

نع لوصول تاديدهتلا نع فشكلا نيوكت نع نمآلا عافدلا ىلع VPN تامدخ ىلا دعب ةيامحل رادج مادختساب ديدهتلا

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسألا تامولعم](#)

[نيوكتلا](#)

[طوقف \(ةحلصل، ريغ\) ةيلخادلا VPN تامدخ لاصلتالا تالواحمل تاديدهتلا فاشتكلا: 1 ةزملا](#)

[دعب نع لوصول VPN ةكبش لي مع ادب تامحل تاديدهتلا فاشتكلا: 2 ةزملا](#)

[دعب نع لوصول VPN ةقداصم لش فل تاديدهتلا فاشتكلا: 3 ةزملا](#)

[ةحصلا نم ققحتلا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ىلع VPN تامدخ ىلا دعب نع لوصول ديدهتلا فاشتكلا نيوكت ةي لمع دنتسملا اذه فصى Cisco نم (FTD) نمآلا ةيامحل رادج ديدهت دض عافدلا

ةيساسألا تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت ناب Cisco ي صوت:

- Cisco نم (FTD) ةيامحل رادج ديدهت نع نمآلا عافدلا
- Cisco نم (FMC) نمآلا ةيامحل رادج ةرادا زكرم
- FTD ىلع (RAVPN) دعب نع لوصول VPN ةكبش

تابلطتملا

نم نمآلا ةيامحل رادج ديدهت دض عافدلا تارادصا ي هذه تاديدهتلا فاشتكلا تازيم معد متي
ةيلاتلا ةمئاقلا ي ةجردملا Cisco:

- 7.0.6.3 ي ف موعدم -> 7.0 رادصإلا راطق

ةمدختسملا تانوكملا

ةغيص ةي جمر بو زاهج اذه ىلع ةقيثو اذه ي فصى ةمولعملا تسسأ:

- Cisco 7.0.6.3 نم نم آلا ةيامحل راج ديدهت دض عافدلل يره اظلا رادصالا

ةصاخ ةي لم عم ةئيبي في ةدوجوملا ةزهجالا نم دنتسمل اذو في ةدراولامول عملا عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسمل اذو في ةمدختسمل ةزهجالا عيمج تادب رما يال لم تحملا ريثاتلل كمهف نم دكأتف، ليغشتلا ديقتك تكبش


ةيساسا تامولعم

(VPN) ةيره اظلا ةصاخلا ةكبشلا تامدخب ةصاخلا تاديدهتلا فاشتك تازيم كل حيتت ةيلالاتلا تاهوي رانيسلا نم يا دض ةيامحل ةينكامل دعب نع لوصولل


1. لاصتالا ةلواحم يا. دعب نع لوصولل VPN تامدخ ةيصالصا غلال لاصتالا تالواحم. طقف يلخادلا مادختسالل ةصصخملا تامدخالل
2. لىل دعب نع لوصولل لاصتالا تالواحم ليغشتب مجاهملا موقبي شبح، ليمعلا ادب تامجه. ال هنكلو دحاو فيضم نم ةرركتتم تارم VPN ةكبشب ةصاخلا ثبالاو لابقستالا ةدحو تالواحملا هذه لمكي
3. حسملا تامجه) VPN تامدخ لىل دعب نع لوصولل ةرركتتملا ةلشافلا ةقداصملا تالواحم. (ةوقلاب رورملا ةمك/مدختسم مسال يئوضلا)

عنمو ةيباسح دراوم كالهتسا، لوصولل ةلواحم في اهلاشف دنع ىتح، تامجهلا هذه نكمي دعب نع لوصولل VPN تامدخب لاصتالا نم نيقيقي قحلا نيمدختسمل

دودحل زواجتي يذلا (IP ناووع) فيضملا نم آلا ةيامحل راج ب نجتتي، تامدخال هذه نيكمت دنع ايودي IP ناووع ةوجف ةلازاب موقت ىتح تالواحملا نم ديزم عنمل، ايئاقلت اهنيوكت مت يئلا

 لكشب VPN لىل دعب نع لوصولل تاديدهتلا فاشتك تامدخ عيمج لي طعت متي: ةظحالم يضا رتفا

نيوكتلا

 "ةيامحل راج تاديدهت نم ةنم آلا ةيامحلا" لىل تازيملا هذه نيوكت معد متي ال: ةظحالم FlexConfig ربع ال ايلاح

1. نم آلا ةيامحل راج ةرادا زكرم لىل لوخدلا لجس.
2. FlexConfig > FlexConfig > تانئال ةرادا > تانئال لىل لقتنا، FlexConfig تانئال نيوكت ل FlexConfig تانئال ةفاضل قوف رقتنا م، Object.

