

# يطلع AnyConnect Remote Access VPN نيوكت FTD

## تايوت حمل

[عمدق مل](#)

[سياس الابلط مل](#)

[ابلط مل](#)

[عمدختس مل تانوك مل](#)

[سياس اس ا تامول عم](#)

[نيوكت مل](#)

[1. سياس الابلط مل](#)

[SSL عدهش داريت سا ا](#)

[VPN يمدختس مل نيوان عل نم عمومجم عاشنا ا](#)

[XML صيصخت فلم عاشنا ا](#)

[AnyConnect روص ليحت ا](#)

[2. دعب نع لوصول ا لاعم](#)

[لاصت ال](#)

[دويق مل](#)

[سي نم ا تارابت ع](#)

[uRPF ني كمت ا](#)

[sysopt VPN لاصت ا ب حامس مل را يخ ني كمت ب](#)

[قلص تا ذ تامول عم](#)

## عمدق مل

FTD يطلع AnyConnect Remote Access VPN ل نيوكت دننتس مل اذ فص ي

## سياس الابلط مل

### ابلط مل

سيالات ل عيصاوم لابل عم كيدل نوكت ن ا Cisco ي صوت

- TLS و IKEv2 و (VPN) سي ره اظلا ع صا خلا عكبش لابل سياس ا عم
- RADIUS عم و سياس ال (AAA) ع بس ا حمل او صي وف تل او ع قدا ص مل
- FirePOWER ع راد ا زكرم عم ع ب رجت

### عمدختس مل تانوك مل

سيالات ل عي دام ل تانوك مل او جم ارب ل ا تاراد ص ا ل دننتس مل اذ يف ع دراو ل تامول عم ل دننتس

- Cisco FTD 7.2.0
- Cisco FMC 7.2.1

- AnyConnect 4.10

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسمل اذه ي ف ةدراول ا تامولعمل اءاشن ا م ت تناك اذا .(يضا رتفا) حوسم م نيوك ت ب دنتسمل اذه ي ف ةمدختسمل ا ةزهجالا عي م ج ت اد ب رما ي ال لم ت حمل ا ري ثا تل ل كم ه ف نم دكا ت ف ، لي غ ش ت ل ا دي ق ك ت ك ت ب ش

## ةيساس ا تامولعمل

FirePOWER دي ده ت نع عاف دلا" نم 7.2.0 رادصل ا اب صاخ ل ا نيوك ت ل ل ال ا ثم دنتسمل ا اذه مدقي ةق ب ط نام ا م ادختس اب دع ب نع لوصول ل VPN ةك ب ش ل حم سي ي ذل او ، ث د ح ال ا ت ا رادصل ا او "(FTD) Cisco م ادختس ا نكم ي ، لي م ع ك .(IKEV2) ت ن ر ت ن ال ا ح ا ت ف م ل د ا ب ت نم 2 رادصل ا او (TLS) ل ق ن ل ل ا ةد د ع ت م ةيساس ا ةم ظ ن ا ي ل ع م و ع دم وه ، AnyConnect.

## نيوك ت ل ا

### ةيساس ال ا ت ا ب ل ط ت م ل ا 1.

Firepower: ةراد ا زكرم ي ف دع ب نع لوصول ا ج ل اع م ربع ل ا ق ت ن ال ل ا

- م دا خ ل ا ةق د ا ص م ل م د خ ت س ت ة د ا ه ش ء ا ش ن ا
- م د خ ت س م ل ا ةق د ا ص م ل LDAP و RADIUS م دا خ ن ي و ك ت ب م ق
- م ي م د خ ت س م ل ن ي و ا ن ع ل ا نم ع م ج ت ء ا ش ن ا ب م ق
- ة ف ل ت خ م ةيساس ا ةم ظ ن ال AnyConnect روص لي م ح ت

### SSL ةداهش داريتس ا ا

م س ال ا " ق ح ل م ي ل ع ةداهش ل ا ي و ت ح ت ن ا ب ج ي . AnyConnect ن ي و ك ت د ن ع ةي رورض ت ا د ا ه ش ل ا ب ي و ل ا ت ا ض ر ع ت س م ي ف ء ا ط خ ال ا ب ن ج ت ل IP ن ا و ن ع و ا و DNS م س ا م ع " ع و و ض و م ل ل ل ي د ب ل ا

ةي ل خ ا د ل ا ت ا و د ال ا ي ل ل ل و و ص و ل ا ط ق ف ن ي ل ج س م ل Cisco م ي م د خ ت س م ل ن ك م ي : ةظ ح ال م ا ط خ ل ا ت ا م و ل ع م و

ةداهش ل ل ي و د ي ل ل ا ل ي ج س ت ل ا ي ل ع د و ي ق ك ا ن ه :

- CSR ء ا ش ن ا ل ب ق CA ةداهش ي ل ل ا ج ا ت ح ت FTD ي ف -

- ة ف ل ت خ م ةق ي ر ط م ادختس ا ب ج ي ف ، ل ش ف ت ةي و د ي ل ا ةق ي ر ط ل ا ن ا ف ، ا ي ج ر ا خ CSR ء ا ش ن ا م ت ا ذ ا - (PKCS12).

وه له س ل ا و نم ال ا راي خ ل ا نك لو ، FTD زا ه ج ي ل ع ةداهش ي ل ع ل و و ص ح ل ل ق ر ط ل ا نم دي د ع ل ا ك ا ن ه داريتس ا م ت (CA) ق د ص م ل ا ع ج ر م ل ا م ادختس اب ه ع ي ق و ت و ، (CSR) ةداهش ع ي ق و ت ب ل ط ء ا ش ن ا : ك ل ذ ب م ا ي ق ل ل ا ةق ي ر ط ك ي ل ل ا و CSR ي ف ت ن ا ك ي ت ل ا و ، م ا ع ل ا ح ا ت ف م ل ل ةر د ا ص ل ا ةداهش ل ا

- ل ي ج س ت ة ف ا ض ا ق و ف ر ق ن ا ، Objects > Object Management > PKI > Cert Enrollment ي ل ل ل ا ق ت ن ال ا ةق ث ل ا

## Add Cert Enrollment



Name\*

vpntestbbed.cisco.com

Description

|

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
Ep0WYTGngteb6JFITtn..SZXR  
YfPCiIB7g  
BMAV7Gzdc4VspS6lJrAhbiiaw  
dBiIQmsBeFz9JkF4..b3l8Bo  
GN+qMa56Y  
lt8una2gY4l2O//on88r5IWJlm  
1L0oA8e4fR2yrBHX..adsGeFK  
kyNrwGi/  
7vQMfXdGsRrXNGRGnX+vWD  
Z3/zWl0joDtCkNnqEpVn..HoX  
-----END CERTIFICATE-----
```

Validation Usage:



IPsec Client



SSL Client



SSL Server



Skip Check for CA flag in basic constraints of the CA Certificate



Allow Overrides

Cancel

Save

- عي قوت ل ةم دخت س م ل ةداه ش ل ا (CA) ق دص م ل ع جرم ل ةداه ش ق ص ل و Enrollment Type دي دحت (CSR).
- ةرورض ل ل و ق ح ل ل ك ةب ع ت و Custom FQDN د د ح و ةي ن ا ث ل ا ب ي و ب ت ل ة م ا ل ع ل ل ق ت ن ا م ث ل ا ث م ل ل ب س ل ع :

## Add Cert Enrollment



Name\*

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Use Device Hostname as FQDN ▾

Include Device's IP Address: 10.88.243.123

Common Name (CN): vpntestbed.cisco.com

Organization Unit (OU): TAC

Organization (O): Mexico

Locality (L): MX

State (ST): CDMX

Country Code (C): MX

Email (E): tac@cisco.com

Include Device's Serial Number

Allow Overrides

Cancel

Save

- دع ت RSA، إلى ةبسنلاب .محل او مسال ارتخأ، Key Type، ددح، ةثلاثال بيوبتلا ةمالع يف ينأ دحك 2048 تب تادحو.
- Devices > Certificates > Add > New Certificate. إلى لقتنا وظفح رقنا.
- Add: قوف رقنا، اهئاشناب تمق يتال TrustPoint ددح Cert Enrollment تحتو، ددح Device، ددح مث

## 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: vpntestbed.cisco.com

- "csr" خسن نېدېدې و، Yes، مټ، ډنوقې أالې  قوف رقنا، TrustPoint، مس راوچې و، دېدې امې فې ډېدالې HTTPS مډاخ تامسل لټام م تامس ېل ع ډاهشل لېوتحت نأ بچې. ووقوا ووصل امډن عو. Import، رقناو صرقلا نم اهددح، base64 قېسننېب CA نم ډاهشل ل ملتست نأ دېدې نورت، كلكذ حجني:

Name	Domain	Enrollment Type	Status
FTD			
vpntestbed.cisco.com	Global	Self-Signed	 

### RADIUS مډاخ نېوكت (ب)

- **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group.**
- Save: رقنا، كرتشم رس عم IP ناووع فضاو مسالا أالما

# Edit RADIUS Server



IP Address/Hostname:\*

192.168.20.7

*Configure DNS at Threat Defense Platform Settings to resolve hostname*

Authentication Port:\* (1-65535)

1812

Key:\*

\*\*\*\*\*

Confirm Key:\*

\*\*\*\*\*

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing  Specific Interface

Default: Management/Diagnostic ▾



Redirect ACL:



Cancel

Save

• عملة اقل الى ع رفرى سلا ي قال تب كيه دع بو :

Name	Value	
RadiusServer	1 Server	

VPN ي مدخت سمل ني وان عل نم ة ومجم ءاشنا ج

- للاقترنت الالى Objects > Object Management > Address Pools > Add IPv4 Pools.
- بولطم ريغ عانقلاو، قاطنلاو مسالا عضو:

Name\*

vpn\_pool

IPv4 Address Range\*

10.72.1.1-10.72.1.150

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Specify a netmask in X.X.X.X format

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

► Override (0)

Cancel

OK

## د) XML صي صخت فلم عاشن |

- هحت فاو Cisco عقوم نم في رعتلا تافل م ررحم لي زنتب مق .
- للاقترنت الالى Server List > Add...
- مداوخل اعمئاق في تال اخلال ادهاشم كنكمي FQDN و ضرعلا مسا عضو:

AnyConnect Profile Editor - VPN

— □ ×

File Help

**VPN**

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

**Server List**

Profile: C:\Users\calo\Documents\Anyconnect\_profile.xml

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins
VPN(SSL)	vpntestbed.cisco....		-- Inherited --			
VPN(IPSEC)	vpntestbed.cisco....		-- Inherited --			

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

Add... Delete Edit... Details

- رقنا OK و File > Save as...

## ه) روص لېمحت AnyConnect

- Cisco عقوم نم pkg روص لېزنت
- Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- Save: رقنا، صرقلا نم PKG فلم ددوم سالال بتكا

### Edit AnyConnect File



Name:\*

File Name:\*

File Type:\*

Description:

- ةصاخلا كتابلطتم ىلع ءانب مزحلا نم ديزملا فضا.

## 2. دعب نع لوصولال جلاع م

- Devices > VPN > Remote Access > Add a new configuration.
- FTD: زاهج ديدحتو فيرعتلا فلم ةيمستب مق



## 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

FTD
-----

Add

#### Selected Devices

FTD 
---

- اقباس اهئاشن اب تمق يتل Pools Address و Authentication Server ددح Connection Profile Name بتك، لاصتال فيرعت فلم ةوطخ في ف:

## 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:\*

**i** 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:\*  +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server:  +

(Realm or 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 (Realm or RADIUS only) **i**

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:\*  +

[Edit Group Policy](#)

- Save: رقنا مٹ Client Profile، دج AnyConnect، بيوبتلا ةمالع ىلعو Edit Group Policy قوف رقنا

Name:\*

DfltGrpPolicy

Description:

General **AnyConnect** Advanced

## Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

AnyConnect profiles contains settings for the VPN client functionality and optional features. Firewall Threat Defense deploys the profiles during AnyConnect client connection.

Client Profile:

Anyconnect\_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](#).

- Next رقن او AnyConnect روص ددح، ةلالتة حفصلال في

## 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"/>	Anyconnectmac4.10	anyconnect-macos-4.10.06079-webdeploy...	Mac OS

- ةلالتة ةشاشلال في Network Interface and Device Certificates ددح،

## 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

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

## 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.

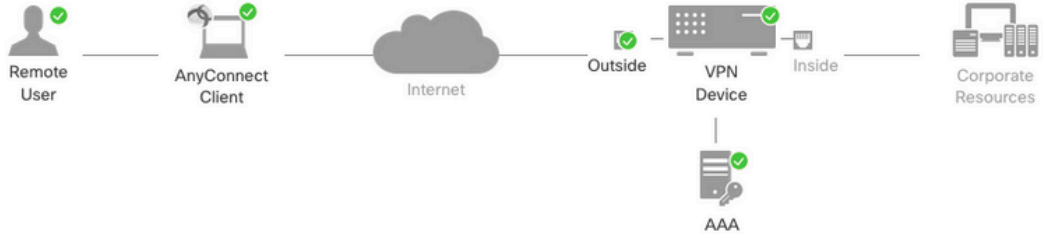
Certificate Enrollment:\*  +

## 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.*

- Deploy: م ث نم و Finish ر ق ن ل ا ك ن ك م ي ، ح ي ح ص ل ك ش ب ع ي ش ل ك ن ي و ك ت د ن ع



### Remote Access VPN Policy Configuration

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

Name:	Anyconnect_RA
Device Targets:	FTD
Connection Profile:	Anyconnect_RA
Connection Alias:	Anyconnect_RA
AAA:	
Authentication Method:	AAA Only
Authentication Server:	RadiusServer (RADIUS)
Authorization Server:	RadiusServer (RADIUS)
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
AnyConnect Images:	Anyconnectmac4.10
Interface Objects:	Outsied
Device Certificates:	vpntestbed.cisco.com

### Device Identity Certificate Enrollment

Certificate enrollment object 'vpntestbed.cisco.com' 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.

### Additional Configuration Requirements

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

#### 1 Access Control Policy Update

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.

#### 2 NAT Exemption

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.

#### 3 DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.

#### 4 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.

#### 5 Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'Outsied'

- FTD. زاهج ىللى AnyConnect مزحو تاداهش لى عم لمالك لابل نى وكتللا خسن ىللى اذه ىدوى .

## لاصتاللا

ىللى رىش ىللى ىذلا IP ناو نع و DNS مسا ب تكا ، ضرعت سم حتف ىللى جاتحت FTD ب لاصتاللا مداخ ىللى فة نزخمل دامتعالا تاناب مادختساب لوخذللى جتس تب موقت م. ةى ج راخلال ةه جاوللا ك ل ذعب جاتحت ، AnyConnect تىب تب درجم . ةشاشللى لىل تامىللى ةللى ذى فن تب مقو RADIUS Connect. قوف رقناو AnyConnect ةذفان ىللى فسفن ناو نع لىللى عضو ىللى

## دوىقلا

ASA ىللى رفوتم هنكلو ، FTD ىللى لىللى موعدم رىللى:

- و 6.2.3 FirePOWER Threat Defense ىللى موعدم رىللى RADIUS مداخ ىللى ةه جاوللا دىدحت رشنللا ءانثا ةه جاوللا رايخ لىللى لهاجت متى . مدقألا تارادصللا
- FirePOWER 6.3 دىدهت دض ةىامح ىللى مانىدىللى لىللى وختللا معدى ىللى ذللا RADIUS مداخ ب لىللى .
- و ىللى مانىدىللى لىللى وختللا لمعىللى شىدحأ رادصللا و
- و ىللى مانىدىللى لىللى وختللا لىللى نم ةومجم لىللى ةساىس رىللى غت VPN posture فTD معدى لىللى (CoA) لىللى وختللى لىللى RADIUS رىللى غت

- صي صي صي Cisco [CSCvq87631](#) ن م ااطخألا حي حصت فرعم :نيسحتل (AnyConnect صي صي صي)
- صي صي صي AnyConnect ج م ارب
- صي صي AnyConnect ب ي رعت
- صي صي WSA ل م ا ك ت
- فرعم :نيسحتل (L2L VPN و RA ل ن م ا ز ت م ل ا IKEv2 صي صي م ا ن ي د ل ا ر ي ف ش ت ل ا ط ي ر خ صي صي صي Cisco [CSCvr52047](#) ن م ااطخألا حي حصت
- ل ا م و Web Security و Umbrella و SBL و AMP Enabler و Hostscan و NAM) AnyConnect ت ا د ح و فرعم :نيسحتل (AMP Enabler ل ت ا ن ي س ح ت) ي ض ا ر ت ف ا ل ك ش ب DART ت ي ب ث ت م ت ي - (ك ل ذ صي صي صي Cisco [CSCvs06642](#) ن م ااطخألا حي حصت فرعم و Cisco [CSCvs03562](#) ن م ااطخألا حي حصت
- TACACS، Kerberos (م ا ص م) KCD و RSA SDI
- صرعت س م ل ا ل ي ك و

## صي ن م ا ت ا ر ا ب ت ع ا

ح ا م س ل ا ل ا ع ا ح ا ب ك ن ا ي ن ع ي ا ذ ه و . ل ط ع م ر ا ي خ ل ا s y s o p t c o n n e c t i o n p e r m i t - v p n ن ا ف ، ي ض ا ر ت ف ا ل ك ش ب ي ف م ك ح ت ل ا ج ه ن ر ب ع صي صي ر ا خ ل ا ه ج ا و ل ا ل ع ن ي و ا ن ع ل ا ع م ج ت ن م ي ت ا ت ي ت ل ا ر و ر م ل ا ك ر ح ب ح ا م س ل ل ا صي صي ل ل ب ق ا م و ا ل و ص و ل ا ي ف م ك ح ت ل ا ع د ع ا ق ع ف ا ض ا ن م م غ ر ل ا ل ع و . ل و ص و ل ا ح و م س م ا ه ن ا ف ، ع د ع ا ق ل ا ر ي ي ا ع م ق ب ا ط ت ل ح ض ا و ص ن ر و ر م ك ر ح ت ت ح ا ا ذ ا ، ط ق ف V P N ر و ر م ك ر ح ب ا ب ا ه ب ل ك ش ب ا ه ب .

ل ا ح ت ن ا ل ا ع ح ف ا ك م ن ي ك م ت و ه ، ه ب ي ص و م ل ا T A C ر ا ي خ ، ا ل و ا . ع ل ك ش م ل ا ه ذ ه ع ج ل ا ع م ل ن ا ج ه ن ك ا ن ه و ع ه ج ا و ل ل ( u R P F - ي د ا ح ا ل ا ث ب ل ل ي س ك ع ل ا ر ا س م ل ا ه ي ج و ت ع د ا ع ا م س ا ب ف ر ع ي ن ا ك A S A ل ع ) ح م س ي . ا م ا م ت ر ي خ ش ل ا ص ح ف ز و ا ج ت ل s y s o p t c o n n e c t i o n p e r m i t - v p n ن ي ك م ت ل ا و ه ، ا ي ن ا ث و ، صي صي ر ا خ ل ا V P N ي م د خ ت س م ن م و ي ل ل ا ل ق ت ن ت ي ت ل ا ر و ر م ل ا ك ر ح ل ي د ا ع ص ح ف ل و ا ل ا ر ا ي خ ل ا .

### ا) uRPF ن ي ك م ت

- م س ق ل ا ي ف د د ح م ، د ع ب ن ع ل و ص و ل ا ي م د خ ت س م ل ع م د خ ت س م ل ا ك ب ش ل ل غ ر ا ف ر ا س م ا ش ن ا ا .  
C. ا د ح و Add route Static Route > Routing > Edit > Device Management > Devices ل ا ل ق ت ن ا .

## Add Static Route Configuration



Type:  IPv4  IPv6

Interface\*

Null0

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

Add

any-ipv4  
FMC  
GW  
IPv4-Benchmark-Tests  
IPv4-Link-Local  
IPv4-Multicast

Selected Network

objvpusers

Gateway\*

Metric:

1

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

Cancel

OK

