

عق ووملا ىلا ةدنتسملا تاسايسلا نيوكت ىلع VPN ىلا دعب نع لوصولل يفارغل نمآلا ةيامحل رادج ديدت دض عافدلا

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتلا](#)

[دودحل او تابلطتلا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ةمدخللا ىلا لوصو نئاك عاشنلا 1. ةوطخللا](#)

[RAVPN. يف ةمدخللا نئاك نيوكت قيبطت 2. ةوطخللا](#)

[ةحصللا نم ققحتلا](#)

[ةبقارملا او Syslog](#)

[تالاصتالار طح بضرعل انا هاج ماق](#)

[اهبجومسملا تالاصتالا ةبقارم](#)

[اهجالصا و عا طخألا فاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ةيفارغل عقاوم ىلا ادا نسا اهضفرو RAPN تالاصتالار حامسلا ةيلمع دنتسملا اذه فصى
"FTD" نمآلا ةيامحل رادج ديدت دض عافدلا" ىلع ةنيعم

ةيساسألا تابلطتلا

دودحل او تابلطتلا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- (FMC) نمآلا ةيامحل رادج ةرادا زكرم
- (RAVPN) دعب نع لوصولل VPN ةكبش
- يساسألا يفارغل عقاوملا نيوكت

يه يفارغل عقاوملا ىلا ةدنتسملا تاسايسلا ةيلاحلا دويقل او تابلطتلا:

- ممت يذلا (FTD) ةعرسلال قئاف لاسرالا جم انرب نم 7.7.0+ رادصإلا ىلع طقف موعدم
FMC نم 7.7.0+ رادصإلا ةطساوب هترادا
- (FDM) نمآلا ةيامحل رادج ةزهجأ ري دم ةطساوب رادملا FTD ىلع موعدم ريغ

- ةومجمل ماظن عضو يف موعدم ريغ
- بسح يفارغجل عقومل الى ةدنتسمل ةفنصمل ريغ IP نيوانع فينصت متي ال ءارج تامدخل الى لوصول يف مكحتل ةدحو ضرقت ،بابسأل هذهلو .يفارغجل لصلال .يضارتفال ةمدخل الى لوصول ةسايس
- تاحفص ىلع يفارغجل عقومل الى ةدنتسمل ةمدخل الى لوصول تاسايس قبطنت ال .دويق نود "نمأل ليمعلا" ليزنت كل حيتي امم ، WebLaunch.

ةمدختسمل تانوكمل

ةيلاتل جماربل تارادصل الى دننتسمل اذه يف ةدراول تامولعمل دننتس

- Secure Firewall، رادصلال 7.7.0
- Secure Firewall Management Center، رادصلال 7.7.0

[VPN لوصول قراذ زاهج](#) نيوكت ليلدي يف ةزيمل هذه لوح ةلماك ليصافت ىلع روثعل نكمي Cisco Secure Firewall Management Center 7.7 لخال [يفارغجل عقومل](#) مسق [ىلا اذانتسا نيدي عبلال ني مدختسمل](#) 7.7.

ةصاخ ةيلمعم ةئيب يف ةدوجومل ةزهجال نم دننتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضارتفا) حوسمم نيوكتب دننتسمل اذه يف ةمدختسمل ةزهجال عيمج تأدب رملأال لمحتمل ريثأتلل كمهف نم دكأف ،ليغشتل دي قكتكبش

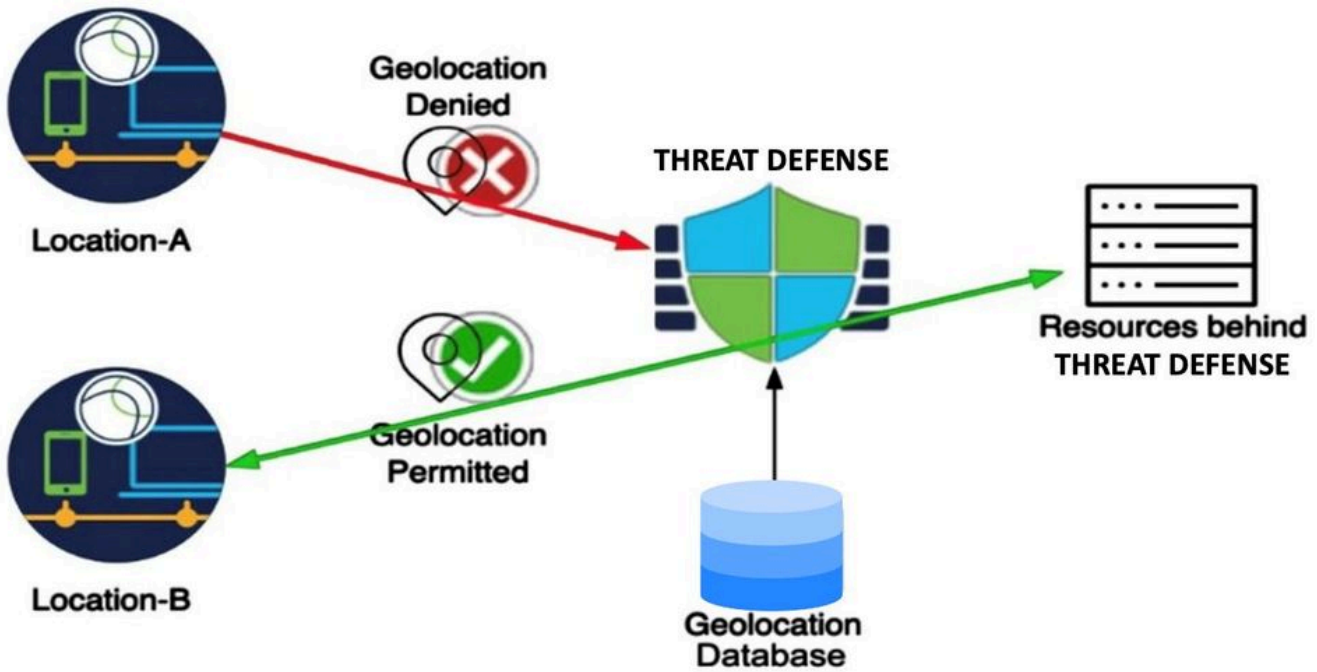
ةيساسأ تامولعمل

ةكبشلل نامأ يف ةريبك ةميقي يفارغجل عقومل ىلع ةمئاقلا لوصول تاسايس رفوت نكمي ،يديلقت لكشبو .يفارغجل اهلاصل الى اذانتسا رورمل ةكرح رطحب حمسي امم ،مويلا ةماعلا ةكبشلل رورم ةكرحل تانايبلا رورم ةكرح الى لوصول تاسايس ديدحت تاسسؤملل يف مكحتل قيبطت نكممل نم ،ةزيمل هذه ميديقت عم ،نأل .ةياملحال رادج ربع رمت يتل ةيرهاظلا ةصاخلا ةكبشلل لمع تاسلج تابلطل يفارغجل عقومل الى دننتسمل لوصول (VPN) دعب نع لوصولل

ةيلاتل تازيمل ةزيمل هذه رفوت

- تابلطب حامسلل دعاوق عاشنإ ءالمعلل نكمي :يفارغجل عقومل الى ةدنتسمل دعاوقل اذهو .تاراقلا وأ نادلبلا لثم ،ةنيعم ةيفارغجل قطانم الى اذانتسا اهضفر وأ RAVPN VPN تاسلج ادب اهنكمي يتل ةيفارغجل عقومل يف قيقلل مكحتلاب حمسي
- ضفرل ءارجال دعاوقل هذه ةطساوب ةدحمل لمعل تاسلج رطح متي :ةقداصلمل لبق رطح اذه دعاسي .نامأل ضارغل حيحص لكشب تالواحمل هذه ليجست متي و ،ةقداصلمل لبق اهب حرصمل ريغ لوصول تالواحمل نم دحل يف يقابتسال ءارجال
- ةيميظنتل تاسايسلاب مازتلال نامضي يف ةزيمل هذه دعاستو :نامأل او قفاوتل يف (VPN) ةيرهاظلا ةصاخلا ةكبشلل مداخل موجهل حطس ليلقت عم ،ةيلحمل ةيرادلل او هسفن تقولا