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** 1 Integration

Deploy 🔍 ⚙️ admin 🔒 SECURE

FlexConfig Object

Add FlexConfig Object 🔍 Filter

FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig policies.

Name	Description	
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]
[Redacted]	[Redacted]	[Icons]

3. تازيم نيكمتل بولطلم نيوكتلل فضا، FlexConfig نئاك ةفاضل ةذفان حتف درجم ب. دعب نع لوصول VPN ةكبش ةصاخلا تاديدهتل فاشتك

- FlexConfig: enable-threat-detection-range نئاك مسا
- FlexConfig: نئاك فصو دعب نع لوصول VPN تامدخل تاديدهتل فاشتك نيكمت
- ةدحاو ةرم: رشنل
- قاحلل: ةباتكلا
- ةحاتملا تازيملا لىل اذانتسا "تاديدهتل فاشتك ةمدخ" رماو افضا: صنلا عبرم اقحالة حضورملا

✎ VPN ةكبش ل ةرفوتملا ثالثل تاديدهتل فاشتك تازيم نيكمت كنكمي: ةظالم نئاك ءاشن كنكمي و، هسفن FlexConfig نئاك مادختساب دعب نع لوصول ةصاخلا اهنيكمت متيل ةزيم لكل يدرف لكشب دحاو FlexConfig.

ريغ) ةيلخادلا VPN تامدخ لاصتالا تالواحمل تاديدهتل فاشتك: 1 ةزيملا طقف (ةحلاصل)


عبرم يف تاديدهتل فاشتك ةمدخل invalid-vpn-access رمال ةفاضل مق، ةمدخل هذه نيكمتل FlexConfig نئاك صن

دعب نع لوصول VPN ةكبش ليمع ادب تامجهل تاديدهتل فاشتك: 2 ةزيملا

access-client-initiations دعب نم تاديدهتل فاشتك ةمدخ رمال فضا، ةمدخل هذه نيكمتل FlexConfig نئاك صن عبرم يف <count> دح <count>:

- تالواحم باسح اهلالخ متي ادب ةلواحم رخا دعب ةرتفل <minutes> تقوئملا فاقيل ددحي متي تل ةبتعلاب يف ةليلاتملا لاصتالا تالواحم ددع ناك اذا. ةليلاتملا لاصتالا نيغيت كنكمي. مجاهملا لاصتالا IPv4 ناوع بنجت متيسف، ةرتفل هذه لالخال اهنيوكت ةقيد 1 و 1440 ني ب ةرتفل هذه
- لىغشتل راطتالا ةرتفل لالخال ةبولطملا لاصتالا تالواحم ددع وه <count> Threshold ني ب لصال دحل نيغيت كنكمي. بنجت 100 و 5

بنجت متيسف 20، ةبتعلال او قئاقد 10 يه قيلعتلا ةرتفل تناك اذا، لالملا لىبس لىل قئاقد 10 يدما يف ةليلاتم لىصوت ةلواحم 20 كانه تناك اذا ايئاقلت IPv4 ناوع


 لمعتسي نإ. رابتعالا في NAT مادختسا عض، دحلاو قيلعتلا ميقي نيعت دنع: عظام الم نمضي اذهو. يلعأ عميقي عار، ناووع هسفن لال نم بلط ريثك حمسي يأ، برض تنأ في، لاثملا ليبس يلع. لاصتال لفاك تقوي لعل نيححيصلال نيمدختسملا لوصح. قريصق عرتف في لاصتالا ةلواحم نيمدختسملا نم ديدعلل نكمي، قندنفلا


دعب نع لوصول VPN ةقداصم لشفل تاديدهتلا فاشتكا: 3 ةزيمل

فاشتكا ةمدخل دعب نع لوصولا دييقت رمأ فضا، ةمدخلال هذه نيكمتمل
ثيح، FlexConfig نئاك صن عبرم في <count> دحلا <قيدق> تاديدهتلا

- تالاح باسح اهلالخ متي ةلشاف ةلواحم رخأ دعب عرتفلا <minutes> تقوؤملا فاقيا إلالا ددحي
يذلا دحلا في فوتسي ةيلالتملا ةقداصملا لشف تالاح ددع ناك اذاو. ةيلالتملا لشفلا
هذه نيعت كنكمي. مجاهم لل IPv4 ناووع بنجت متيسف، عرتفلا هذه لالخن نيوكتم
ةقيدق 1 و 1440 ني ب عرتفلا.
- راطت نالا عرتف لالخن ةبولطملا ةلشافلا ةقداصملا تالواحم ددع وه <count> Threshold
1 و 100. ني ب لصاللا دحلا نيعت كنكمي. بنجت ليغشتل

بنجت متيسف، 20 يه ةبتعالو قئاقد 10 يه قيلعتلا عرتف تناك اذا، لاثملا ليبس يلع
قئاقد 10 دم يأ في عباتم ةقداصم لشف 20 كانه ناك اذا ايئاقلت IPv4 ناووع

 لمعتسي نإ. رابتعالا في NAT مادختسا عض، دحلاو قيلعتلا ميقي نيعت دنع: عظام الم نمضي اذهو. يلعأ عميقي عار، ناووع هسفن لال نم بلط ريثك حمسي يأ، برض تنأ في، لاثملا ليبس يلع. لاصتال لفاك تقوي لعل نيححيصلال نيمدختسملا لوصح. قريصق عرتف في لاصتالا ةلواحم نيمدختسملا نم ديدعلل نكمي، قندنفلا

 ن.آلا يتح ةمومدم ريغ SAML ربع ةقداصملا لشف تالاح: عظام الم

VPN ةكبشلة ةرفوتملا ةثالثل تاديدهتلا فاشتكا تامدخ يلاتلا نيوكتلا لاثم حيتي و
ليمعالا عدبل 20 غلبت ةبتعو قئاقد 10 غلبت فوقوت عرتف عم دعب نع لوصولاب ةصاخلا
ةئيبلال تابلطتملا اقفو دحلاو فاقيا إلالا ميقي نيوكتب مق. ةلشافلا ةقداصملا تالواحم و
كب ةصاخلا

عحاتملا ثالثل تازيمل نيكمتمل ادحاو FlexConfig نئاك لاثملا اذه مدختسي

```
threat-detection service invalid-vpn-access  
threat-detection service remote-access-client-initiations hold-down 10 threshold 20  
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

Add FlexConfig Object



Name:

enable-threat-detection-ravpn

Description:

Enable threat-detection for remote access VPN services

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment: Once ▾

Type: Append ▾

```
threat-detection service invalid-vpn-access  
threat-detection service remote-access-client-initiations hold-down 10 threshold 20  
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

▸ Variables

Cancel Save

4. FlexConfig نئىك ظرفح.

5. صاخال نامآل ةيماحل رادجل ةني عمل FlexConfig ةسايس ددحو FlexConfig > ةزهجال لىل لقتنا ك.

6. تمق يذل FlexConfig نئىك ددح، رسيال اعزل ي ةضورعمل ةحاتمل FlexConfig تانئىك نم. تاريغتلل ظرفحو، > قوف رقناو، 3 ةوطخلل ي ف هنيوكتب

The screenshot shows the Firewall Management Center interface. The main heading is "Flex-Config-vFTD1". Below it, there are tabs for "Overview", "Analysis", "Policies", "Devices", "Objects", and "Integration". The "Objects" tab is active. On the right side, there are buttons for "Deploy", "Migrate Config", "Preview Config", "Save", and "Cancel". A red notification says "You have unsaved changes".

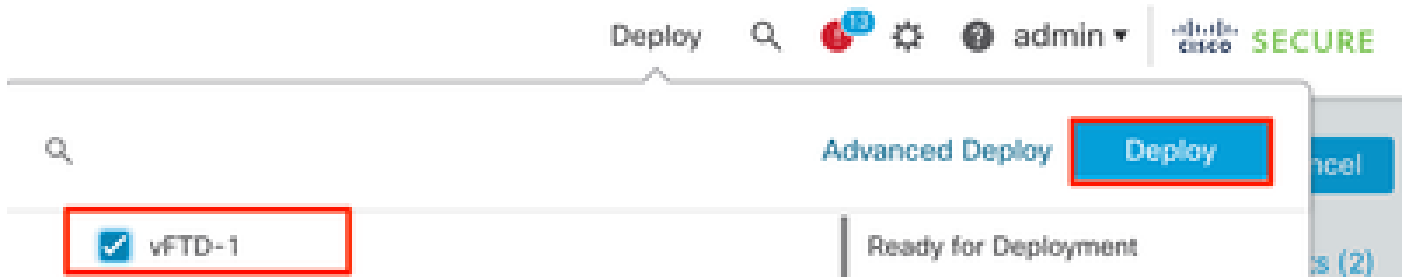
On the left, there is a search bar for "FlexConfig Object". Below it, there are two sections: "User Defined" and "System Defined". In the "User Defined" section, the object "enable-threat-detection-ravpn" is selected and highlighted with a red box and a red number "1".

In the "System Defined" section, the object "Default_DNS_Configure" is selected and highlighted with a red box and a red number "2".

On the right, there are two tables. The top table is "Selected Prepend FlexConfigs" and the bottom table is "Selected Append FlexConfigs". In the "Selected Append FlexConfigs" table, the object "enable-threat-detection-ravpn" is listed with the description "Enable threat-detection for remote access VPN services" and is highlighted with a red box and a red number "3".

At the top right of the main content area, there are buttons for "Save" (highlighted with a red box and a red number "4") and "Cancel".

7. ققحتال او تارييغتال رشن ب مق .



ةحصلال نم ققحتال

ىل ل وخذال ليجس تب مق ، تاديدهتال فشك ب ةصاخال WAPN تامدخل تايئاصح | ضرع لچأ نم
CLI ل وخذال ليجس تب مق و FTD ب صاخال CLI
و ليجس تب مق ب ن ل واصل و ادب و ادب ن ل واصل و ةقداصم : ةمدخلال نوكت نأ نكمي شيح
حل اص ريغ VPN ل واصل و

تامل عمل هذه ةفاضا قيرط ن ل واصل و ةقيرط نم دحلال كنكمي

- تاديدهتال فشك ةمدخلال نم طقف اهبقت متي يتال تالخال ضرع — تالخال
- ةقداصم تال واصل و تلش ف يتال IP نيوانع ، لثال ل ليجس تب مق
- ةمدخلال تالخال و ةمدخلال ليجس تب مق ل ضرع — ليجس تب مق

فاشك تامدخ عيجم تايئاصح | ضرع ل show threat-detection service رمأل ليجس تب مق
اهنكم مت يتال تاديدهتال

```
<#root>
```

```
ciscoftd# show threat-detection service
```

```
Service: invalid-vpn-access State : Enabled
```

```
Hold-down : 1 minutes
```

```
Threshold : 1
```

```
Stats:
```

```
failed : 0
```

```
blocking : 0
```

```
recording : 0
```

```
unsupported : 0
```

```
disabled : 0
```

```
Total entries: 0
```

```
Service: remote-access-authentication State : Enabled
```

```
Hold-down : 10 minutes
```

```
Threshold : 20
```

```
Stats:
```

```
failed : 0
```

```
blocking : 1
```

```
recording : 4
```

```
unsupported : 0
```

```
disabled : 0
```

Total entries: 2

Name: remote-access-client-initiations State : Enabled

Hold-down : 10 minutes

Threshold : 20

Stats:

failed : 0
blocking : 0
recording : 0
unsupported : 0
disabled : 0

Total entries: 0

قد اصم ةم دخل مهب قعت متي نيذال ني لم تحت حمل ني مجاهم لاي صافات نم ديزم ضرعل
قداصم ةم دخل مهب قعت متي نيذال ني لم تحت حمل ني مجاهم لاي صافات نم ديزم ضرعل
لوا show threat-detection service <service> entries. دع ب نع لوصول

ciscoftd# show threat-detection service remote-access-authentication entries

Service: remote-access-authentication

Total entries: 2

Idx	Source	Interface	Count	Age	Hold-down
1	192.168.100.101/ 32	outside	1	721	0
2	192.168.100.102/ 32	outside	2	486	114

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.

تاديدهتال نع فشكلل دع ب نع لوصول ةم دخل صاخلا لاي صافات لاول ةم اعلا تاءاصح لال ضرعل
تاديدهتال نع فشكلل دع ب نع لوصول ةم دخل صاخلا لاي صافات لاول ةم اعلا تاءاصح لال ضرعل
لوا show threat-detection service <service> details. دع ب نع لوصول VPN، لىل ةدحمل

ciscoftd# show threat-detection service remote-access-authentication details

Service: remote-access-authentication

State : Enabled

Hold-down : 10 minutes

Threshold : 20

Stats:


failed : 0
blocking : 1
recording : 4
unsupported : 0
disabled : 0

Total entries: 2

Idx	Source	Interface	Count	Age	Hold-down
1	192.168.100.101/ 32	outside	1	721	0
2	192.168.100.102/ 32	outside	2	486	114

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.

 فاشتكأ ةمدخ ةطساوب اهبقعت متي يتل IP نيوانع تالخدال ضرعت :ةظالم ددع دادزي ،اهبنتج بولطم لاطورش لى فوتسا دق IP ناوع ناك اذا .طقف تاديدهتال لخدك IP ناوع ضرع متي الورطحل

ناوع لصفر لازاؤ ،ةمدخ VPN بقبطي صفر تبقرار عي طتسي تنأ ،كلذ لىل ةفاضل ابو يلاتل رمأل عم IP ل ناوع لك وأ ديحو :

- [ip_address لهاجت ضرع]


ةطساوب ايئاقلت اهلهاجت متي لتلك لذ ي ف امب ،ةدع بمل ةفيضم ل تائي ببل رهظي ضرع ل ةقيرط ديدحت كنكمي .ماجلال رمأ مادختساب ايودي وأ ،VPN تامدخل ديدهتال فشك ددحم IP ناوع لىل ايراي تخا

- ip_address [interface if_name] لهاجت دجوي ال

نا ،ةنعلل ل مس ل نراق ل تنيع ايراي تخا عي طتسي تنأ .طقف ددحم ل IP ناوع ب نجت ةلازا لىل هناكم يف قشن ل كرتي نأ ديرت تنأ نراق دحاو نم رثكأ لىل تذب نوكي ناوع ل نراق صعب

- حضاو لهاجت

تاهجاو ل عي م جو IP نيوانع عي م جم نم زواجت ل ةلازا

 VPN تامدخل تاديدهتال فاشتكأ ةطساوب اهبنتج متي يتل IP نيوانع رهظت ال :ةظالم طقف تاديدهتال فاشتكأ حسم لىل قبطني يذلاو ،"show threat-detection" رمأل يف

تامدخب ةقلعت م ل ةحات م ل syslog لئاسرورم أ جرخا لكل لي صافات ل عي م ةعارق لجأ نم .[رمأولأ عجرم](#) دنتسم لىل عوجر ل اءجر ل ،دعب نع لوصول VPN ب ةصاخ ل تاديدهتال فاشتكأ

ةلص تاذا تامول عم

- مزلي .(TAC) ةي نقت ل ةدعاس م ل زكرم ب لاصتال اىجري ،ةي فاضا ةدعاس م لىل لوصحلل [Cisco](#) نم ةي م ل اءل مءدل ل لاصتال تاهج :حل اص معد دقع
- [إنه](#) Cisco VPN عم تجم ةرايز اضيأ كنكمي
- [Cisco](#) نم تاليزنت ل اوي نفل مءدل

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يصلأل يزلچنلإل دن تسمل