- يلى ع روثل لى VPN اتالاصت اهي في هتنت تي التة جاولى ع uRPF ني كمتب مق ، كلذ دع ب  
اذه **Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing.**

General	IPv4	IPv6	Path Monitoring	Hardware Configuration	Manager Access	Advanced
Information	ARP	Security Configuration				

Enable Anti Spoofing:

Allow Full Fragment Reassembly:

Override Default Fragment Setting:

Cancel OK

حسما. هيجوتلا لودج يف مدختسملا كلذل تب 32 راسملا تيبتت متي، مدختسم لاصتا دن ع uRFP ةطساوب تطقس ةكربلا نم ناو نع لمعتسم ريغ، رخآلا نم sourced رورم ةكرح صنلا يدهت دض ةياملحلا ىلع نامألا نيوكت تاملعم نييعت ىلإ عجارا Anti-Spoofing فصو ىلع عالطالل [FirePOWER](#).

## رايخ Sysopt connection permit-vpn نيكمت ب)

- وأ جلاع عمل مادختساب كلذب مايقلل رايخ كانهف، ثدحأ رادصا وأ 6.2.3 رادصا إلكيدل ناك اذا [Devices > VPN > Remote Access > VPN Profile > Access Interfaces](#).

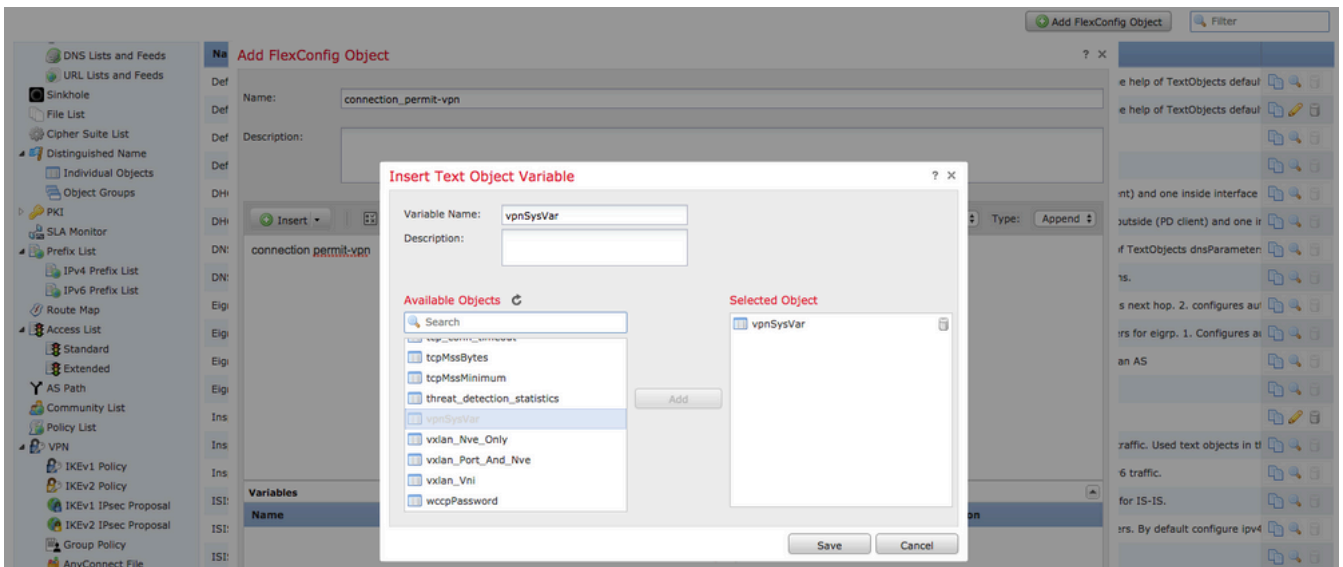
## Access Control for VPN Traffic

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

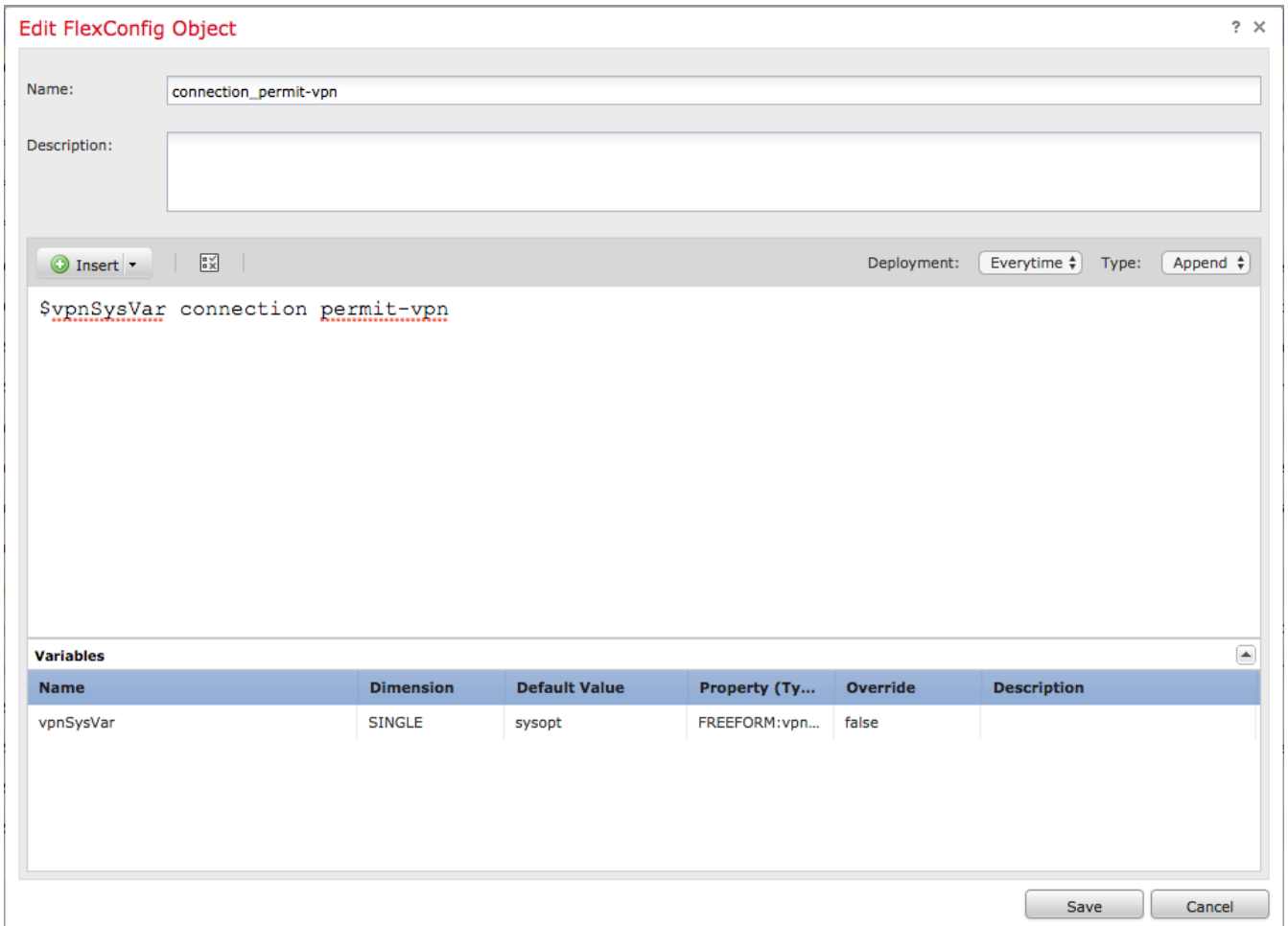
*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

- لابق تارادصإلل 6.2.3 لبق لقتنا، [Objects > Object Management > FlexConfig > Text Object > Add Text Object](#).
- sysopt ةمبيقب درفم لخدم vpnSysVar لاثملا ليبس ىلع، صن نئاك ريغتم عاشنإ.
- [Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object](#).
- رماوأل رطس ةهجاوب نئاك FlexConfig عاشنإ connection permit-vpn.
- رماوأل رطس ةهجاو يف نئاك FlexConfig يف صنلا نئاك ريغتم چاردا `$vpnSysVar connection permit-vpn` رقا Save:





- Everytime: رشن دي دحت و Append ك نئ الك FlexConfig قى ب ط ت



- New مادختساب دي دج چن عاشن و اولي لاجال چن ل ريرحت و FlexConfig Devices ل ل ا ق ت ن ال ا رز.
  - Save قوف رقنا FlexConfig، هؤاشن ا مت ي ذل ا ط ق ف ة ف ا ض ا .
  - زاهجلا لى ل ع ر م ا ل sysopt connection permit-vpn دي ورتل ل ني وكتل ا رشن .
- ن م ة دراو لا رورم ل ا ة ك ر ح ص ح ف ل ل و ص و ل ا ي ف م ك ح ت ل ا ج ن م ا د خ ت س ا ا ذ ه د ع ب ك ن ك م ي ا ل ، ك ل ذ ع م و ي ف م ك ح ت ل ا ة م ئ ا ق و ا VPN ة ك ب ش ة ي ف ص ت ل م ا ع م ا د خ ت س ا ك ن ك م ي ل ا ز ي ا ل . ن ي م د خ ت س م ل ا م د خ ت س م ل ا رورم ة ك ر ح ة ي ف ص ت ل ل ي ز ن ت ل ل ة ل ب ا ق ل ل (ACL) ل و ص و ل ا

id قېب cisco عجرم و TAC ب لصلتا ،لمعتسم VPN ل نم snort عم طبر تطقس تنأ ىري نإ [CSCvg91399](#).

## ةلص تاذا تامولعم

- [Cisco نم تاليزنتلا او ينقتلا م عدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچال مچرئى. ةصاغل متهتبل ب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لاعل او  
ىل اءمءاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيل وئسم Cisco  
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل