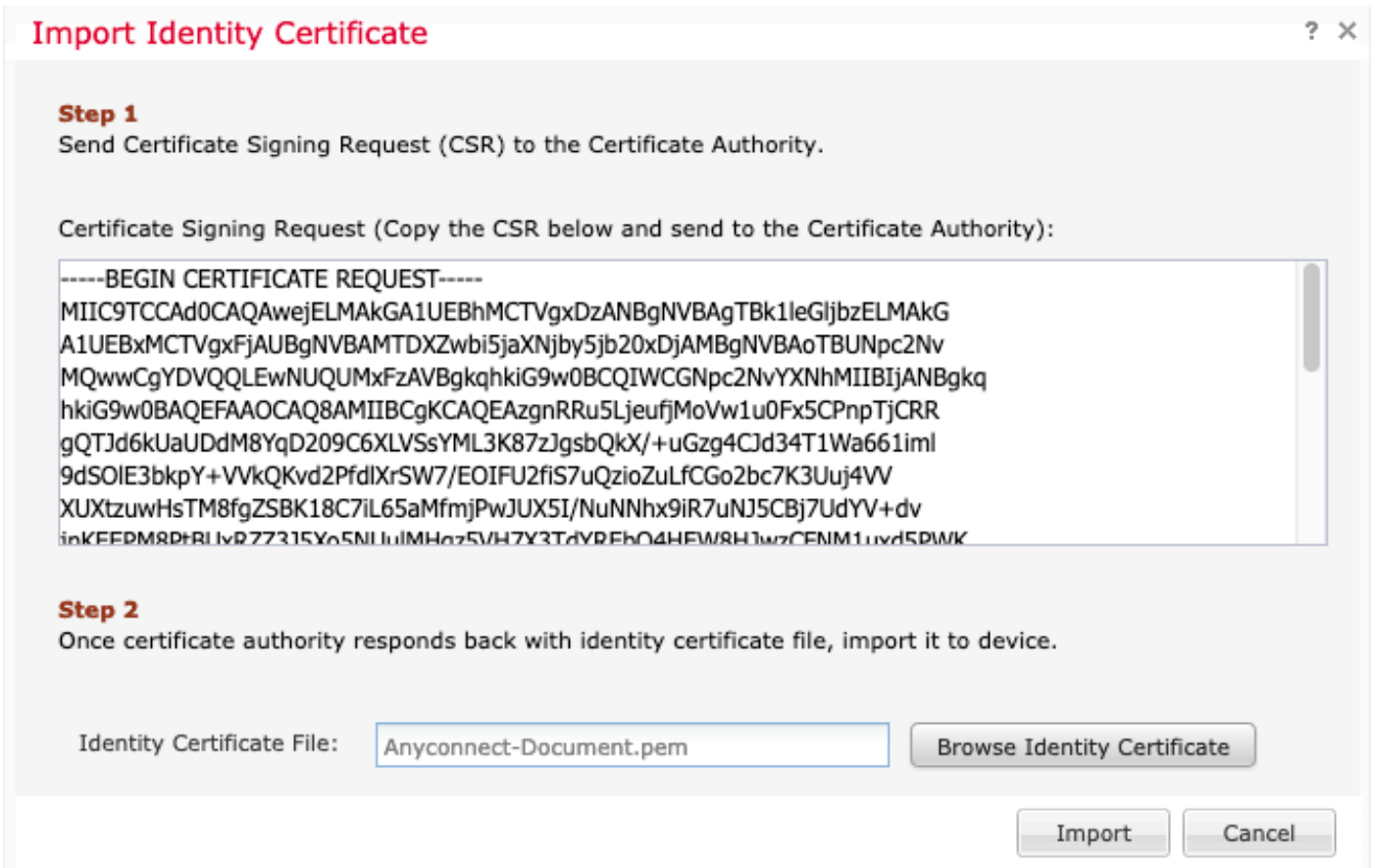
Cancel

7. ةروصلال ي ف حضورم وه امك CSR ءاشنال م عن ددحو فرعمل ةنوقيأ دح، ةلحال دومع ي ف.

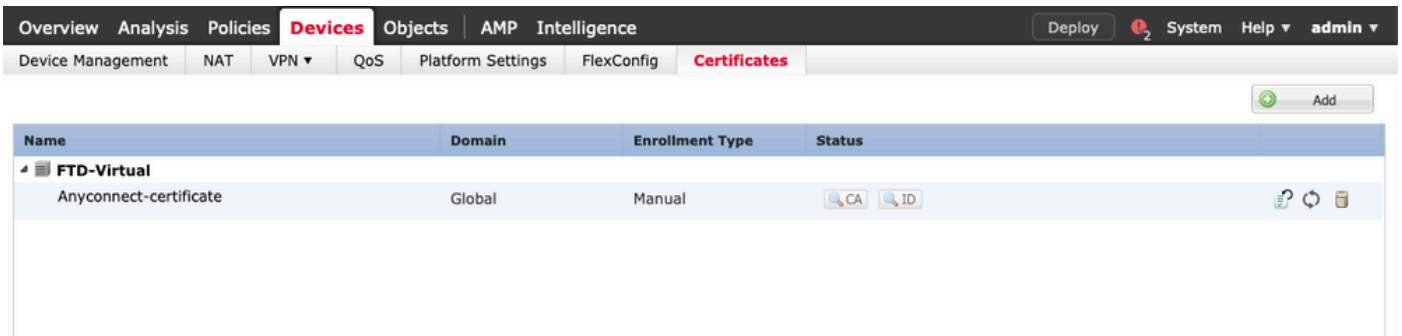
The screenshot shows the Cisco FTD GUI with the 'Certificates' tab selected. A warning dialog box is open, asking for confirmation to generate a Certificate Signing Request (CSR). The dialog text reads: "Warning: This operation will generate Certificate Signing Request do you want to continue?" with "Yes" and "No" buttons.

8. (DigiCert أو GoDaddy لاثم ال ل ي بس ى ل ع) ك ي دل ل ض ف م ال CA عم ه ع ي ق و ت و CSR خ س نا .

9. (base64 ق ي س ن ت ب نو ك ي ن أ ب ج ي ي ذ ل و) ق د ص م ال ع ج ر م ال ن م ة ي و ه ال ة د ا ه ش م ال ت س ا د ر ج م ب . دار ي ت س ا د ح . ي ل ح م ال ر ت و ي م ك ال ي ف ة د ا ه ش ال ن ا ك م د د ح و ة ي و ه ال ة د ا ه ش ض ا ر ع ت س ا د ح .



10. ءاوس دح ىلع ةي وهلا فرعمو ق دصم عجرم ةداهش لى صافات رفوتتس ،داريتسال درجم ب .
ضرعلل .



RADIUS مداخل نيوك ت . 2 ةوطخلال

بجي ،ةم و عدم ريغ ةي ل حملال مدختس ملال تانايب ةدعاق ، FMC ةطساوب ةرادم لال FTD ةزهجأ يف
LDAP و RADIUS لثم ، ىرخأ ةق داصم ةقيرط مادختس ل .

1. RADIUS مداخل ةومجم ةفاضل > RADIUS مداخل ةومجم > نئاللا ةرادل > تانئاللا لىل لقتنا .
ةروصلال يف حضوم وه امك .

Add RADIUS Server Group



Name:*

Radius-server

Description:

Group Accounting Mode:

Single

Retry Interval:*

10 (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update

Interval:*

24 (1-120) hours

Enable dynamic authorization

Port:*

1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

No records to display

Save

Cancel

كترشم رس عم RADIUS مداخل IP ناوع فضاو RADIUS مداوخة وجمم لاسا نييعت ب مق 2. جذومنلا اذه لامتك درجم ب ظفح ددحو، (RADIUS مداخ عم FTD نارقإل بولطم كترشم لاسلا) ةروصلال يف حضوم وه امك.

Add RADIUS Server Group

Name:* Radius-server

Description:

Group Accounting Mode: Single

Retrieval Interval: (1-10) Seconds

New RADIUS Server

IP Address/Hostname:* 192.168.10.34
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* 1812 (1-65535)

Key:*

Confirm Key:*

Accounting Port: 1813 (1-65535)

Timeout: 10 (1-300) Seconds

Connect using: Routing Specific Interface ⓘ

Default: Diagnostic Interface

Redirect ACL:

Save Cancel

Save Cancel

3. ةوصول ال ي ف حضورم وه امك RADIUS م داخ ةمئاق ي ف RADIUS م داخ تامولعم نآلا رفوت ت.

Add RADIUS Server Group



Name:* Radius-server

Description:

Group Accounting Mode: Single

Retry Interval:* 10 (1-10) Seconds

Realms:

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		
192.168.10.34		

Save Cancel

IP عمجت عاشن. 3. ةوطخال

1. IPv4 عمجت ةفاض | > نيوانعلا عمجت > تانئاللا ةراد | > تانئاللا لىل لقتنا.

2. امك هديجت نكمي نكلو ابولطم عانقلا لقق نوكي ال، IP نيوانع قاطنوم سا نييعت ب مق. ةروصلال ي ف حضوم وه.

Add IPv4 Pool



Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

ⓘ Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

XML فيرعت فلم ءاشنإ 4. ةوطخلال

1. ليغشتب مقو Cisco.com بيولا عقوم نم فيرعتال تافل مرحم ةادأ ليزنتب مق. قيبتال.

2. في حضورم وه امك ةفاضإ ددحو مداوخلال ةمئاق ىلإ لقتنا، فيرعتال فلم مرحم قيبتب في ةروصلال.

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins

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

3. وه امك قفاوم ددحو IP ناووع وأ (FQDN) لمالكلاب لهؤم لاجم مسا وأ ضرع مسا نييعتب مق. ةروصلال في حضورم.

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) Corporate - FTD (SSL)

FQDN or IP Address vpn.cisco.com / User Group ssl

Group URL

Connection Information

Primary Protocol SSL

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address Add

Move Up

Move Down

Delete

OK Cancel

4. مداوخل اعمىاق يف نآلا لاخذإلا رهظي :

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List
Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobile Settings	Certificate Pins
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --			

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

Add... Delete

Edit... Details

5. م س اب ظ ف ح > ف ل م إ ل ل ق ت ن ا .

.xml ق ح ل م م ا د خ ت س ا ب ة ل و ه س ب ه ي ل ع ف ر ع ت ل ل ن ك م ي م س ا ب ف ي ر ع ت ل ل ف ل م ظ ف ح ا : ة ظ ح ا ل م

AnyConnect XML ف ي ر ع ت ف ل م ل ي م ح ت . 5 ة و ط خ ل ل ا

1. فلم ةفاضل > AnyConnect فلم > VPN > نائل ةرادل > تائل لىل لقتنا، FMC ي ف AnyConnect.

2. كمالن ي ف لىمعلل فىرعت فلم ددو، ضارعتس قوف روناو نائل لل مسا نىىعت ب مق. ظفح ددو لىل حملل.

فلمل اعونك AnyConnect لىمعل فىرعت فلم دىحت نم دكأت: رىحت

Add AnyConnect File

Name:*




File Name:*

File Type:*

Description:

AnyConnect روص لىمحت 6. ةوطخلل

1. Cisco تالزنتب ةصائل بىولل ةحفص نم (.pkg) بىولل ربع رشنل روص لىزنت.

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

2. AnyConnect فلم ةفاضل > AnyConnect فلم > VPN > نائل لىل ةرادل > تائل لىل لقتنا.

3. دىحت درجم ب، لىل حملل كمالن نم pkg. فلم ددو AnyConnect ةمزح فلمل مسا نىىعت ب مق. فلمل.

4. ظفح ددو.

Add AnyConnect File

Name:*

File Name:*

File Type:*

Description:

Mac و Windows لى غش التال ماظن) كتاب لى لى اذانتسا ةيفاضا مزح لى محت نكمي :ةظحالما و Linux).

Remote Access VPN جالعام 7. ةوطخلال

لكلذل اقفو "دعب نع لوصول جالعام" عابتا نكمي ،ةقباسللا تاوطخلال لى اذانتسا

1. دعب نع لوصول > VPN > ةزهجال لى لى لقتنا.

2. ةحاتملا ةزهجال نم FTD زاهج ددحو دعب نع لوصول جهن مسا نييعتب مق.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 2 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:*

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices: Available Devices Selected Devices

Search

FTD-Virtual

FTD-Virtual

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.

3. ةومجم مسا وه لاصتالافيرت فلم مسا) لاصتالافيرت فلم مسا نييعتب مق 3. ةروصلافحوضوم وه امك نيوانعلتاعمجتو ةقداصلمالمدخ دح، (قفلل

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: (v)
 Authentication Server:* (+) (Realm or RADIUS)
 Authorization Server: (+) (RADIUS)
 Accounting Server: (+) (RADIUS)

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

Use AAA Server (RADIUS only) (i)
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools: (pencil)
 IPv6 Address Pools: (pencil)

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:* (+)
[Edit Group Policy](#)

Back Next Cancel

4. ةومجمالجهن عاشنالزمرلا + دح.

Add Group Policy



Name:* RemoteAccess-GP

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Save

Cancel

5. مدع ة ل ا ح ي ف . ة و م ج م ل ا ة س ا ي س س ا س ا ي ف ل ح م IP ن ي و ا ن ع ع م ج ت ن ي و ك ت ن ك م ي (ي ر ا ي ت خ ا) . ل ا ص ت ا ل ا ف ي ر ع ت ف ل م ي ف ه ن ي و ك ت م ت ي ذ ل ا ع م ج ت ل ا ن م ع م ج ت ل ا ث ي ر و ت م ت ي ، ا ه ن ي و ك ت (ق ف ن ل ا ة و م ج م) .

Add Group Policy



Name:* RemoteAccess-GP

Description:

General AnyConnect Advanced

VPN Protocols



IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:

Name	IP Address Range	
vpn-pool	192.168.55.1-192.168.55.253	 

Save Cancel

6. نېيېت مېتېو، قفنل رېع لمالك لاب تانا يېل رورم ةكرح هېجوت مېتې، وېرانېسلا اذهل
حضوم وه امك قفنل رېع رورم ل ةكرح عېمجل حامسلل مسقملا قفنل IPv4 لاصتاسايس
ةروصلال ي ف.

Edit Group Policy



Name: *

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling:

IPv6 Split Tunneling:

Split Tunnel Network List Type: Standard Access List Extended Access List

Standard Access List:

DNS Request Split Tunneling

DNS Requests:

Domain List:

Save Cancel

7. ەروصلالاي فحضوروم وه امك ظفح ددحو AnyConnect فيرعت فلمل xml. فيرعت فلم ددح.

Add Group Policy



Name:*

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](#).

Save

Cancel

8. في حالات الدخ، يلي غش التماظن التابلطتم إلى اءان ساءة بولطم ال AnyConnect روص دح. ةروص ال.

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

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

Remote Access VPN Policy Wizard

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

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

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

Show Re-order buttons

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	MAC4.7	anyconnect-macos-4.7.04056-webdeploy-k9...	Mac OS

Back Next Cancel

9. DeviceCertificates و نام ألقطنم ددح:

- SSL لىل تم دق نو كى نأ ةداهش لاو يهني VPN لىل أى لىل نراق لىل ليكشت اذه ني عى لىل صوت.

رايخ زواجتو و VPN رورم ةكح يأ صحف مدعل FTD نيوكت متي، ويرانيسلا اذه في: ةظحالمةطوطخ رييغت مت يذلا (ACP) لوصولا في مكحتلا تاسايس.

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

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

Remote Access VPN Policy Wizard

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

Network Interface for Incoming VPN Access
 Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

Device Certificates
 Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic
 All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

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

Back Next Cancel

10. تاريغيغتلار رشنو اهان إدح:

- ربح AnyConnect مزحو SSL تاداهشو VPN ةكبش ب طبترمال نيوكتلا عي مج عفد متي ةروصلال ي ف حضم وه امك (FMC) دعب نع لوصولال ي ف مكحتلا ةدحو رشن

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 Access VPN Policy Configuration

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

Name: TAC

Device Targets: FTD-Virtual

Connection Profile: TAC

Connection Alias: TAC

AAA:

- Authentication Method: AAA Only
- Authentication Server: Radius-server
- Authorization Server: Radius-server
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): vpn-pool
- Address Pools (IPv6): -

Group Policy: RemoteAccess-GP-SSL

AnyConnect Images: MAC4.7

Interface Objects: outside

Device Certificates: Anyconnect-certificate

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 Policy](#) 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.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.
- Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'outside'

Device Identity Certificate Enrollment

Certificate enrollment object 'Anyconnect-certificate' 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.

Back Finish Cancel

إفاعة NAT و HairPin

NAT ءانثتسا نيوكت 1. ةوطخال

إلى اههيجوت متيس يتل رورمال ةكرح عنمل مدختست ةلضفم ةمچرت ةقيرط وه nat افاعة نم لوصولا وأ دعب نع لوصولا) VPN قفن ربع قفدتلا وه دوصقملا نوكي امدنع تنرتنإلا (عقوم إلى عقوم).

كتكېش نم تانايېل رورم ةكرح قفدتت نأ ضرتمفملا نم نوکي آمدنع ايوررض نوکي اذه ةمچرت يأ نود قافنألأ ربع ةيلخادلا

1. ةروصلال ي فحضوم وه امك نئك ةفاضل > ةكېش ةفاضل > ةكېشل > تانئكلا لىل لقتنا

New Network Object

Name: vpn-pool

Description:

Network: Host Range Network FQDN

192.168.55.0/24

Allow Overrides:

Save Cancel

2. مقو ينعملا زاهجلا لبق نم اهمادختسا متي يتلا NAT ةسايس ددحو، NAT > زاهج لىل لقتنا

جراخلا لىل لخدلا نم رورملا ةكرح قفدت لقتني: ةظالم

Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects: Translation PAT Pool Advanced

Available Interface Objects: calo-internal-outside, inside-zone, outside-zone, outsideFW

Source Interface Objects (1): inside-zone

Destination Interface Objects (1): outside-zone

Add to Source Add to Destination

OK Cancel

3. IP عمچتك ةهوجلوا (مچرتملا ردملاو يلىصلأ ردملا) FTD فلخ ةيلخادلا دراوملا ددح ي فحضوم وه امك (مچرتملا ةهوجلوا ةيلصلأ ةهوجلوا) AnyConnect يمدختسمل يلىلملا ةروصلال

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* FTDv-Inside-SUPERNE	Translated Source: Address
Original Destination: Address	Translated Destination: FTDv-Inside-SUPERNE
Original Source Port:	Translated Source Port:
Original Destination Port:	Translated Destination Port:
vpn-pool	vpn-pool

OK Cancel

4. ةروصولل يف حضوم وه امك) تارايخلال ليدبت نم دكأت. "no-proxy-arp" و "route-lookup" نينكم تل، ةروصولل يف حضوم وه امك ok دح، NAT ةدعاق يف.

Edit NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination Interface
- Unidirectional

OK Cancel

5. NAT ءانثتسإ نينوك تل ةجيتن وه اذه.



هاندا ةحضومال تانئاللا يه قباسلال مسقلال يف ةمدختسمال تانئاللا.

Name	FTDv-Inside-SUPERNE		
Description			
Network	<input type="radio"/> Host	<input type="radio"/> Range	<input checked="" type="radio"/> Network
	<input type="radio"/> FQDN		
	10.124.0.0/16		
Allow Overrides	<input type="checkbox"/>		

Name	vpn-pool		
Description			
Network	<input type="radio"/> Host	<input type="radio"/> Range	<input checked="" type="radio"/> Network
	<input type="radio"/> FQDN		
	192.168.55.0/24		
Allow Overrides	<input type="checkbox"/>		

رغش لاس و ب د ني وكت 2. ة و ط خ ل ا

نراق هسفن ل ربق قفدتي نأ رورم ة كرح ل ا حمسي نأ ة قيرط ة مچرت اذه ، U-turn اضي أ فرعي
ىل ع نوكتي رورم ة كرح تملتس ا

دراوم ل ا ل ا ل و ص و ل ا م تي ، ل م ا ك ق ف ن ة س ا ي س ب AnyConnect ني وكت دن ع ، ل ا ث م ل ا ل ي ب س ل ع
AnyConnect ل ي م ع رورم ة كرح ن م د و ص ق م ل ا ن ا ك ا ذ ا . NAT ا ن ا ث ت س ا ة س ا ي س ل ا ق ف و ة ي ل خ ا د ل ا
ة كرح ه ي ج و ت ن ع ل و و س م ر ص ا ق ل ا (U-turn أو) NAT ن ا ف ، ت ن ر ت ن ا ل ا ل ع ي ج ر ا خ ع ق و م ل ا ل و ص و ل ا
ج ر ا خ ل ا ل ا ج ر ا خ ل ا ن م رورم ل ا

NAT ني وكت ل ب ق VPN ع مچت ن ئ ا ك ا ش ن ا ب ج ي

1. ددحو NAT ة د ع ا ق ل ق ح ي ف ة ي ئ ا ق ل ل ا NAT ة د ع ا ق د د ح و ، ة د ي د ج NAT ة ر ا ب ع ا ش ن ا ب م ق .
NAT type ك ي ك ي م ا ن ي د

2. (ج ر ا خ) ة ه و ل ا و ر د ص م ل ا ة ه ج ا و ل ا ت ا ن ئ ا ك ل ة ه ج ا و ل ا س ف ن د د ح :

Add NAT Rule ? X

NAT Rule: Auto NAT Rule

Type: Dynamic Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- calo-internal-outside
- inside-zone
- outside-zone
- outsideFW

Add to Source

Add to Destination

Source Interface Objects (1): outside-zone

Destination Interface Objects (1): outside-zone

OK Cancel

3. ردصمك IP ةهجولا ةهجاو ددحو VPN عمجت نئاك ي ل صأ ردصمك ددح ، ةمجت ب ي وبتلا ةمالع ي ف . ةروصلال ي ف حضوم وه امك ق ف اوم ددح ، مجت م .

Add NAT Rule ? X

NAT Rule: Auto NAT Rule

Type: Dynamic Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source: * vpn-pool

Original Port: TCP

Translated Packet

Translated Source: Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

OK Cancel

4. ةروصلال ي ف حضوم وه امك NAT نيوكت صخلم وه اذه .

Rules

Filter by Device Filter Rules Add Rule

#	Direction	Type	Original Packet		Translated Packet			Options	
			Source Interface Obj...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services		Translated Sources
NAT Rules Before									
1		Static	inside-zone	outside-zone	FTDv-Inside-SUPERNE	vpn-pool	FTDv-Inside-SUPERNE	vpn-pool	Dns:false route-lookup no-proxy-arr
Auto NAT Rules									
#		Dyna...	outside-zone	outside-zone	vpn-pool		Interface		Dns:false
NAT Rules After									

5. تاريغيغتلا رشنو ظفح قوف رقنا .

ةحصلا نم ققحتلا

ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

FTD رم اوأ رطس يف رم اوألا هذه ليغشتب مق

- SH crypto CA تاداهش
- show running-config ip ip pool يلملا
- show running-config webVPN
- show running-config tunnel-group
- show running-config group-policy
- show running-config ssl
- show running-config nat

اهحالص او ااطخال فاشكتسا

 نيوكتلا اذهل ةرفوتم اهلص او ااطخال فاشكتساب ةصاخ تامولعم ي ايلاح دجوت ال

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسملا اذ ه Cisco ت مچرت
ملا علاء ان أ عي مچ ي ف ن ي م دخت سمل ل معد ي و ت م م ي دقت ل ي رش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل أ مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن ت س م ل ا