

# 使用FlexConfig策略禁用FTD站點到站點VPN空閒超時

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[配置FlexConfig策略和FlexConfig對象](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本檔案介紹如何在Cisco Firepower管理中心(FMC)中修改使用FlexConfig策略的VPN的vpn-idle-timeout屬性，以防止由於不活動或空閒超時而導致通道停機。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Firepower Threat Defense (FTD)
- FMC
- FlexConfig策略
- 站點到站點VPN拓撲

### 採用元件

本檔案中的資訊是根據以下軟體版本：

- FMCv - 6.5.0.4 ( 內部版本57 )
- FTDv - 6.4.0.10 ( 內部版本95 )

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

Internet金鑰交換版本1(IKEv1)和Internet金鑰交換版本2(IKEv2)基於策略 ( 加密對映 ) 的站點到站點VPN都是按需隧道。預設情況下，如果在稱為vpn-idle-timeout的某一時間段內通道上沒有通訊活動，則FTD會終止VPN連線。預設情況下，此計時器設定為30分鐘。

## 設定

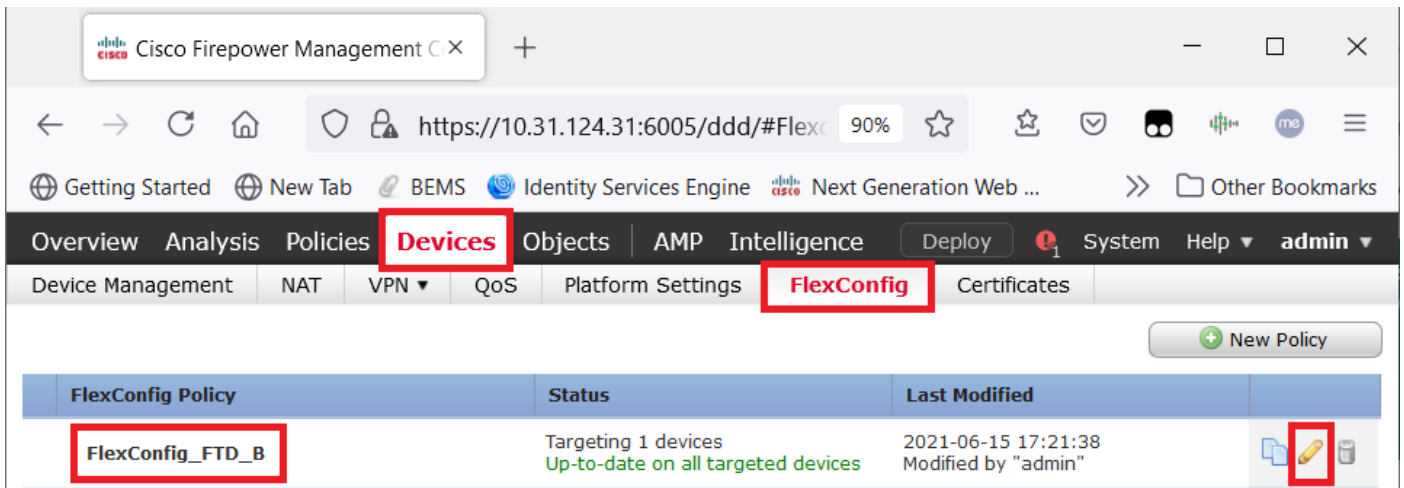
### 配置FlexConfig策略和FlexConfig對象

步驟1。在Devices > FlexConfig下，建立一個新的FlexConfig策略 ( 如果尚不存在 )，並將其連線到已設定點對點VPN的FTD。

The screenshot shows the Cisco Firepower Management Center interface. The browser address bar displays `https://10.31.124.31:6005/ddd/#FlexConfig`. The navigation menu includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', 'System', 'Help', and 'admin'. The 'Devices' tab is active, and the 'FlexConfig' sub-tab is selected. A 'New Policy' button is highlighted in the top right. The 'New Policy' dialog box is open, showing the following details:

- Name:** FlexConfig\_FTD\_B
- Description:** (empty)
- Targeted Devices:**
  - Available Devices:** FTDv\_B (selected), FTDv\_C
  - Selected Devices:** FTDv B
  - Add to Policy** button
- Buttons:** Save, Cancel

或



步驟2.在該策略內建立一個FlexConfig對象，如下所示：

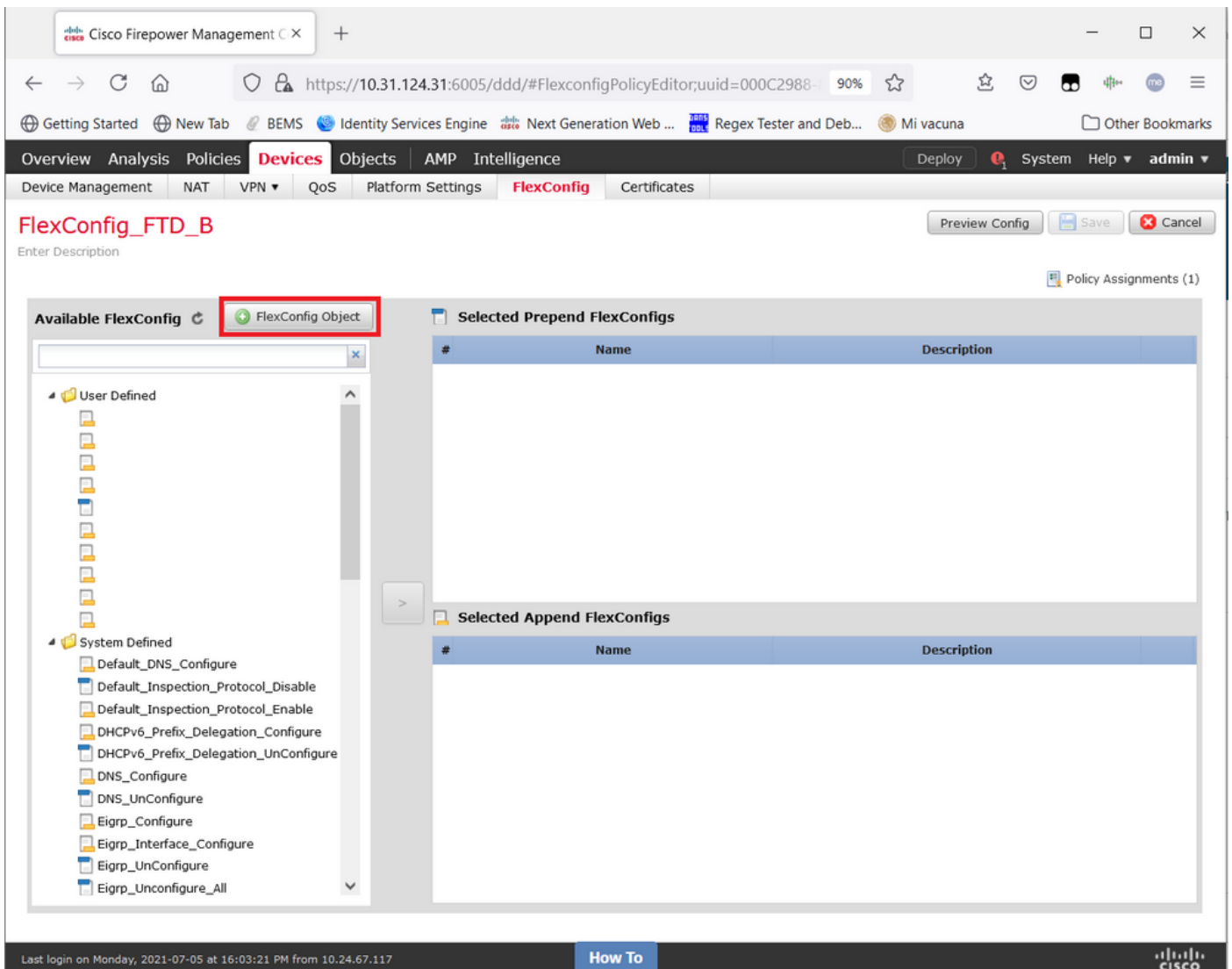
名稱:S2S\_Idle\_TimeOut

部署:每次

Type:附加

*group-policy .DefaultS2SGroupPolicy屬性*

*vpn-idle-timeout none*



The screenshot shows the Cisco Firepower Management console with the 'Add FlexConfig Object' dialog open. The dialog contains the following elements:

- Name:** S2S\_Idle\_TimeOut
- Description:** (Empty text area)
- Code Editor:** Contains the text `group-policy .DefaultS2SGroupPolicy attributes vpn-idle-timeout none`.
- Deployment:** Dropdown menu set to 'Everytime'.
- Type:** Dropdown menu set to 'Append'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

A yellow warning banner above the code editor states: "Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment."

並儲存它。

步驟3.在左窗格中搜尋並拖至右窗格，並顯示>。

Cisco Firepower Management C X

https://10.31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C2988- 90%

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

### FlexConfig\_FTD\_B

Enter Description

You have unsaved changes Preview Config Save Cancel

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



FlexConfig\_FTD\_B

Available FlexConfig

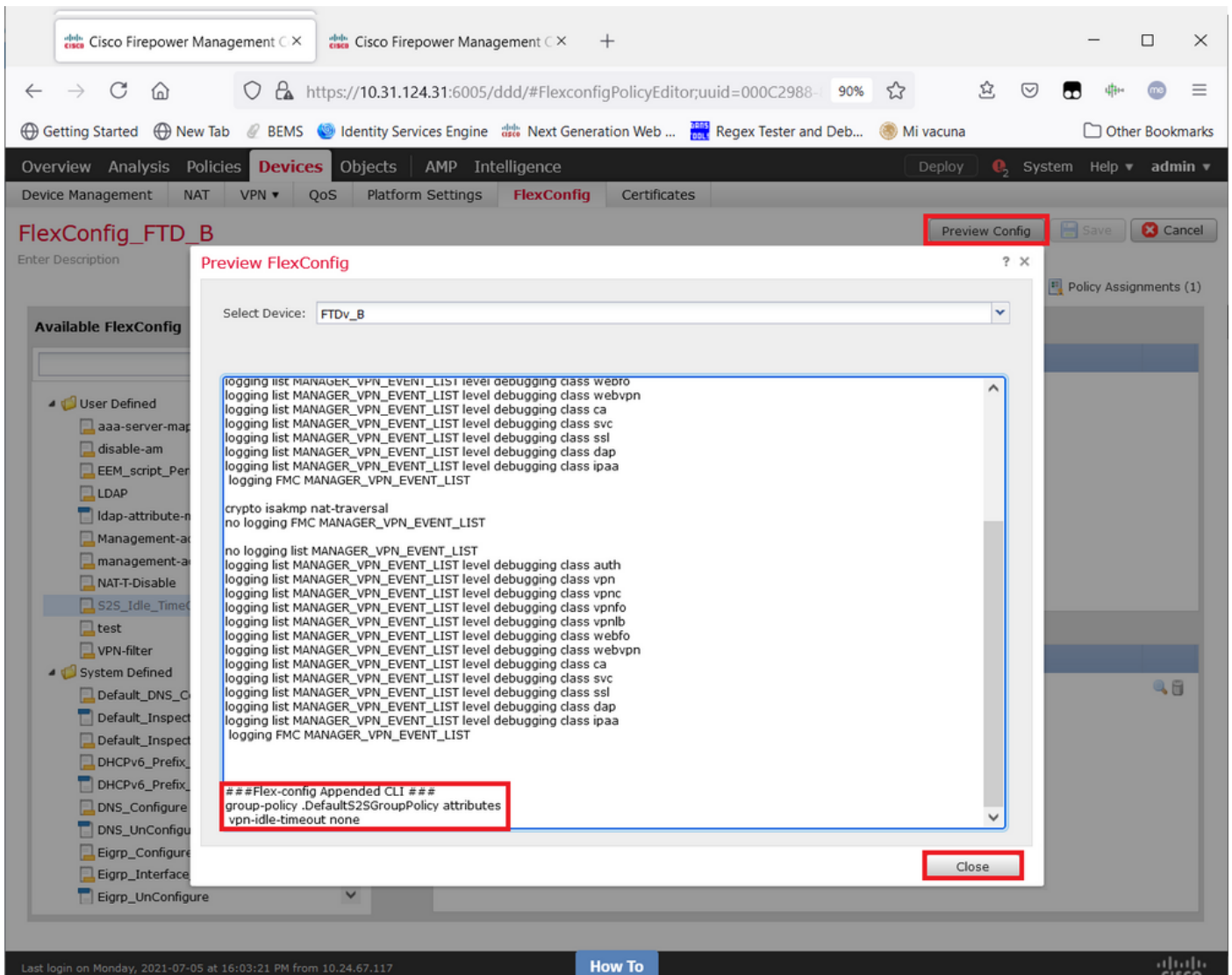
- User Defined
  - aaa-server-map
  - disable-am
  - EEM\_script\_PeriodicLogOffAnyconnect
  - LDAP
  - ldap-attribute-map
  - Management-access
  - management-access-agarciam
  - NAT-T-Disable
  - S2S\_idle\_timeout
  - test
  - VPN-filter
- System Defined
  - Default\_DNS\_Configure
  - Default\_Inspection\_Protocol\_Disable
  - Default\_Inspection\_Protocol\_Enable
  - DHCPv6\_Prefix\_Delegation\_Configure
  - DHCPv6\_Prefix\_Delegation\_UnConfigure
  - DNS\_Configure
  - DNS\_UnConfigure
  - Eigrp\_Configure
  - Eigrp\_Interface\_Configure
  - Eigrp\_UnConfigure

Selected Append FlexConfigs

#	Name	Description
1	S2S_idle_timeout	

儲存變更並進行部署。

第3.1步（可選）作為中間步驟，在儲存配置更改後，可以選擇Preview Config，以確保在配置結束時可以推送FlexConfig命令。



## 驗證

部署完成後，您可以在LINA(>系統支援diagnostic-cli)中運行此命令，以確認新的組態是否存在：

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

**注意：**請記住，此變更會影響FTD上的所有S2S VPN。這不是每個通道的設定，而是全域性設定。

即使存在配置，活動隧道也需要被退回(`clear crypto ipsec sa peer<Remote_Peer_IP_Address>`)，因此更改將在再次建立隧道時生效。您可以使用此命令確認更改生效：

```
firepower# show vpn-sessiondb detail l2l 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

空閒超時計數器必須設定為0分鐘而不是30分鐘，並且VPN必須保持活動狀態，而不管其上運行的活動/流量。

附註：在撰寫本文時，存在一個增強型錯誤，用於整合直接在FMC上修改此設定而不需要Flexconfig的功能。請參閱思科錯誤ID [CSCvr8274](#) — 增強型：配置vpn-idle-timeout

## 疑難排解

目前沒有特定資訊可用於故障排除。

## 相關資訊

- [Firepower管理中心配置指南7.0版 — 章節：適用於Firepower威脅防禦的FlexConfig策略](#)
- [Firepower管理中心配置指南7.0版 — 章節：適用於Firepower威脅防禦的站點到站點VPN](#)
- [技術支援與文件 - Cisco Systems](#)