

عقوم ىلا عقوم نم VPN ۆلەم لىطعت FTD مادختساب FlexConfig

تايىوت حملا

ةمدقمل

[ةيىس اس ألا تابل طتملا](#)

[تابل طتملا](#)

[ةمدختسملا تانوكمل](#)

[ةيىس اس أتامولعم](#)

[نېوكتلا](#)

[نېاكو و FlexConfig ئاسىس نېوكت](#)

[قحصلا نم ققحتلا](#)

[اهالص او عاطخ ألا فاشكتسا](#)

[ةلص تاذ تامولعم](#)

ةمدقمل

مادختساب VPN ۆكبس شب ۆصالخا ئيفيك دنتسمل اذه فصي نع قفنلا فقوت تقو عنم لجأ نم FirePOWER (FMC) ئارادا زكرم يف تاسىس لومخلا ۆلەم عاهتنا وأ طاشنلا مدع ببسب لمعلا.

ةيىس اس ألا تابل طتملا

تابل طتملا

ةيلاتلا عيضاوملا ئافرۇم كىدل نوكت نأب Cisco يصوت:

- Firepower Threat Defense (FTD)
- FMC
- FlexConfig تاسىس
- عقوم ىلا عقوم نم (VPN) ئيرهاظلا ۆصالخا تاكبىشلا تاططخم

ةمدختسملا تانوكمل

ةيلاتلا جماربلا تارادصىلى دنتسمل اذه يف ۆدراولى تامولعملا دنتسست:

- FMCv - 6.5.0.4 (يىنب 57)
- FTDv - 6.4.0.10 (يىنب 95)

ۆصالخ ئىلمۇم ئىيپ يف ۆدوچوملا ۆزەج ألا نم دنتسمل اذه يف ۆدراولى تامولعملا عاشنامت تناك اذى. (يىضارتفا) حوسىم نېوكتب دنتسمل اذه يف ۆمدختسملا ۆزەج ألا عىمچ تأدب رمأ يأ لىمتحىملا رىيڭتلىل كەھف نم دكأتف، لىيغشتلا دىق كىتكېش.

ةيـسـاسـاـتـامـولـعـم

نم 1 رادص إلـا نـم لـكـل بـلـطـلـا يـلـع عـانـب عـقـوم يـلـا عـقـوم يـف ةـدـوـجـوـمـلـا VPN تـاكـبـش عـاشـنـا مـتـي
يـلـع مـئـاـقـلـا (IKEv2) يـلـدـابـتـلـا تـنـرـتـنـإـلـا حـاتـفـمـ نـم 2 رـادـصـإـلـاو (IKEv1) تـنـرـتـنـإـلـا حـاتـفـمـ
يـأـ كـانـهـ نـكـيـ مـلـ اـذـا FTD يـهـنـيـ، يـضـارـتـفـاـ لـكـشـبـ. (رـيـفـشـتـلـا ةـطـيـرـخـ) ةـسـاـيـسـلـاـ
يـضـارـتـفـاـ لـكـشـبـ ةـقـيـقـدـ 30 يـلـا تـقـفـمـلـا نـيـيـعـتـ.

نيـوـكـتـلـا

FlexConfig ةـسـاـيـسـ نـيـوـكـتـ FlexConfig

اهـدـحـأـ نـكـيـ مـلـ اـذـا) ةـدـيـدـجـ FlexConfig ةـسـاـيـسـ عـاشـنـاـبـ مـقـ <ـةـمـجـأـلـاـ تـحـتـ 1ـ ةـوـطـخـلـاـ
عـقـومـ يـلـاـ عـقـومـ نـمـ VPN ةـكـبـشـ نـيـوـكـتـ مـتـيـ ثـيـحـ FTD بـ اـهـقـافـرـاـوـ (لـعـفـلـاـبـ اـدـوـجـوـمـ

Cisco Firepower Management

https://10.31.124.31:6005/ddd/#Flex

Getting Started New Tab BEMS Identity Services Engine Next Generation Web ... Other Bookmarks

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings **FlexConfig** Certificates

New Policy

FlexConfig Policy	Status	Last Modified
-------------------	--------	---------------

New Policy

Name: **FlexConfig_FTD_B**

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

FTDv_B FTDv_C

Selected Devices

FTDv_B

Add to Policy

Save Cancel

Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.117

How To

CISCO

و

The screenshot shows the Cisco Firepower Management web interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices (highlighted with a red box), Objects, AMP, Intelligence, Deploy, System, Help, and admin. Below the navigation is a sub-menu with tabs for Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig (highlighted with a red box), and Certificates. A 'New Policy' button is visible. The main content area displays a table for 'FlexConfig Policy'. The first row shows 'FlexConfig_FTD_B' with a status of 'Up-to-date on all targeted devices' and last modified on '2021-06-15 17:21:38' by 'admin'. Action icons for edit and delete are shown to the right of the row.

يلى امك FlexConfig نئاك ئاشناب مق جىنلا اذه لخاد 2. ۋە طەخلى:

مسالا: S2S_Idle_TimeOut
ۋەرمىكىيە: رشنىلى
قاچلى: ئېباتكىلى

تامس Group-Policy .DefaultS2SGgroupPolicy
VPN-idle-timeout none

The screenshot shows the 'FlexConfig Policy Editor' for the policy 'FlexConfig_FTD_B'. The top navigation bar and sub-menu are identical to the previous screenshot. The main area is titled 'FlexConfig_FTD_B' and contains a 'Preview Config' and 'Save' button. Below this is a 'Policy Assignments (1)' section. The interface features two main panels: 'Available FlexConfig Object' (left) and 'Selected FlexConfig' (right). The 'Available FlexConfig Object' panel shows a tree view of 'User Defined' and 'System Defined' objects, with a 'FlexConfig Object' button highlighted with a red box. The 'Selected FlexConfig' panel is divided into 'Selected Prepend FlexConfigs' and 'Selected Append FlexConfigs', both of which are currently empty.

The screenshot shows the Cisco Firepower Management interface with the 'Devices' tab selected. A new FlexConfig Object is being created with the name 'S2S_Idle_TimeOut'. The configuration text entered is:

```
group-policy .Defaults2SGroupPolicy attributes
vpn-idle-timeout none
```

The 'Deployment' dropdown is set to 'Everytime' and the 'Type' dropdown is set to 'Append'. The 'Save' button at the bottom right is highlighted with a red box.

و ظفح.

< رزلاب نميألا عزجلالا يلإ بحسأو منع ثجبا رسيلألا عزجلالا يف 3. ۋەطخىل.

Cisco Firepower Management +

Getting Started New Tab BEMS Identity Services Engine Next Generation Web ... Regex Tester and Deb... Mi vacuna Other Bookmarks

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

You have unsaved changes Preview Config Save Cancel

FlexConfig_FTD_B

Enter Description

Policy Assignments (1)

Available FlexConfig FlexConfig Object

- User Defined
 - aaa-server-map
 - disable-am
 - EEM_script_PeriodicLogOffAnyconnect
 - LDAP
 - ldap-attribute-map
 - Management-access
 - management-access-agarciam
 - NAT-T-Disable
 - S2S_idle_timeout
 - test
 - VPN-filter
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure

Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description

Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.117

How To

CISCO

The screenshot shows the Cisco Firepower Management interface for editing FlexConfig policies. In the 'Available FlexConfig' list, the 'S2S_idle_timeout' entry under 'User Defined' is highlighted with a red box. A red arrow points from this highlighted item to the right-side 'Selected Prepend FlexConfigs' table, indicating it has been selected for prepend. The 'Selected Append FlexConfigs' table is currently empty.

The screenshot shows the Cisco Firepower Management interface with the 'FlexConfig' tab selected. In the 'Selected Append FlexConfigs' section, the entry 'S2S_idle_timeout' is highlighted with a red box. The top right of the screen has a red box around the 'Save' button, which is labeled 'Save' with a blue icon.

Available FlexConfig

- User Defined
 - aaa-server-map
 - disable-am
 - EEM_script_PeriodicLogOffAnyconnect
 - LDAP
 - ldap-attribute-map
 - Management-access
 - management-access-agarciam
 - NAT-T-Disable
 - S2S_idle_timeout
 - test
 - VPN-filter
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure

Selected Prepend FlexConfigs

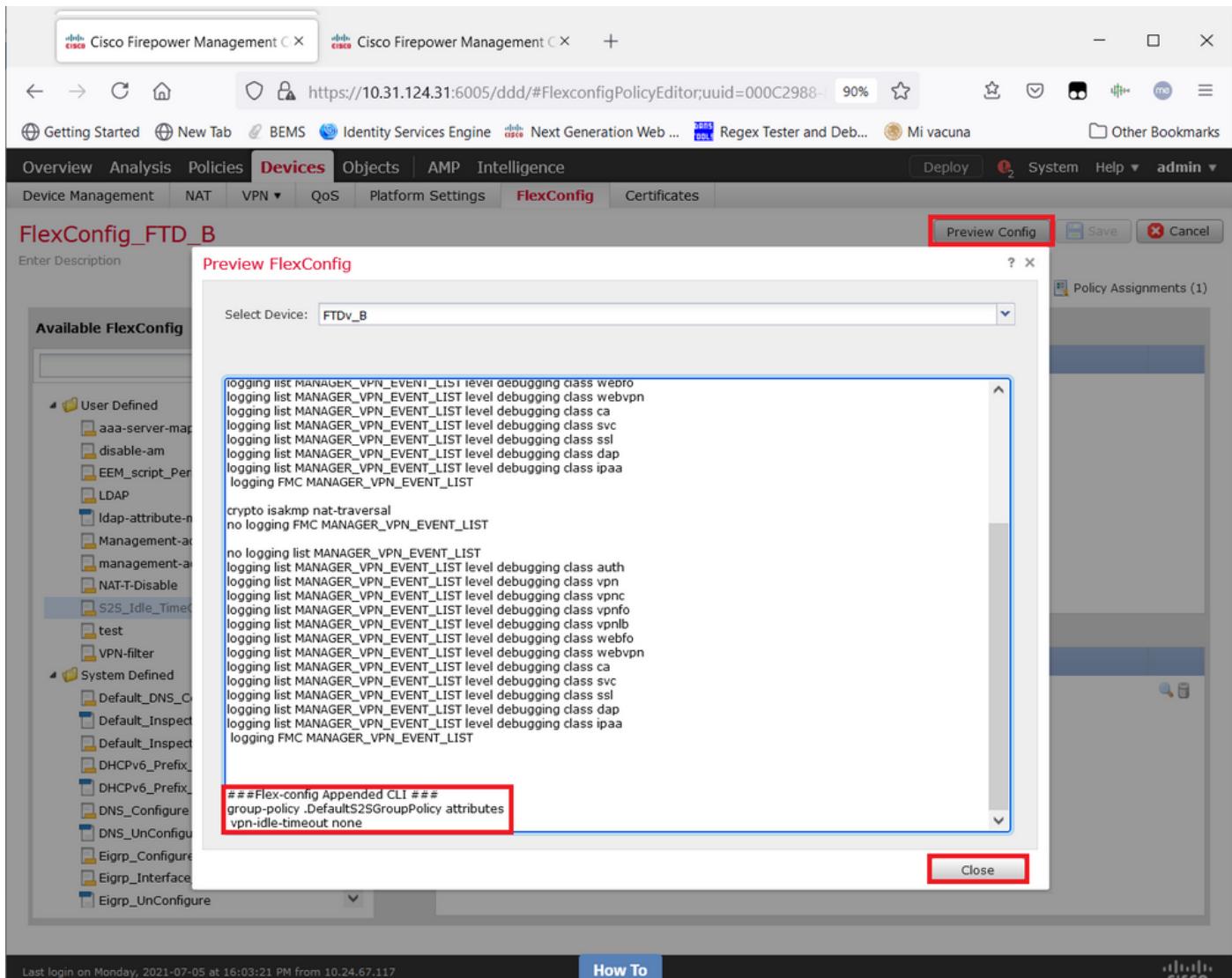
#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	S2S_idle_timeout	

رشنل او تارييغتل ا ظف赫.

ةندياعم رايتخا كنكمي ،نيوكتلا تارييغت ظفح دعب ،ةطيسو ووطخك (يرايتخا) 3.1 وةوطخل نيوكتلا ئيان يف عفدلل ۋەزەج رماوا نامضل نيوكتلا.



ةحصـلـا نـم قـقـحـتـلـا

يـف رـمـأـلـا اـذـهـ لـيـغـشـتـ كـنـكـمـيـ، رـشـنـلـا لـامـتـكـا درـجـمـبـ: دـيـدـجـلـا نـيـوـكـتـلـا دـوـجـوـ دـيـكـأـتـلـا:

```
firepower# show running-config group-policy .DefaultS2SGroupPolicy
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout none <<<-----
<committed output>
```

ةـصـاخـلـا (VPN) ةـيرـهـاظـلـا ةـصـاخـلـا تـاـكـبـشـلـا عـيـمـجـىـلـعـ رـثـؤـيـ رـيـيـغـتـلـا اـذـهـ نـأـ رـكـذـتـ: رـيـذـتـ

يـمـومـعـ دـادـعـا لـبـ قـفـنـ لـكـلـ دـادـعـا سـيـلـ هـنـاـ (S2S) لـوـحـمـلـابـ ةـصـاخـلـا (FTD).

ريـفـشـتـ حـسـمـ) دـادـتـرـالـا ىـلـا جـاتـحـيـ طـشـنـلـا قـفـنـلـا نـأـ الـاـ، دـوـجـوـمـ نـيـوـكـتـلـا نـأـ نـمـ مـغـرـلـا ىـلـعـ

عاـشـنـا دـنـعـ لـوـعـفـمـلـا يـرـاسـ رـيـيـغـتـلـا حـبـصـيـ يـلـاتـلـابـ وـ(<remote_peer_ip_address>) رـيـظـنـ

رـمـأـلـا اـذـهـ مـاـدـخـتـسـاـبـ لـوـعـفـمـلـا يـرـاسـ رـيـيـغـتـلـا نـأـ دـيـكـأـتـ كـنـكـمـيـ. يـرـخـأـ ۆـرمـ قـفـنـلـا:

```
firepower# show vpn-sessiondb detail 121 filter ipaddress
```

Session Type: LAN-to-LAN Detailed

```

Connection : X.X.X.X
Index : 7 IP Addr : X.X.X.X
Protocol : IKEv1 IPsec
Encryption : IKEv1: (1)AES256 IPsec: (1)AES256
Hashing : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 400 Bytes Rx : 400
Login Time : 22:06:56 UTC Tue Jun 15 2021
Duration : 0h:18m:00s
Tunnel Zone : 0

IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
Tunnel ID : 7.1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Main Auth Mode : preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 85319 Seconds
D/H Group : 5
Filter Name :

IPsec:
Tunnel ID : 7.2
Local Addr : A.A.A.A/255.255.255.255/0/0
Remote Addr : B.B.B.B/255.255.255.128/0/0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 27719 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes <<<<<<
Bytes Tx : 400 Bytes Rx : 400
Pkts Tx : 4 Pkts Rx : 4

```

نأ بجي و ٖقٖيٖقد 30 نم الدب قٖاقد 0 ىلٖع لومخلٖا عضوٖيٖف ٖلهملا عاهتنٖا دادع نٖيٖيعٖت بجي ٖوقوف لمعٖت يٖتلٖا تانٖايٖبٖلٖا رورم ٖكٖرٖح/طاشنٖلٖا نع رظنٖنٖلٖا ضغٖب ٖقطشٖنٖ ٖكٖبٖش لظٖت

دادع إلٖا اذه ليٖدعت ىلٖع ٖردقلٖا جمدلٖا نٖيٖسحت أطخ دجوي، ٖباتكلٖا تقوٖيف: **ٖظحٖالٖم**
Cisco نم ٖاطخٖالٖا حٖيٖحصٖت فرعٖم عجٖار FlexConfig. ىلٖا ٖظحٖالٖا نود FMC ىلٖع ٖرشٖابٖم
[CSCvr82274](#) - ENH: لـعجـأ VPN-idle-timeout

اهحالصٖ او ٖاطخٖالٖا فاشكتسٖا

اهحالصٖ او ٖاطخٖالٖا فاشكتسٖا الـ ددمـ تـامـولـعـم ايـلـاحـ دـجـوتـ الـ.

ٖلـصـ تـاذـ تـامـولـعـم

- نـعـ عـافـدلـلـ FlexConfig تـاسـايـسـ: لـصـفـلـا ـ 7.0ـ رـادـصـالـا ـFirepowerـ نـيـوـكـتـ لـيـلـدـ
- عـقـومـ ىـلـاـ عـقـومـ نـمـ VPNـ تـاكـبـشـ: لـصـفـلـا ـ 7.0ـ رـادـصـالـا ـFirepowerـ نـيـوـكـتـ لـيـلـدـ
- ـ دـيـدـهـ FirePOWER
- ـ دـيـدـهـ Firepower
- ـ تـادـنـتـسـمـلـاوـيـنـقـتـلـاـ مـعـدـلـاـ Cisco Systems

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).