

# ىلع دعب نع لوصولل VPN ةكبش نيوكت FDM ةطساوب ةرادملا FTD

## تايوتحمل

---

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[صيخرتلا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ةكبش لىطىطختلا مسرلا](#)

[FTD ىلع صيخرتلا تمققختلا](#)

[ةيمحمل تالكبشلا فيرعت](#)

[نييخلم نييمدختسم عاشنا](#)

[ةداهش ةفاضا](#)

[دعب نع لوصولل VPN ةكبش نيوكت](#)

[ةحصلا تمققختلا](#)

[اهجالصاوا عااطخألا فاشكتسا](#)

[AnyConnect لىمع لكاشم](#)

[ةيلوالا لىصتالا تالكشم](#)

[رورملا ةكرب ةصاخلا لكاشملا](#)

## ةمدقملا

ةطساوب اهترادا متت FTD ىلع RA VPN ةكبش رشن نيوكت ةيفيك دنتسملا اذه فصوي  
ثدحألا تارادصإلاو 6.5.0 رادصإلا لغشي يذلا عبرملا يف دوجوملا FDM ري دم.

## ةيساسألا تابلطتملا

### تابلطتملا

(RA ةيرهاظلا ةصاخلا دعب نع لوصولا ةكبش نيوكت بة فرعم كي دل نوكت نأب Cisco ىصوت  
VPN) FirePOWER Device Manager (FDM) ىلع

### صيخرتلا

- عم يذلا صيخرتلا ةبواب عم Firepower (FTD) ديدهت نع عافدلا ةمدخ لىجست مت  
ةمالع نيكم تب حامسلل ري دصتلا يف اهيف مكحتلا متي يتلا تازيملا نيكم مت  
("RA VPN نيوكت" بيوبتلا)

- (طوقف VPN أو Plus، APEX) انه ني كمت مت ي تال AnyConnect صي خارت نم يا

## ةمدختسمل تانوكملا

ةيلال ةيدامل تانوكملا وجماربال تارادصا لىل دنن تسملا اذه يف ةدراولا تامولعمل دنن تست

- Cisco 6.5.0-115 رادصال لغشي يذل فTD نم فTD جم انرب
- Cisco AnyConnect Secure Mobility Client، رادصال 4.7.01076

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنن تسملا اذه يف ةدراولا تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنن تسملا اذه يف ةمدختسمل ةزهجال عيمج تادب رمأ يال لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتال دي قكتك بش

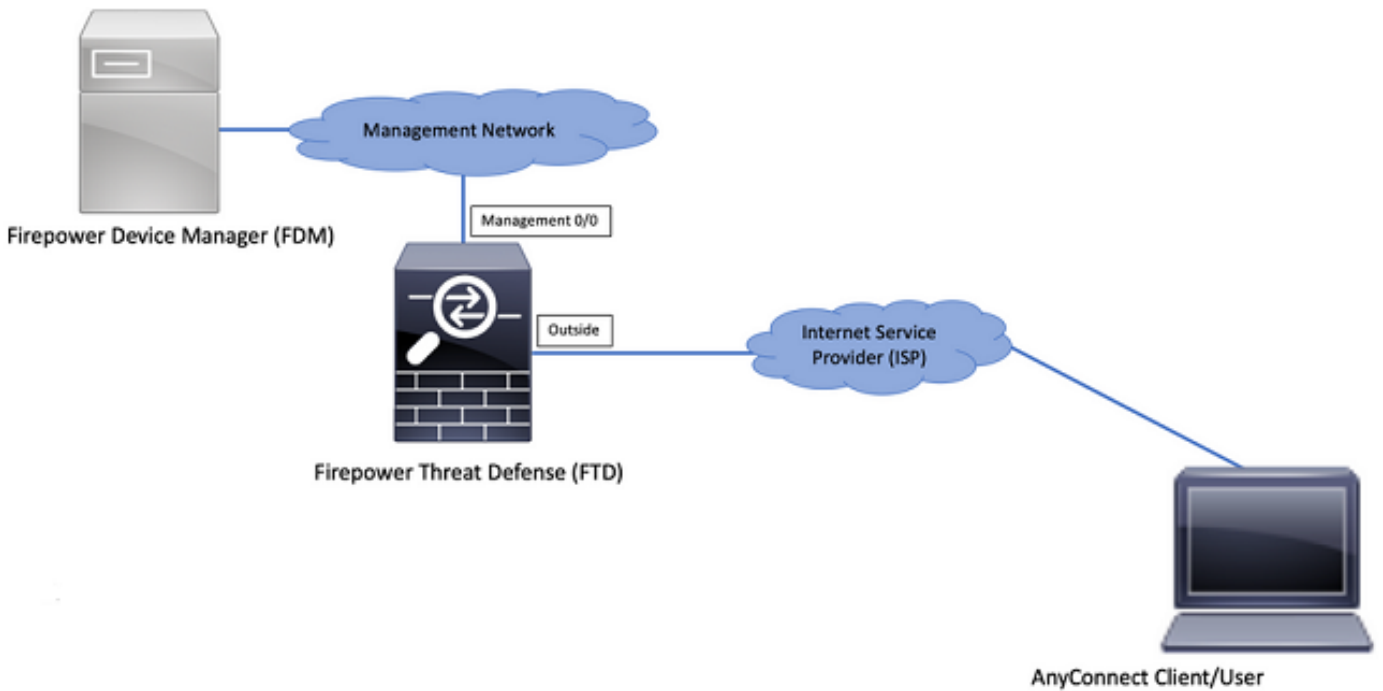
## ةيساسأ تامولعم

ءالمعل تالاصتإ عاشنإ ةلواجم دنن تابوعص FDM لال خ نم FTD لوكوتورب نيوكت هجاوي اذه. اهسفن ةهجاولا لال خ نم ةرادال لىل لوصولا ءانثأ ةيجراخلا ةهجاولا لال خ نم AnyConnect ةلكشمل هذهل [CSCvm76499](#) زيزعتال بلط فينصت مت. fdm. ةرادا لىل ع فورعم دي ق

## نيوكتلا

### ةكبشلل يطيختال مسرلا

ةيلحملا مادختساب AnyConnect Client ةقداصم



FTD لىل ع صي خرتلا نم ققحتلا

ةروصلال يف حضورم وه امك "يكلذل صيخرتلال" يف زاوجلال ليجست نم ققحت 1. ةوطخلال

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for a Cisco Firepower Threat Defense (FTD) device. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area shows a network diagram with an 'Inside Network' connected to the device's O/1 interface, and an 'ISP/WAN/Gateway' connected to O/0. The device status shows 'High Availability: Not Configured'. Below the diagram is a grid of configuration sections: 'Interfaces' (Connected, Enabled 3 of 4), 'Smart License' (Registered, highlighted with a red box), 'Routing' (No routes yet), 'Updates' (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), 'Backup and Restore', 'Troubleshoot' (No files created yet), 'Site-to-Site VPN', 'Remote Access VPN', 'Advanced Configuration', and 'Device Administration'.

ةروصلال يف حضورم وه امك زاوجلال لىل AnyConnect صيخرت نيكمت نم ققحت 2. ةوطخلال









Choose the type of internal certificate you want to create



### Upload Certificate and Key

Create a certificate from existing files.  
PEM and DER files are supported.



### Self-Signed Certificate

Create a new certificate that is signed  
by the device.

وه امك فلم لكل لي محتال رز وأ قصلل او خسنللا قيرط نع حاتفملاو ةداهشلا لي محت نكمي  
ةروصللا في حضورم:

## Add Internal Certificate



Name

Anyconnect\_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrg777/9NgonwTpLI/8/J
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRqxq3+1yBDsfVFCaKT9wWcnUveQd6LZp
k+iaN+V24yOj3vCJILihtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvwvV2TL
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

```
QzYPpjCgYEAqJ9nlk8sfPfmotyOwprlBEdwMMDeKLX3KDY58jv1/8a/wsX+uz
3A7VQn6gA6ISWHgxHdmqYnD38P6kCuK/hQMUCqdIKUITXkh0ZpglQbfW2lJ0VD4M
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGgqEfSju0Zsy2ifWtsbJrE=
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

## دع ب ن ع لوصول VPN ةك بش نيوكت

وه امك FDM لى RA VPN ج ل اع م ربع ل ق ت نا . Remote Access VPN > Create Connection Profile لى ل ق ت نا  
ةروصل ل ا ي ف ح ض وم :



Firepower Device Manager

Monitoring Policies Objects Device: firepower

Model Cisco Firepower Threat Defense for VMWa... Software 6.5.0-115 VDB 309.0 Rule Update 2019-08-12-001-vrt High Availability Not Configured CONFIGURE

Interfaces  
Connected  
Enabled 3 of 4  
View All Interfaces

Smart License  
Registered  
View Configuration

Site-to-Site VPN  
There are no connections yet  
View Configuration

Remote Access VPN  
Configured  
No connections | 1 Group Policy  
View Configuration

Advanced Configuration  
Includes: FlexConfig, Smart CLI  
View Configuration

System Settings  
Management Access  
Logging Settings  
DHCP Server  
DNS Server  
Management Interface  
Hostname  
NTP  
Cloud Services  
Reboot/Shutdown  
Traffic Settings  
URL Filtering Preferences

Device Administration  
Audit Events, Deployment History, Download Configuration  
View Configuration

Firepower Device Manager

Monitoring Policies Objects Device: firepower

RA VPN

Connection Profiles

Group Policies

Device Summary  
Remote Access VPN Connection Profiles

Search

+	NAME	AAA	GROUP POLICY	ACTIONS
<p>There are no Remote Access Connections yet. Start by creating the first Connection.</p> <p><a href="#">CREATE CONNECTION PROFILE</a></p>				

ةروصل لآ فآ ءصوم وه امك نآوك لآ ءءب و لآ صوآ فآ صوآ ءاشن:

## Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

### Connection Profile Name

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

Anyconnect

### Group Alias

Anyconnect

[Add Group Alias](#)

### Group URL

[Add Group URL](#)

ةي لحملا ةقداصملا ليلدلا اذه مدختسي . ةروصلال يف حضوم وه امك ةقداصملا قرط رتخأ

## Primary Identity Source

Authentication Type

AAA Only

Client Certificate Only

AAA and Client Certificate

Primary Identity Source for User Authentication

LocalIdentitySource



Fallback Local Identity Source 

Please Select Local Identity Source



Strip Identity Source server from username

Strip Group from Username

---

## Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source



 **Advanced**

---

Authorization Server

Please select



Accounting Server

Please select



ةروصل لا يف حضورم وه امك نئاك Anyconnect\_Pool رتخأ

## Client Address Pool Assignment

### IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect\_Pool

### IPv6 Address Pool

Endpoints are provided an address from this pool



### DHCP Servers



CANCEL

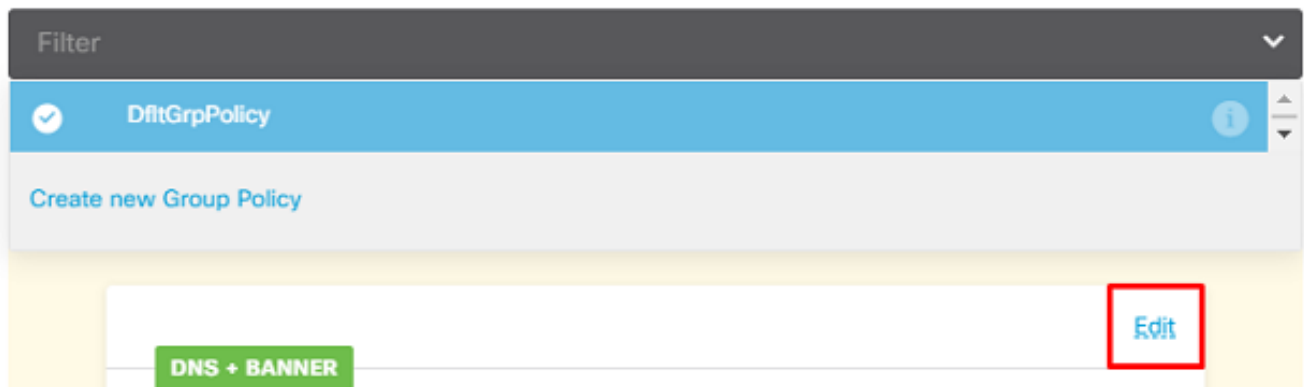
NEXT

جهن عاشن انكمي. ةلالتل ةحفصلل ي في ضارثفالا ةومجملل جهنل صللم ضرع متي اذهل Create a new Group Policy. لرايخلل رايتخاو ةلدسنملا ةمئاقلا لعل طغضلا دنع ديجه ةومجم امك ةسايسلا لعل في ريرحتلل رايتخا. ي ضارثفالا "ةومجملل جهن" مادختسا متي، ليلدللا ةروصلل ي في حضوم وه

## Remote User Experience

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.

### View Group Policy



ب نولصلتملا نومدختسملل موقبي يتح يققنلل لاصلتالا ميسقت فضا، ةومجملل جهن ي ليمع ربع ةيلخادلا FTD ةكبش لىل ةهجوملا تانايبلا رورم ةكرح لاسراب AnyConnect مدختسملل لاصلتالا نم ىرخألا تانايبلا رورم ةكرح عيمج جرت ام نيب طقف AnyConnect ةروصلل ي في حضوم وه امك

## Corporate Resources (Split Tunneling)

### IPv4 Split Tunneling

Allow specified traffic over tunnel



### IPv6 Split Tunneling

Allow all traffic over tunnel



### IPv4 Split Tunneling Networks



FDM\_Local\_Network

كلذ دع ب .تاداهشال مسق يف اهتفاضل تم Anyconnect\_Certificate رتخأ ،ةيالاتل ءحفصلال يف لوصولال يف مكحتلال جهن رتخأ . AnyConnect تالاصتلا اهيلع FTD عمسي يتللا ءهجالول رتخأ sysopt permit- اذا يرايتخأ رمأ اذه . (sysopt permit-vpn) اهريفشت ك ف مت يتللا رورملا ءكرحل يف افاتلالا ءالمع نم رورملا ءكرحل حمست يتللا لوصولال يف مكحتلال ءسايس ءاشنل بجي . راتخم ريغ sysopt permit-vpn ءروصولال يف حضورم وه امك ءةلخالل ءكبشلال ال لوصولال AnyConnect

## Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

### Certificate of Device Identity

Anyconnect\_Certificate



### Outside Interface

outside (GigabitEthernet0/0)



### Fully-qualified Domain Name for the Outside Interface

e.g. ravpn.example.com

### Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

ءطساوب ايئاقلت هن يوكت نم مي وأ Policies > NAT تحت ايودي NAT ءانثتسلا نيوكت نم مي امك لوصولال AnyConnect ءالمع اهيلع لجالحتي يتللا تالكبشلالاو ءةلخالل ءهجالول رتخأ . جالعمل ءروصولال يف حضورم وه

## NAT Exempt



### Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

### Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM\_Local\_Network

نېم دځت سمل ل نك مې (Windows/Mac/Linux) لې غشت ماظن ل لك ل AnyConnect ؤ مزح رتځأ ؤ روصال ي ف حضوم وه امك ، هب لاصتالا

## AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from [software.cisco.com](https://software.cisco.com). You must have the necessary AnyConnect software license.

### Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

NEXT

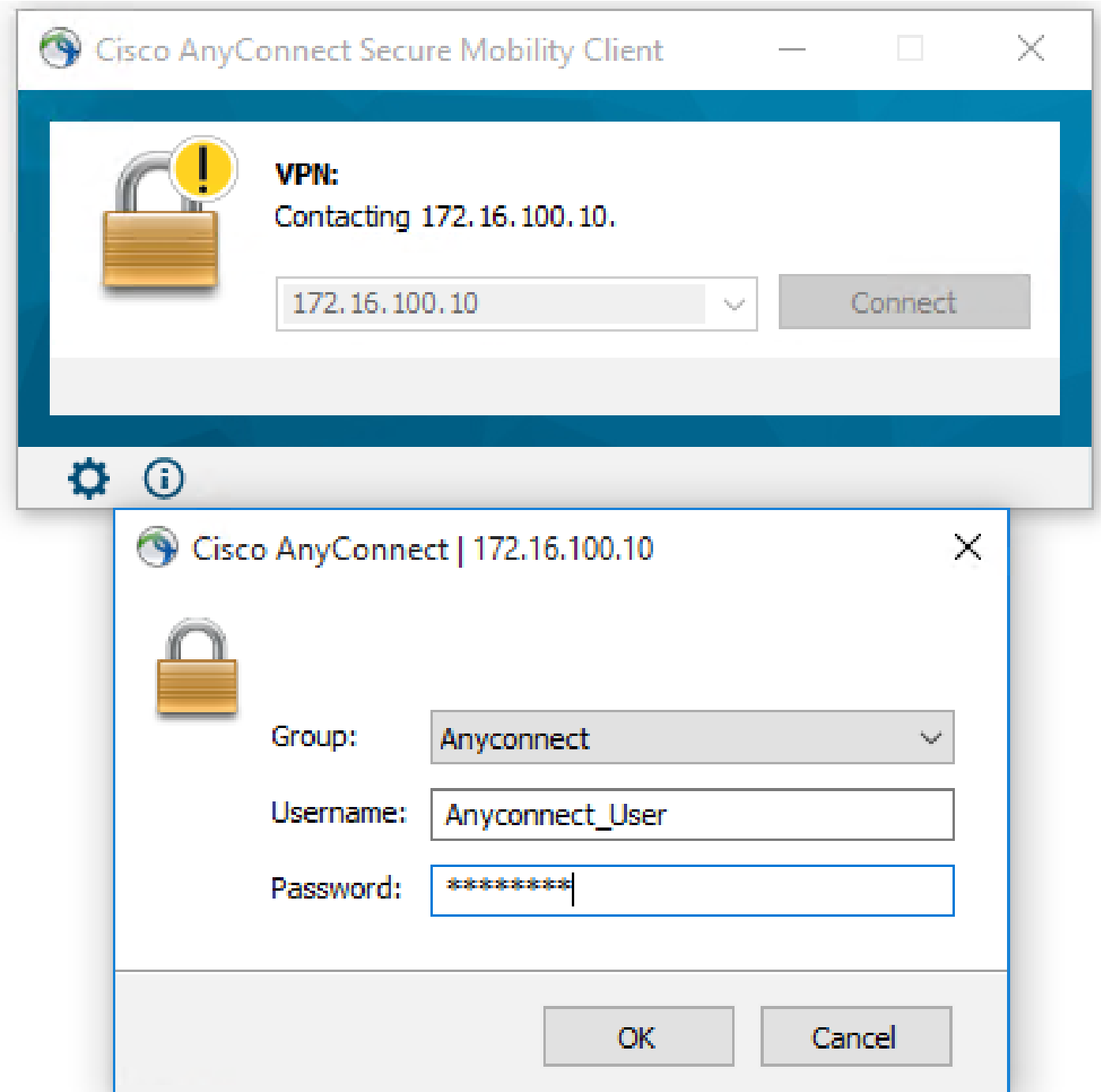
قححصلا تامل عمل نېي عت نم دكأت . هلمكأب نېوكتلل اصخلم ؤ ريځأالا ؤ حفصلال ي طعت دې دجل نېوكتل رشنو "ءاهنإ" رزلا ىلع طغضاو

## قححصلا نم ققحتلا

قححص لكشب نېوكتل لمع دېكأتل مسقلا اذه مدختسا

قجراځلا IP ىلا ل لجال موقت FQDN ؤ كېش كېدل تناك اذإ . ل لاصتالا لواچ ، نېوكتل رشن درجمب مادختسا مې ، لاثلما اذه ي ف . AnyConnect ل لاصتال ع برم ي ف ؤ كېشلا ل خدأف ، FTD ب صاځلا مسق ي ف اهؤاشنإ مت ي تال رورملا ؤ مل ك/مدختسا مسالا مدختسا . FTD ل قجراځلا IP ناوئع

ةروصولا يف حضوم وه امك FDM يف تانئاكلال



ةهجاو لال خ نم AnyConnect يف مدختسم ةبقارمل ةقيرط دجوت ال ، FDM 6.5.0 نم ارابتعا  
CLI ربع AnyConnect يف مدختسم ةبقارم وه ديحول رايلخا ل FDM ل (GUI) ةيموسرلا مدختسملا  
ةهجاوب ةصاخلا (CLI) رماوالا رطس ةهجاو مكحت ةدحو مادختسا نكمي . (رماوالا رطس ةهجاو)  
اذه مدختسا . نيمدختسملا لاصتا نم ققحتلل كلك فدم ل (GUI) ةيموسرلا مدختسملا  
رماوالا ، Show vpn-sessiondb anyconnect.



```
CLI Console
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : Anyconnect_User      Index      : 19
Assigned IP   : 192.168.19.1      Public IP  : 172.16.100.15
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx      : 15532              Bytes Rx   : 2354
Group Policy  : DfltGrpPolicy      Tunnel Group : Anyconnect
Login Time    : 11:43:20 UTC Thu Apr 16 2020
Duration      : 0h:01m:12s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                VLAN       : none
Audt Sess ID  : 000000000000130005e9844d8
Security Grp  : none                Tunnel Zone : 0

>
```

رم اوألا رطس ةهجاو نم ةرشابم هسفن رمألا ليغشت نكمي (CLI).

```
> show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : Anyconnect_User      Index      : 15
Assigned IP   : 192.168.19.1      Public IP  : 172.16.100.15
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx      : 38830              Bytes Rx   : 172
Group Policy  : DfltGrpPolicy      Tunnel Group : Anyconnect
Login Time    : 01:08:10 UTC Thu Apr 9 2020
Duration      : 0h:00m:53s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                VLAN       : none
Audt Sess ID  : 000000000000f0005e8e757a
Security Grp  : none                Tunnel Zone : 0
```





ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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 ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا