

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

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسألا تامولعم](#)

[نيوكتلا](#)

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

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

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

[ةحصللا نم ققحتلا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

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

ةيساسألا تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت ناب Cisco ي صوت:

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

تابلطتملا

نم نمآلا ةيامحل راج ديدهت دض عافدلا تارادصا ي ف هذه تاديدهتلا فاشتكلا تازيم معد متي
ةيلاتلا ةمئاقلا ي ةجرءملا Cisco:

- ديدهتلا هجو ىلع راطقلا اذه ي ف ثدحألا تارادصا او 7.0.6.3 ي ف موعدم -> 7.0 ةخسن راطق



متي 7.4 وأ 7.3 وأ 7.2 وأ 7.1 trains رادصا ي ف ايلاح ةموعدم ريغ تازيملا هذه: ةظحالم
اهرفوت درجمب دنتسملا اذه شيدهت

ةمدختسملا تانوكملا

ةغص ةيجمربو زاهج اذه ىلع ةقيثو اذه يف فصى ةمولعمل تسسأ

- Cisco 7.0.6.3 نم نمآلا ةيامل رادج ديدته دض عافدلل يرهظلا رادصلا

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضايرتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيجم تادب رملأال لمحتمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تكبش

ةيساسأ تامولعمل

(VPN) ةيرهظلا ةصاخلا ةكبشلا تامدخب ةصاخلا تاديدهتلا فاشتك تازيم كل حيتت ةيلائلا تاهويرانيسلا نم يادص ةيامل ةينكامل دعب نع لوصول

1. لاصتالا ةلواحم يادع نع لوصول VPN تامدخ ةيصالص اغلال لاصتالا تالواحم. طقف يلاخلال مادختسالل ةصصخمل تامدخالل
2. لىل دعب نع لوصول لاصتالا تالواحم ليغشتب مجاهمل موقى شيح، ليمعل ادب تامجه ال هنكلو دحاو فيضم نم ةرركتم تارم VPN ةكبش ةصاخلا ثبلاو لابقستالا ةدحو تالواحملا هذه لمكي
3. حسملا تامجه) VPN تامدخ لىل دعب نع لوصول ةرركتملا ةلشافلا ةقداصملا تالواحم. (ةوقلاب رورملا ةمكل/مدختسم مسال يئوولل

عنمو ةيباسح دراوم كالهتسا، لوصول ةلواحم يف اهلاشف دنع ىتح، تامجهلا هذه نكمي دعب نع لوصول VPN تامدخب لاصتالا نم نيقيقيقحلا نيمدختسمل

دودحل زواجتي يذلا (IP ناووع) فيضملا نمآلا ةيامل رادج بنجتي، تامدخال هذه نيكمت دنع ايودي IP ناووع ةوجف ةلازاب موقت ىتح تالواحملا نم ديزم عنمل، ايئاقلا اهنيوكت مت يتلا

 لكشب VPN لىل دعب نع لوصول تاديدهتلا فاشتك تامدخ عيجم ليطعت متي: ةظالم يضايرتفا

نيوكتلا

 "ةيامل رادج تاديدهت نم ةنمآلا ةيامل" لىل تازيملا هذه نيوكت معد متي ال: ةظالم FlexConfig ربع ال ايلا

1. نمآلا ةيامل رادج ةرادا زكرم لىل لوخدلا لچس.

2. FlexConfig > FlexConfig > تانئاللا ةرادا > تانئاللا لىل لقتنا، FlexConfig نئال نيوكتل. FlexConfig نئال ةفاضا 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]

3. تازيم نيكمتل بولطلم نيوكتلل فضا، FlexConfig نئاك ةفاضل ةذفان حتف درجم ب. دعب نع لوصولل VPN ةكبش ةصاخلل تاديدهتلل فاشتك:

- FlexConfig: enable-threat-detection-range نئاك مسا
- FlexConfig: نئاك فصو دعب نع لوصولل VPN تامدخل تاديدهتلل فاشتك نيكمت
- ةدحاو ةرم: رشنلل
- قاحلل: ةباتكلل
- ةحاتملا تازيملا لىل اذانتسا "تاديدهتلل فاشتك ةمدخ" رماو افضا: صنلل عبرم اقحال ةحصولل

✎ VPN ةكبش ل ةرفوتملا ثالثلل تاديدهتلل فاشتك تازيم نيكمت كنكمي: ةظحالم نئاك ءاشن كنكمي و، هسفن FlexConfig نئاك مادختساب دعب نع لوصولل ةصاخلل اهنيكمت متيل ةزيم لكل يدرف لكشب دحاو FlexConfig.

ريغ) ةيلخادل VPN تامدخ لاصتالال تالواحمل تاديدهتلل فاشتك: 1 ةزيملا طقف (ةحلصلال

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

دعب نع لوصولل VPN ةكبش ليمع ادب تامجهل تاديدهتلل فاشتك: 2 ةزيملا

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

- تالواحم باسح اهلالخ متي ادب ةلواحم رخا دعب ةرتفلل <minutes> تقوئملا فاقيلل ددحي متي تلل ةبتعلاب يف ةليلاتملا لاصتالال تالواحم ددع ناك اذا. ةليلاتملا لاصتالال نييغت كنكمي. مجاهملا لصال IPv4 ناونع بنجت متيسف، ةرتفلل هذه لخالل اهنيوكت ةقويق 1 و 1440 ني ب ةرتفلل هذه
- لىغشتل راطتالال ةرتفلل لخالل ةبولطلملا لاصتالال تالواحم ددع وه <count> Threshold ني ب لصالل دحلل نييغت كنكمي. بنجت 100 و 5

بنجت متيسف 20، هه ةبتعلال او قواق 10 هه قيلعتل ةرتفلل تناك اذا، لالملا لىبس لىل قواق 10 دم ي يف ةليلاتم لىصوت ةلواحم 20 كانه تناك اذا ايلاقلل IPv4 ناونع

 لمعتسي نإ. رابتعالا في NAT مادختسا عض، دحل او قيلعتلا ميقي نبيعت دنع: عظام الم نمضي اذهو. يلعأ عميقي عار، ناوونع هسفن لال نم بلط ريثك حمسي يأ، برض تنأ في، لاثم الم لبيس يلع. لاصتال لفاك تقوي لعل نيححيصل لال نيمدختسم الم لوصح. قريصق عرتف في لاصتالال ةلواحم نيمدختسم الم نم ديدعل ل نكمي، قندنف لال

دعب نع لوصول VPN ةقداصم لش فل تاديدهتلا فاشتكا: 3 ةزي الم

فاشتكا ةمدخل دعب نع لوصول دييقت رمأ فضا، ةمدخلال هذه نيكم تل ثيح، FlexConfig نئاك صن ع برم في <count> دحل <count> قديقتاديدهتلا

- تالاح باسح اهلالخ متي ةلشاف ةلواحم رخأ دعب عرتفال <minutes> تقوؤم الم فاقبي إلال ددحي يذلال دحل في فوتسي ةيلالتتم الم ةقداصم الم لشف تالاح ددع ناك اذو. ةيلالتتم الم لشف لال هذه نبيعت كنكمي. مجاهم لل IPv4 ناوونع بنجت متيسف، عرتفال هذه لالخن نيوكت مت راطت نالال عرتف لالخبولط الم ةلشاف لال ةقداصم الم تالواحم ددع وه <count> Threshold 100 و 1 نيبل لصالفال دحل نبيعت كنكمي. بنجت ليغشتل

بنجت متيسف، 20 يه ةبتعالو قئاق د 10 يه قيلعتلا عرتف تناك اذو، لاثم الم لبيس يلع قئاق د 10 دم يأ في عباتتم ةقداصم لشف 20 كانه ناك اذو ايئاق لت IPv4 ناوونع

 لمعتسي نإ. رابتعالا في NAT مادختسا عض، دحل او قيلعتلا ميقي نبيعت دنع: عظام الم نمضي اذهو. يلعأ عميقي عار، ناوونع هسفن لال نم بلط ريثك حمسي يأ، برض تنأ في، لاثم الم لبيس يلع. لاصتال لفاك تقوي لعل نيححيصل لال نيمدختسم الم لوصح. قريصق عرتف في لاصتالال ةلواحم نيمدختسم الم نم ديدعل ل نكمي، قندنف لال

 ن. آلا يتح ةم و عدم ريغ SAML ربع ةقداصم الم لشف تالاح: عظام الم

VPN ةكبشل ةرفوت الم ةثالثل تاديدهتلا فاشتكا تامدخ يلاتل نبيوكتل لاثم حي تي و لي م ال ادبل 20 غلبت ةبتعو قئاق د 10 غلبت فوقوت عرتف عم دعب نع لوصول اب ةصاخال ةئيبلال تابلطتم لاقفو دحل او فاقبي إلال ميقي نيوكتب مق. ةلشاف لال ةقداصم الم تالواحم و ك ب ةصاخال

عحات الم ثالثل تازي الم نيكم تل ادحو FlexConfig نئاك لاثم الم 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.

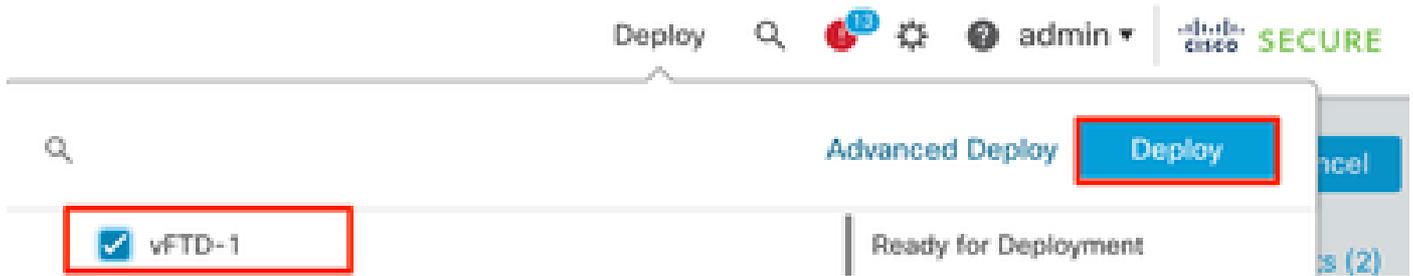
5. صاخال نامآل ةيماحل رادجل ةني عمل FlexConfig ةسايس ددحو FlexConfig > ةزهجال لىل لقتنا ك.

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

The screenshot shows the Firewall Management Center interface. The main title is "Flex-Config-vFTD1". The interface is divided into several sections:

- Available FlexConfig:** A list of FlexConfig objects. The "enable-threat-detection-ravpn" object is highlighted with a red box and labeled with a red "1".
- Selected Prepend FlexConfigs:** An empty table with columns for #, Name, and Description.
- Selected Append FlexConfigs:** A table with one row: # 1, Name "enable-threat-detection-ravpn", and Description "Enable threat-detection for remote access VPN services". This row is highlighted with a red box and labeled with a red "3".
- Buttons:** At the top right, there are buttons for "Migrate Config", "Preview Config", "Save", and "Cancel". The "Save" button is highlighted with a red box and labeled with a red "4".

7. ققحتال او تاريغتلال رشن ب مق .



ةحصلال نم ققحتال

ىل ل وخذال ليجس تب مق ، تاديدهتلال فشك ب ةصاخال WAPN تامدخل تايئاصح | ضرع لچأ نم
CLI صاخال FT D مقو ب show threat-detection service [service] [entries|details].
أ ليمعلا لىل دعب نع لوصولا ادب وأ دعب نع لوصولا ةقداصم : ةمدخلال نوكت نأ نكمي شيح
حلصا ريغ VPN لىل لوصولا

تاملعملال هذه ةفاضا قيرط نع ضرعلا ةقيرط نم دحلال كنكمي

- تاديدهتلال فشك ةمدخلال نم طقف اهبقت متي يتال تالخالال ضرع — تالخالال
ةقداصم التواجم تلشف يتال IP نيوانع ، لاثملا لىبس لىل
- ةمدخلال تالخالال ةمدخلال لىصافت نم لك ضرع — لىصافتال

فاشك تامدخ عيمج تايئاصح | ضرع show threat-detection service رمأل لىغش تب مق
اهنكمتم يتال تاديدهتلال .

```
<#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.

فأشركنا ممدخة طساوب اهبقت متي يتل IP نيوانع تالخدال ضرعت: عظمالم
دع دادزي، اهبنت بولطم ل طورشلل ي فوتسا دق IP ناوع ناك اذا. طقف تاديدهتال
لخدك IP ناوع ضرع متي الورطحل.

ناوع ل ضرر لازا، ممدخ VPN ب قبطي ضرر تبقرار عي طتسي تنأ، كلذلى لى فاضل ابو
ي: لالتل رمأل عم IP ل ناوع لك وأ ديحو:

- [ip_address] لهاجت ضرع]

ةطساوب ايئاقلت اهلهاجت متي يتل كلت كلذبي فامب، ةدع بملة فيضم ل تائي ببل رهظي
ضرع لة قيرط ديحت كنكمي. ماجحل رمأ مادختساب ايودي وأ، VPN تامدخل ديدهتال فشك
ددم IP ناوع لى ل اي راي تخا.

- ip_address [interface if_name] لهاجت دجوي ال

نا، ةنعلل ل مس ل نراق ل تنيع اي راي تخا عي طتسي تنأ. طقف ددم ل IP ناوع ب نجت ةلازا
لىل هناكم في قشن ل كرتي نأ ديرت تنأ نراق دحاو نم رثكأ لىل تذب نوكي ناوع ل
نراق ضرع ب.

- حضاو لهاجت

تاهجاول عي ممو IP نيوانع عي ممو نم زواجت لةلازا.

VPN تامدخل تاديدهتال فاشتك اةطساوب اهبنت متي يتل IP نيوانع رهظت ال: عظمالم
طقف تاديدهتال فاشتك ا حسم لىل قبطني يذلاو، "show threat-detection" رمأل في.

تامدخب ةقلعت ملة حاتم ل syslog لئاسرورم أ جرخا لكل لىل صافات ل عي ممو ةعارق لجا نم
رمأولأ عجرم. دنتسم لىل عوجر ل اءجرل، دعب نع لوصول VPN ب ةصاخ ل تاديدهتال فاشتك

ةلص تاذا تامول عم

- مزلي (TAC) ةي نقت لة دعاسم ل زكرم ب لاصتال اىجري، ةي فاضل ا دعاسم لىل لوصحلل
Cisco. نم ةي مل اعل ا مع دل ل لاصتال اءج: ج لاص م عدد قع
- [إنه](#) Cisco VPN عم تجم ةرايز اضي أ كنكمي
- [Cisco نم تاليزنت ل اوى نفل ا مع دل ا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل