

# FTD: ىلج AnyConnect VPN ليمع نيوكت NAT و HAIRpin ءانثتسا

## تايوتحملا

---

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[SSL ةءاهش ءاريتسا 1. ةوطخللا](#)

[RADIUS مءاخ نيوكت 2. ةوطخللا](#)

[IP عمجت ءاشنا 3. ةوطخللا](#)

[XML فيرعت فلم ءاشنا 4. ةوطخللا](#)

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

[AnyConnect روص ليءمجت 6. ةوطخللا](#)

[Remote Access VPN ءلاعم 7. ةوطخللا](#)

[NAT و HairPin ءافء](#)

[NAT ءانثتسا نيوكت 1. ةوطخللا](#)

[رءشلا سوبء نيوكت 2. ةوطخللا](#)

[ءحصلا نم ققءتلا](#)

[ءءالص او ءاطءألا فاشكسا](#)

---

## ةمدقملا

ىلج Cisco (AnyConnect) لىءا ءعب نع لوصولل VPN لء نيوكت ةيفيك ءنتسملا اءه فصى  
FMC ةطساوب هءراءا مءت يءلا، 6.3 راءصإلا، (FTD) FirePOWER Threat Defense

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلاءلا ءيضاوملاب ةفرعم كىءل نوكت نأب Cisco يءصوت:

- لىءصوتلا ءءآم ةقبطو ءعب نع لوصولل ةيساسألا (VPN) ةيروهائلا ءصاخلا ءكءبشلا  
ةفرعمل نم 2 راءصإلا (IKEv2) ءنءرنإلا ءاءءم لءابء ءقءاطبو (SSL) ءنمألا
- RADIUS ةفرعمو ةيساسألا (AAA) ءبسا ءملاو ضىوفءلاو ءقءاصملا
- ةيساسألا FMC ةفرعم
- FTD لوكو ءوربب ةيساسألا ةفرعم

## عمدختسملا تانوكملا

ةيلاللا ةيداملا تانوكملا وجماربالا تارادصلا لىل دنننسملا اذه يف ةدراولا تامولعملل دنننست

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

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالا نم دنننسملا اذه يف ةدراولا تامولعملل ءاشنلا مت تنانك اذا. (يضارتفا) حوسمم نيوكتب دنننسملا اذه يف عمدختسملل ةزهجالا عيمج تادب رما يال لم تحملا ريثاتلل كمهف نم دكاتف، ليغشتلا ديق كتكباش

## ةيساسا تامولعم

ASA، نيوكت لاثم ديرت تنك اذا. FTD ةزهجالا لىل نيوكتلا ةيطغت لىل دنننسملا اذه فدهي [لىل AnyConnect VPN Client U-turn تانايب رورم ةكرح نيوكت](#): دنننسملا لىل عوجرلا يجرىف [ASA 9.X](#)

دويقلا:

ةادا ASA لىل رفوتى دعب نأ ريغ، FTD لىل دنناسى ال قمس اذه، ايلاح

- FTD نم 6.5 رادصلا لىل ةرفوتم) ةجودزم AAA ةقداصم
- يكيما نيديلا لوصولل قسايس
- فيضملل صخف
- ISE Posture
- RADIUS COA
- VPN لمح نزاوم
- Cisco [CSCvf92680](#) نم ءاطخالل حيحصت فرعم 6.3 رادصلا، FirePOWER Device Manager لىل ةرفوتم) ةيلحملل ةقداصملا
- Cisco [CSCvd64585](#) نم ءاطخالل حيحصت فرعم، FlexConfig ربع ةرفوتم) LDAP قمس ةطيرخ
- AnyConnect صيصخت
- AnyConnect جمارب
- AnyConnect بييرت
- قيبطت لكل VPN ةكبش
- SCEP ليكو
- WSA لملك
- Cisco [CSCvq90789](#) نم ءاطخالل فرعم) SAML SSO
- L2L VPN و RA ل IKEv2 ةنمازتملا ةيكيما نيديلا ريفشتلا ةطيرخ
- DART، (كلذ لىل) امو بيولا نامو Umbrella و SBL و AMP Enabler و Hostscan و NAM) AnyConnect تادحو رادصلا اذه لىل يضرارتفا
- TACACS، Kerberos (KCD و RSA SDI) ةقداصم
- ضرعتسملل ليكو

## نيوكتلا

ةيلاللا تاوطخالل لامك بجى، FMC يف Remote Access VPN جلالعم لالخنم لاقنتال

## SSL ةداهش داريتسا 1. ةوطخال

ل طقف RSA لىل ةدنننسملا تاداهشلا معد متي. AnyConnect نيوكت دنننست ةيرورض تاداهشلا يف ةمومدم (ECDSA) يواضيبلا ينحنم لل يمقرلا عيقوتلا ةيمزراوخ تاداهش و IPsec و SSL ةداهش مادختسا دنننست XML فيصوت و اءديج AnyConnect ةمزح رشن نكمي ال، كلذ عم و IPsec مزحل قببسملا رشنلا لكيل بجى نكل و IPsec ل همادختسا نكمي. ECDSA لىل دنننست لك لىل ايودي XML فيرعت فلم تاثيرت عيمج عفف بجى و XML فيرعت فلم عم AnyConnect

Cisco CSCtx42595) نم ءاطخأل احيحصت فرعم) ليمع

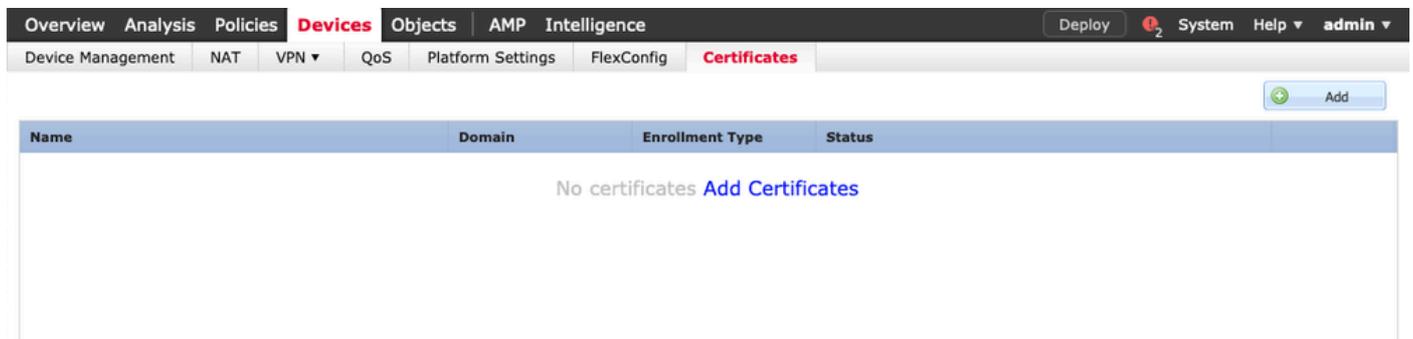
أو DNS مساب (CN) كرتشم مسا قحلم ىلع ءداهشلا يوتحت نأ بجي ،كلذ ىل ءفاضإلاب  
ببولات اضرتسم يف "اهب قوئوم ريغ مداخ ءداهش" ءاطخأ بئحتل IP ناوئع

عيقوت بلط ءاشنإ لبق (CA) قدصملا عجرملا ءداهش دوجو مزلي ،FTD ءزهجأ يف :ءظحال  
ءداهشلا (CSR).

- ءقيرط نم دصقيف ،(OpenSSL أو Windows Server لثم) يجرخ مداخ يف CSR ءاشنإ مت اذإ  
يويلا حاتفملا ليچست معددي ال FTD نأل ارظن ،لشفال ءيويلا ليچستلا
- PKCS12 لثم فلتم بولسأ مادختسا بجي .

مق CSR ءاشنإ مزلي ،يويلا ليچستلا ءقيرط مادختساب FTD زاهج ءداهش ىلع لوصحلل  
ءيول ءداهش داريتساب مق مئ قدصم عجرم مادختساب هعيقوتب

ءروصلال يف حضوم وه امك ءفاضإ دحو تاداهشلا > ءزهجأل ىل لقتنا .1



Name	Domain	Enrollment Type	Status
No certificates <a href="#">Add Certificates</a>			

ءروصلال يف حضوم وه امك ديء ءداهش ليچست نئاك فضاأو زاهجال دح .2

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 <a href="#">Add Certificates</a>			

### 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. عي قوت اه ب دصقي يتي لال اءاهش لال) CA ءءاهش قصل و ي وءي لال ليجست لال عون دء.

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:\*  

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3lTUhYpfbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogklzou6
RqV66G9IE7Z2
xIVrSrJFghkrT795kMb8am8xhb4eXYXxUgJmODIPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/lJG2LgRDraOKt+jwb57DG5K4mfZsZqhFdQP
LhBNFbyBvb9
dOjUkmdSvzQDRSqSo+HINEm3E8/q20wrtZp04MpAabyhr+hEpeP
VMrhvBOT8h
H8eMjSQjGhhHbuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDr
mwNgy5mTP9cHa
9Or3RlWRzEa11HE3mHC4Rj6DOnmgulfjx+TZRYczownSKILL7LcW1
D18ZclYmfaldC
W2cZuBR0yVDx0vq4f04ISE1BfOWFSd5rAD/bvk2n6xrJI1SLqABMJJ
uslu9KTGH1
bYKEYACKVvETw==
-----END CERTIFICATE-----
```

Allow Overrides

4. مقو FQDN نيمضت لقحل صصخم FQDN ددو ةداهشلا تاملعم بيوبتلا ةمالع ددح . ةروصلال يف ةحصولل ةداهشلا لئصافت ةئبعتب

## Add Cert Enrollment

? X

Name\*

Description

CA Information **Certificate Parameters** Key Revocation

Include 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

5. إلى ةبسنلاب .محل او مسالا رايتخا كنكمي .حاتفملا عون ددو ،حاتفم بيوپتلا ةمالع ددح . RSA ،يندا ابلطتم تياب 2048 دعي .

6. وتلل اهؤاشنإ متي تال TrustPoint ددح CERT ليحست تحتو ،زاهجل ديكاتب مقو ،ظفح ددح . ةداهشلا رشنل ةفاضإ ددح .

## 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 table lists the certificate 'Anyconnect-certificate' with a status of 'Identity certificate import required'. A warning dialog box is open, asking for confirmation to generate a Certificate Signing Request (CSR).

8. (DigiCert وأ GoDaddy، لالم لابس لىع) كيدل لضمالم CA عم هعيقوتو CSR خسنا.

9. (base64 قيسنتب نوكي نأ بجي يذلاو) قوصمالم عجرمالم نم ةيوهالا ةءاش مالتسإ درجمب، داريتسإ دح. يلحمل رتوي بمكلال ي ف ةءاشلال ناكم ددحو ةيوهالا ةءاش ضارعتسإ دح.



## 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 ناو نع فض أو Radius مداوخة ومجم يلإ مسا نيي عتب مق 2. وه امك جذومنلا اذه لامتك ا درجمب ظفح ددح، (Radius مداخل عم FTD نارق ال كترشم رس دوحو مزلي) ةروصلال ي ف حضوم.

### Add RADIUS Server Group

Name:\* Radius-server

Description:

Group Accounting Mode: Single

Retrieval Interval: (1-10) Seconds

Real-time Accounting:

- Enable
- Enable
- Enable

#### 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 عاشنإ 3. ةوطخلال

1. IPv4 تاعمجت ةفاضإ > نيوانعلا تاعمجت > تانئاللا ةرادإ > تانئاللا ىلإ لقتنا.
2. وه امك هديجت نكمي نكلو، عانقلا لقق مزلي الو، IP نيوانع قاطنوم سا نييعتب مق. ةروصلال يف حضوم.

## 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 فيرعتلال تافل مرحم ةادأ ليزنتب مق. قيبتلال.

2. في حضورم وه امك ةفاضإ ددحو مداوخلال ةمئاق ىلإ لقتنا، فيرعتلال فلم مرحم قيبتبتي 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 ناوئع وأ (FQDN) لمالكلاب لهؤم لاجم مسا وأ ضرع مسا نييغتب 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. مداخل الة مئاق ي ف اي ئرم نآل ل ا خ دإل ا ح ب صأ .

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 ا ب ظ ف ح > ف ل م ل ا ل ق ت ن ا .

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 ا ن ك م ي م س ا ب ف ي ر ع ت ل ا ف ل م ظ ف ح ا : ة ظ ح ا ل م

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

1. فلم ةفاضل > AnyConnect فلم > VPN > نئال ةرادا > تانئال ةل لقتنا FMC، ف AnyConnect.

2. كماظن ف ليمعلا فيرعت فلم عقوم دح. ضارعتسا رقناوانئال ل مسا نبيعتب مق. ظفح دحو ليلحملا.

فلملا عونك AnyConnect ليمع فيرعت فلم ددحت نم دكأت: ريدحت

## Add AnyConnect File



Name:*	<input type="text" value="Corporate-profile(SSL)"/>
File Name:*	<input type="text" value="FTD-corp-ssl.xml"/> <input type="button" value="Browse.."/>
File Type:*	<input type="text" value="AnyConnect Client Profile"/> ▾
Description:	<input type="text"/>

## AnyConnect روص ليمحت 6. ةوطخل

1. Cisco تاليزنتب ةصاخلا بيولا ةحفص نم (.pkg) بيولا ربع رشنلا روص ليزنت.

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 > نئال ةرادا > تانئال ةل لقتنا.

3. ديدحت درجمب، ليلحملا كماظن نم pkg. فلم دحو AnyConnect ةمزح فلمل مسا نبيعتب مق. فلملا.

4. ظفح دح.

## Add AnyConnect File

Name:\*

File Name:\*

File Type:\*

Description:

ملاحظة: (Windows و MAS و Linux) كتاب لظمت الى اذانتسا ةيفاضا مزح ليحت نكمي: ةظحال

## Remote Access VPN ةظخال 7. ةظخال

كذل اقو "دع نع لوصول ةظخال" ةابتا نكمي، ةقباسلا تاوخال الى اذانتسا

1. دع نع لوصول > VPN > ةزهال الى لقتنا.

2. ةحاتم ال ةزهال نم FTD زاخ دحو دع نع لوصول ةهن مسا ني عتب مق.

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:\*

Description:

VPN Protocols:  SSL  IPsec-IKEv2

Targeted Devices: **Available Devices** **Selected Devices**

Available Devices:   
FTD-Virtual

Selected Devices: 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. ةومجممال جهن عاشنال زمرلا + 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 لاصتاسا  
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:\* RemoteAccess-GP-SSL

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: Corporate-profileSSL 

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

أليات الدخ، يلي غش التماظن التابل ل طتم إلى اءان ساءة بول طم ال AnyConnect روص دح. 8. ة روص ال ف ة ضرع 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 ألة قطنم ددح:

- تم دق نوكي نأ ةداهشلاو يهني VPN لآ ي أى لى لى نراقلا لى كشت اذه ني عى لى لى صوت SSL لى لى.

رايخ زواجتو و VPN رورم ةكح ي أ صحف مدعل FTD نيوكت متي، ويرانيسلا اذه ي ف: ةظالم هطوطخ ريغ مت يذلا (ACP) لوصول ي ف 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. تاريغيغتلا رشنو ءاهنإ ددح:

- مزحو SSL تاداهشو VPN ةكبش ب ةقولعتملا تانيوكتلا عي مج عفد متي امك (FMC) ةيساسأل ةرادإلا يف مكحتلا ةدحو رشن لالخنم AnyConnect ةروصللا يف حضوم وه.

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 ءانثتسإ نيوكت 1. ةوطخال

اههيجوت متيس يتللا رورملا ةكرح عنمل مدختست ةلضفم ةمچرت ةقيرط وه NAT ءانثتسإ لوصولاً وأ دعب نع لوصولاً) VPN قفن ربع قفدتلا وه دوصقملا نوكتي امدنع تنرتنإلا لىل (عقوم لىل عقوم نم

كتكبش نم تانايبلا رورم ةكرح قفدتت نأ ضرتمفملا نم نوكي امدنع ايرورض نوكي اذه ةمجرت يأ نود قافنألا ربع ةيلخادلا

1. ةروصللا يف حضورم وه امك نئاك ةفاضلا > ةكبش ةفاضلا > ةكبش > تانئاك ىلإ لقتنا.

## New Network Object

Name: vpn-pool

Description:

Network:  Host  Range  Network  FQDN

192.168.55.0/24

Allow Overrides:

Save Cancel

2. ينعمل زاهجلا ةطساوب اهمادختسا متي يتلا NAT ةسايس ددحو، NAT > زاهجلا ىلإ لقتنا. ةديج ةلمج ءاشناب مقو

✎ جراخلا ىلإ لخادلا 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. عمجتك ةهوجل او (مجرتملا رصملا و يلصلأا رصملا) FTD فلخ ةيلخادلا دراوملا دح. IP يف حضورم وه امك (مجرتملا ةهوجل او يلصلأا ةهوجل) AnyConnect يمدختس مل يلحمللا ةروصللا.

### 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. نودبو راسملا نع شحبالا نيكم تل، (ةروصلا يف حضوم وه امك) تارايلال ليديت نم دكأت. ةروصلا يف حضوم وه امك قفاوم دح. nat. ةدعاق يف ليكو.

### 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. ءانثتسا نيوك تل ةجيتن وه اذه.



هاندا ةحضوملا تانئاللا يه قباسلا مسقلا يف ةمدختسملا 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 لاربع قفدتي نأ رورم ة ك ر ل ا حمسي نأ ة قيرط ة م ح ر ت ا ذه ، u-turn ب اضي أ فرعي  
ىل ع ت م ل ت س ا ن و كي رورم ة ك ر ل ا

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

NAT ني وكت ل ب ق VPN ع م ح ت ن ئ ا ك ا ش ن ا ب ج ي

1. د د و ، 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 و ، ة د ي ج NAT ة ر ا ب ع ا ش ن ا ب م ق .  
NAT ع و ن ك Dynamic

2. ( ج ر ا خ ) ة ه ج 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**

NAT Rule: Auto NAT Rule

Type: Dynamic  Enable

**Interface Objects** Translation PAT Pool Advanced

Available Interface Objects

Search by name

- 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. هه اول IP ناونع ددحو، VPN عمجت نئك، يلصلال ردصملا دح، عمجرت بيوبتلا عمال ع يف ة. ةروصلال يف حضورم وه امك قفاوم دح. مجرتملا ردصملا ك هه اول.

**Add NAT Rule**

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 يف حضورم وه امك NAT نيوكت صخلم وه اذه.

**Rules**

Filter by Device Filter Rules Add Rule

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

5. تاريخي غتلا رشنو ظفح قوف رقنا.

## ةحصلا نم ققحتلا

ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

FTD رماوأ رطس يف رماوأل ا هذله 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

## اهحالصإو عاطخأل فاشكتسا

نيوكتلا اذهل ا هحالصإو عاطخأل فاشكتسال ةددم تامولعم أيلاح رفوتت ال

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزي لچنل دن تسمل