لوصول انكومي IP نيوانع ىل عيوتحت (VPN) ةيرهاظلا ةصاخلا تاكبشلل مداوخ نأل ارظنو
تاسسؤملا نكمي يفارغلل عقوملا ىللا ةدنتسملل دعاوقلا لاخدا نإف ،تنترنال ربع اهيلي
نم دحلل يلاتلابو ،لاعف لكشب ةنيعم ةيفارغلل عقاوم نم مدختسملل تابلط ديقت نم
ةمشاغلل ةوقلا تامجهل ضرعتلا

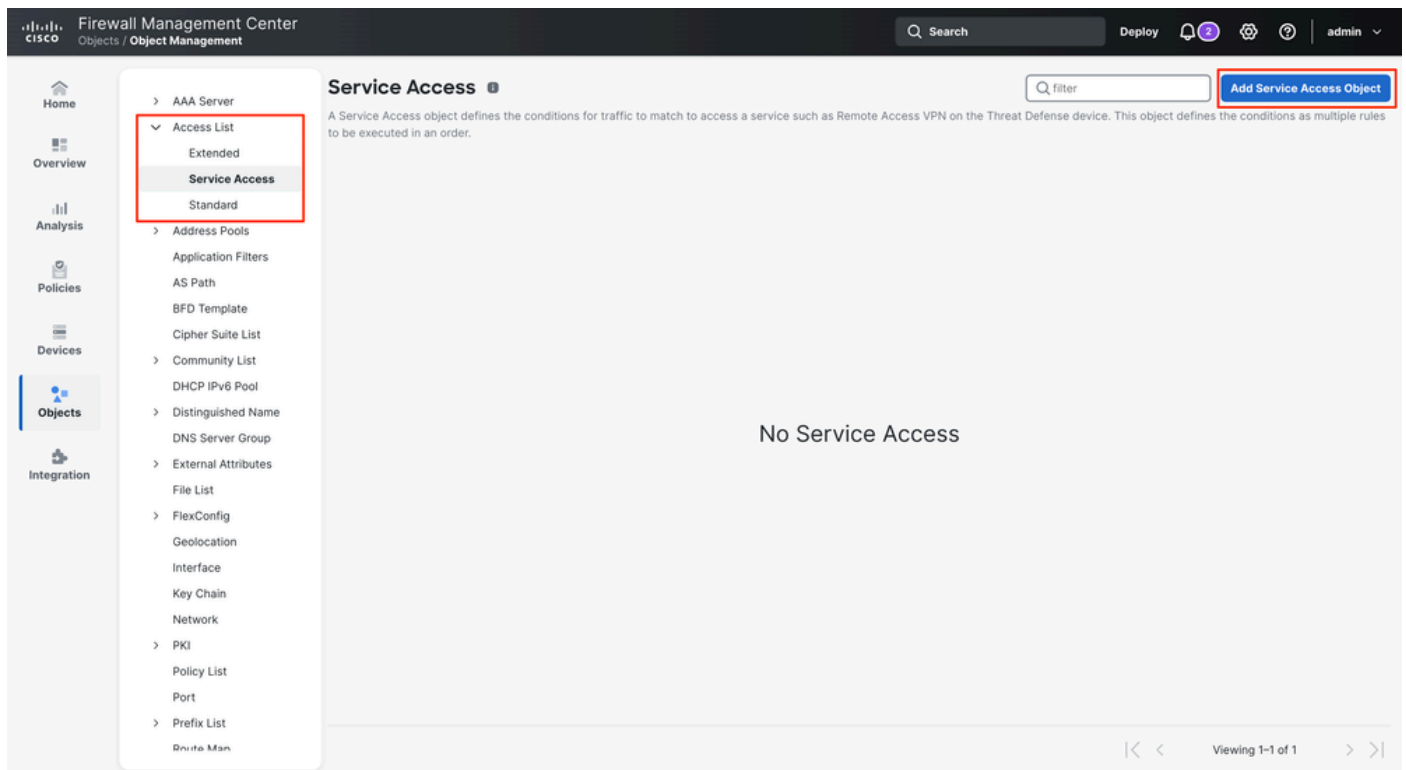


نيوكتلا

ةمدخللا ىللا لوصولل نئاك ءاشنإ 1. ةوطخلل

1. نمآلا ةياملل رادج ةرادإ زكرم ىللا لوخدلا لچس .

2. قوف رقناو ةمدخللا ىللا لوصولل ءاشنإ > تانئاكلا ةرادإ > تانئاكلا ىللا لقتنا .
ةمدخللا ىللا لوصولل نئاك ءاشنإ



3. ةدعاق ةفاضل قوف رقنا مٲ ،ةدعاقلا مسا ددح .

Add Service Access Object ?

Name *

deny-X-locations

Add Rule

Sequence	Action	Geolocation

Default Action
☒ Allow All Countries
 ☐ Allow Overrides

Cancel

Save

4. ةمدخلال ال لوصول ةدعاق نلوكٲب مق :

- ضفرل وأ حامسلا :ةدعاقلا ءارجإ ددح .
- لبق نم يفارغجل عقوملا ديدحت تانئاك وأ تاراق وأ نادلب ددح ،ةحاتملا نادلبلا نم .
- يفارغجل عقوملا ديدحت ةمئاق ىلا اهلقنو مدختسملا .
- ةدعاقلا ءاشنإل ةفاضل قوف رقنا .

✎ وأ دلبل) يفارغجل عقوملا نئاك مادختسا نكمي ،ةمدخل ىلا لوصول نئاك يف :ةظحالم طقف ةدحاو ةدعاق يف (صصخملا يفارغجل عقوملا وأ ةراقلا .

✎ نكمي ال شيح ،حيحصلا بيترتلاب ةمدخل ىلا لوصول دعاقو نيوكت نم دكأت :ةظحالم دعاقولا هذه بيترت ةداع .

Add Service Access Rule



☐ Deny

Available Countries *

Available Geolocation

254 available

☐ Africa
 ☐ Aland Islands
 ☐ Albania
 ☐ Algeria
 ☐ American Samoa
 ☐ Andorra
 ☐ Angola



Selected Geolocation

3 available

☐
☐
☐

Cancel

Add

5. ىلع ءارجإلا اذه قبطني .لودلا لك ضفرت اي لودلا لكل حمست اي :يضارتفالا ءارجإلا رتخأ .

اهنيوكت مت يتلا ةمدخل ىلا لوصول دعاقو نم يأ قباطت ال يتلا تالاصتالا .

Add Service Access Object



Name *

deny-X-location

Add Rule

Sequence	Action	Geolocation	
1	DENY	 +1 more	 

Default Action

Allow All Countries

☐ Allow Overrides

Cancel

Save

6. حذف قوف رقنا.

RAVPN في مداخل نئك نيوك قيبطت 2. موطخا

هجاو > RAPN نيوك نئك > دع نع لوصول > زهجال في RAPN نيوك الى لقتنا 1. لوصول.

هأشنأ يذلا مداخل الى لوصول نئك دح، مداخل الى لوصول في مكحتل مسق في 2. اقباس.

Firewall Management Center

Devices / VPN / Edit Interface Profile

Q Search

Deploy

13

admin

Home

Overview

Analysis

Policies

Devices

Objects

Integration

RAVPN-ao-ftdv-02

You have unsaved changes

Save

Cancel

Enter Description

Name	Interface Trustpoint	DTLS	SSL	IPsec-IKEv2
Outside				

Access Settings

Allow Users to select connection profile while logging in

Enable HTTP-only VPN Cookies

SSL Settings

Web Access Port Number:*

443

DTLS Port Number:*

443

SSL Global Identity Certificate:

+

Note: Ensure the port used in VPN configuration is not used in other services

IPsec-IKEv2 Settings

IKEv2 Identity Certificate:

+

Service Access Control

Remote clients' access to VPN can be controlled in Threat Defense devices from Version 7.7 and later using a service access object. This object provides geolocation-based access control to clients before VPN authentication.

Service Access Object:

deny-X-location

+

Add Rule

Sequence	Action	Geolocation
1	DENY	

+1 more

Default Action

Allow All Countries

Note: By default, there is no access control for RA VPN, and remote clients can connect from any geolocation unless specified by a service access object.

3. عارجال او دعاوقال صخلم نآلا هديحتب تمق يذلا ةمدخال الى لوصولو نئاك ضرعي .
كلذ ةحص نم دكأت .يضا رتفال

4. نيوكتال رشنب مقو تاريغيغتال ظفحا ،اريخأ .

ةحصلال نم ققحتال

كل حيتي امم ،ةمدخال الى لوصولو ي ف مكحتال مسق ي ف دعاوقال رهظت ،نيوكتال ظفح درجمب
اهب خامسال وأ اهرظح مت ي تال لودالو تاوعومحمال نم ققحتال

Service Access Control

Remote clients' access to VPN can be controlled in Threat Defense devices from Version 7.7 and later using a service access object. This object provides geolocation-based access control to clients before VPN authentication.

Service Access Object:

deny-X-location

+

✎

Add Rule

Sequence	Action	Geolocation
1	DENY	 +1 more

Default Action

Allow All Countries

Note: By default, there is no access control for RA VPN, and remote clients can connect from any geolocation unless specified by a service access object.

إلى لوصول دعاوق رفوت نامضل show running-config service-access رمأل لىغشتب مق
ب ةصاخال (CLI) رمأوال رطس ةهجاو نم ةمدخلال FTD.

<#root>

firepower#

show running-config service-access

```
service-access deny ra-ssl-client geolocation FMC_GEOLOCATION_146028889448_536980902
service-access permit ra-ssl-client geolocation any
```

```
firepower# show running-config object-group idFMC_GEOLOCATION_146028889448_536980902
object-group geolocation FMC_GEOLOCATION_146028889448_536980902
location "Country X"
location "Country Y"
```

ةبقارملل او Syslog

RAPN تالاصتاب ةقلعتمل ائادخال طاقائل ةديج syslog تافرم نمأل ةيامل راج مدقي
ي:فارغلل عقومل إلى ةدنتسمل تاسايسل ةطساوب اهرطح متي يتل

- عقومل إلى دنتسي جهن لبق نم IKEv2 لاصتا ضفرة لى إلى 761031 ري شي
ةي:فارغلل VPN ليجست ةئف نم اعزج syslog اذه دي .ي:فارغلل

<device_ip> ناوع <client_ip> ل IKEv2 ل دعب نع لوصول لمع ةسلج ضفر مت :%ftd-6-751031
(geo=<country_name>, id=<country_code>) ةي:فارغلل ةدعاق ةطساوب

- يفارغجلا عقوملا ىلإ دنتسي جهن لبق نم SSL لاصتا ضفر تقوى ىلإ: 751031 ري شي .
ةيلاجلا WebVPN ليجست ةئف نم اعرج syslog اذه دعي .

ةدعاق ةطساوب <client_ip> ل SSL ىلإ دعب نع لوصول لمع ةسلج ضفر مت :%ftd-6-716166
(geo=<country_name>, id=<country_code>) ةيفارغج

 اهنى كم مت دنع ايمولعم ةدي دجلال syslogs هذهل يضارتفالا ةروطخالا ىوتسم نو كي :ةظحال م
لكشب هذهل syslog تافرعم ني كم مت كن كم مي ، كلذ عم و .ةلباقم لال ليجستالا تائف نم
اهتروطخ صيصختو يدرف .

تالاصتالا رظحب ضرعلا زاهج ماق

> اءالصالوا ءاطخالا فاشكتسا > ةزهجالا ىلإ لقتنا ، ةروطخم لال تالاصتالا ءحص نم ققحتلل
تالاصتالا ب ءقلعتم لال ءالءسالا ضرعت ، انه . ءالءسالا ءاطخالا فاشكتسا
ةسلجلال عونو لالاصتالا ىلع رثؤت يتلا ءاوقلا نع تامولعم كلذ ي ف ام ب ، ةروطخم لال

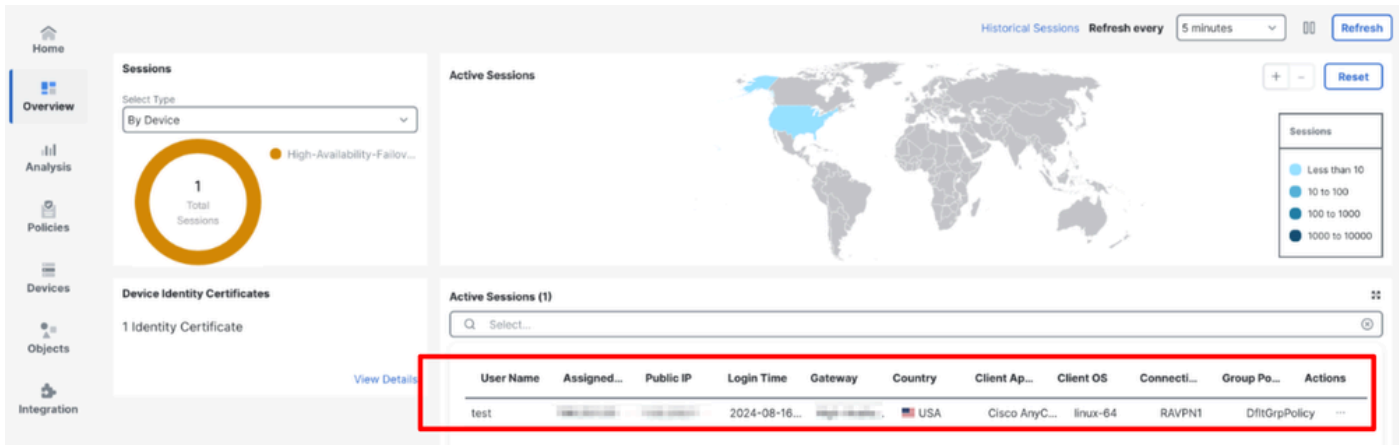
 ءاطخالا فاشكتسا ءالءس ي ف تامولعملال هذهل عمجل syslog ني وكت ب جي :ةظحال م
اءالصالوا .

Bookmark This Page Create Report Dashboard View Bookmarks Search									
No Search Constraints (Edit Search)									
Table View of Troubleshooting Logs									
	Time	Severity	Message	Message Class	Username	Device			
+	11:05:58	Emergency	Denied IKEv2 remote access session for faddr [redacted] laddr [redacted] by a geo-based rule (geo="North Korea", id=408)	IKE and IPsec		192.168.0.141			
+	11:05:41	Emergency	Denied SSL remote access session for faddr [redacted] by a geo-based rule (geo="North Korea", id=408)	WebVPN and AnyConnect Client		192.168.0.141			

اهب حومسم لالاصتالا ءبقارم

دع ب نع لوصول ل VPN تامولعم ءحول > ءماع ءرظن ي ف اهب حومسم لال ءاسللال ءبقارم مت
أشنم لال ءلود كلذ ي ف ام ب ، ءسلجلال تامولعم ضرع متي شيح .

 حومسم لال ني مدختسم لالوا اهب حومسم لال لودلا نم طقف تالاصتالا ضرع متي :ةظحال م
ي ف اهضفر مت يتلا تالاصتالا ضرع متي ال . هذهل تامولعملال ءحول ي ف لالاصتالا ب مهل
هذهل تامولعملال ءحول .



اهحال صإو عا طخال فاشكتسا

ةيلاتلا تاوطخال عبتا ، اھحال صإو عا طخال فاشكتسا ضارغل

1. ةمدخلال ىلا لوصوللا نئاك يف ححص لكشب دعاوقلا نيوكت نم ققحت .
2. دن ع اھحال صإو عا طخال فاشكتسا تالچس مسق يف syslog ضفر رهظي ناك اذا امم ققحت .
لمع ةسلجل هب حومسمل يف ارغل عقوملا بلط
3. وه ام قباطي (FTD) ةيساسالا ةرادإلا يف مكحتلا ةدحو يف حضوملا نيوكتلا نا نم دكأت .
FTD يف (CLI) رماوالا رطس ةهجاو يف
4. فاشكتسا ضارغل ةديفملا لىصافتلا نم ديزملا عمجل ةيلاتلا رماوالا مدختسا .
اهحال صإو عا طخال :

- debug geolocation <1-255>
- show service-access
- show service-access detail
- show service-access interface
- ةمدخلال ىلا لوصوللا عقوم راهظا
- show service-access service
- <Country> Geodb IPv4 عقوم لىصافت ضرع
- show geodb counters
- show geodb ipV4 [lookup <ip address>]
- show geodb ipV6

ةلص تاذا تاملولعم

- [تاهج](#): حلص ممد دقع مزلي . TAC ب لاصلتالا ىجري ، ةيفاضا ةدعاسم ىلع لوصولل
- [Cisco نم ةيملعلا ممدلا لاصلتا](#)
- [انه](#) Cisco VPN عم تجم ةرايز اضيا كنكمي

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل 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 م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا