Disable FTD Site-to-Site VPN Idle Timeout with FlexConfig Policies

Contents

Introduction

This document describes how to modify the **vpn-idle-timeout** attribute of a VPN with FlexConfig Policies in Cisco Firepower Management Center (FMC) in order to prevent tunnel downtime due to Inactivity or Idle Timeout.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Threat Defense (FTD)
- FMC
- FlexConfig Policies
- Site-to-Site VPN topologies

Components Used

The information in this document is based on these software versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

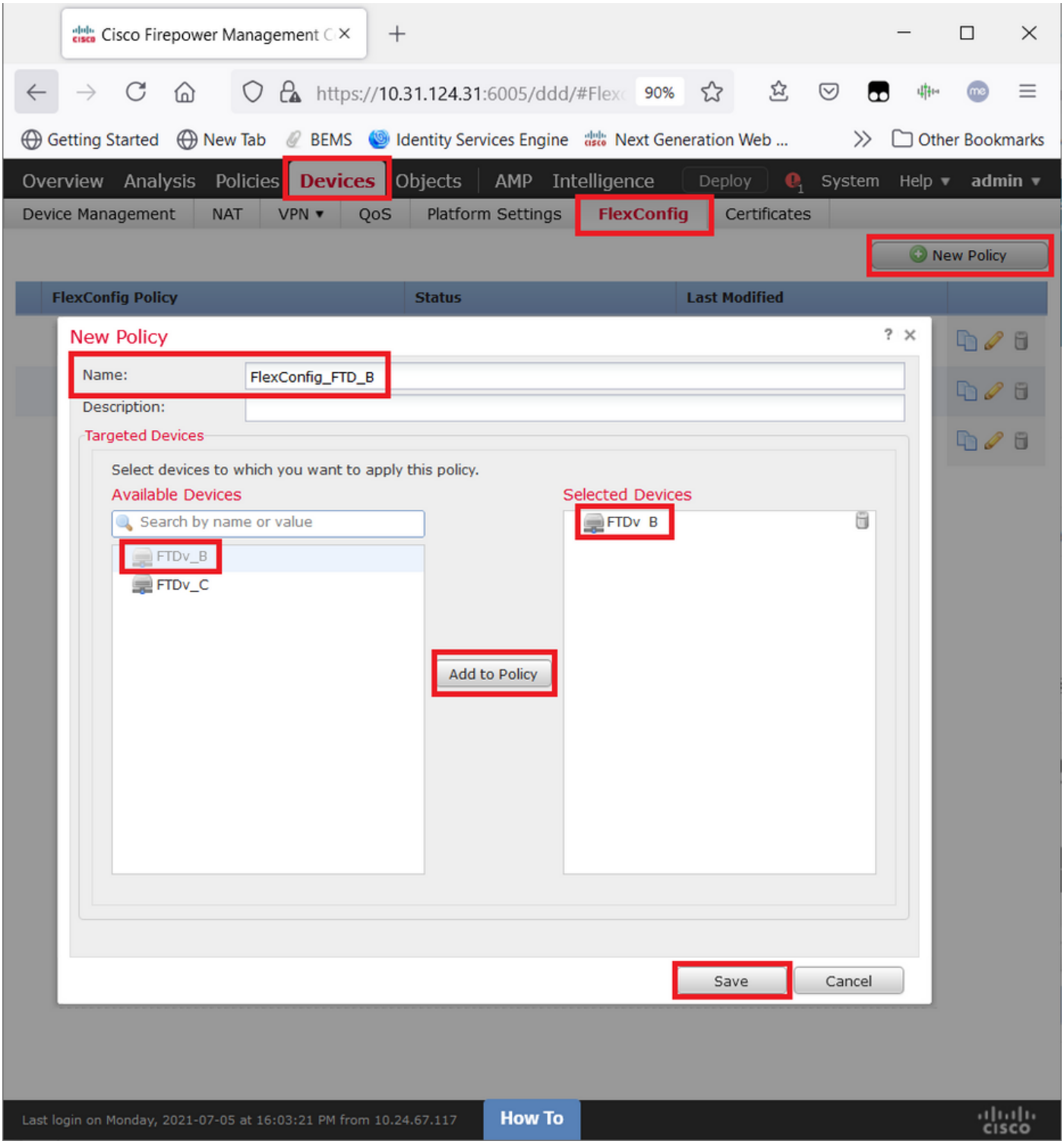
Background Information

Both Internet Key Exchange version 1 (IKEv1) and Internet Key Exchange version 2 (IKEv2) Policy Based (Crypto map) Site-to-Site VPNs are on-demand tunnels. By default, the FTD terminates the VPN connection if there is no communication activity over the tunnel in a certain period of time called **vpn-idle-timeout**. This timer is set to 30 minutes by default.

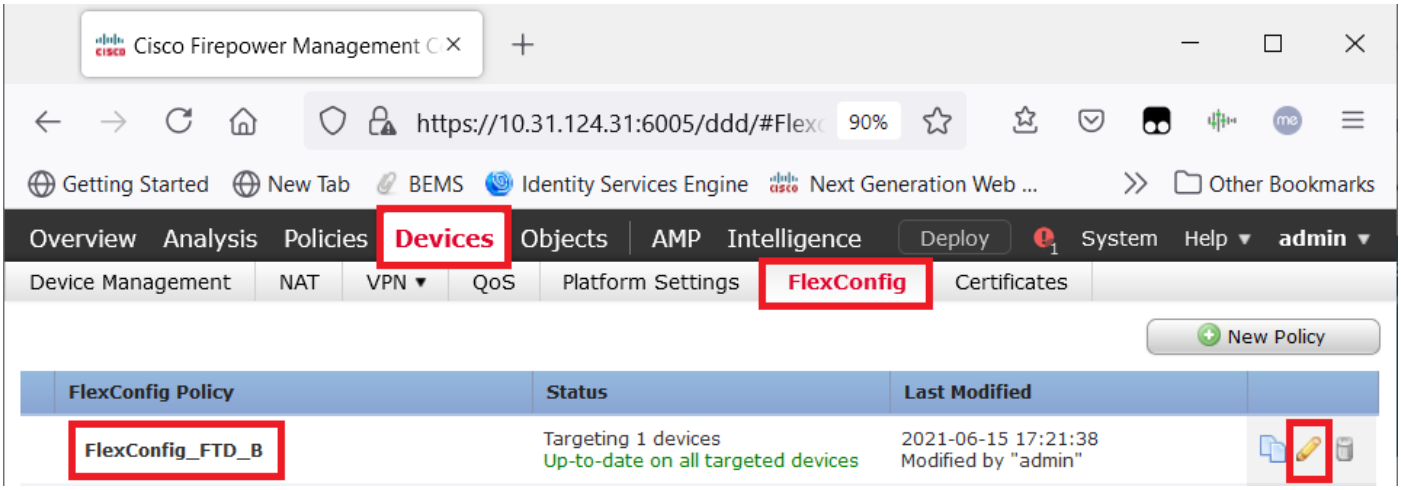
Configure

Configure FlexConfig Policy and FlexConfig Object

Step 1. Under **Devices > FlexConfig** create a new FlexConfig Policy (if one does not already exist) and attach it to the FTD where the Site-to-Site VPN is configured.


Cisco Firepower Management C
https://10.31.124.31:6005/ddd/#Flex
90%
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
Add to Policy
Selected Devices
FTDv_B
Save
Cancel
Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.117
How To

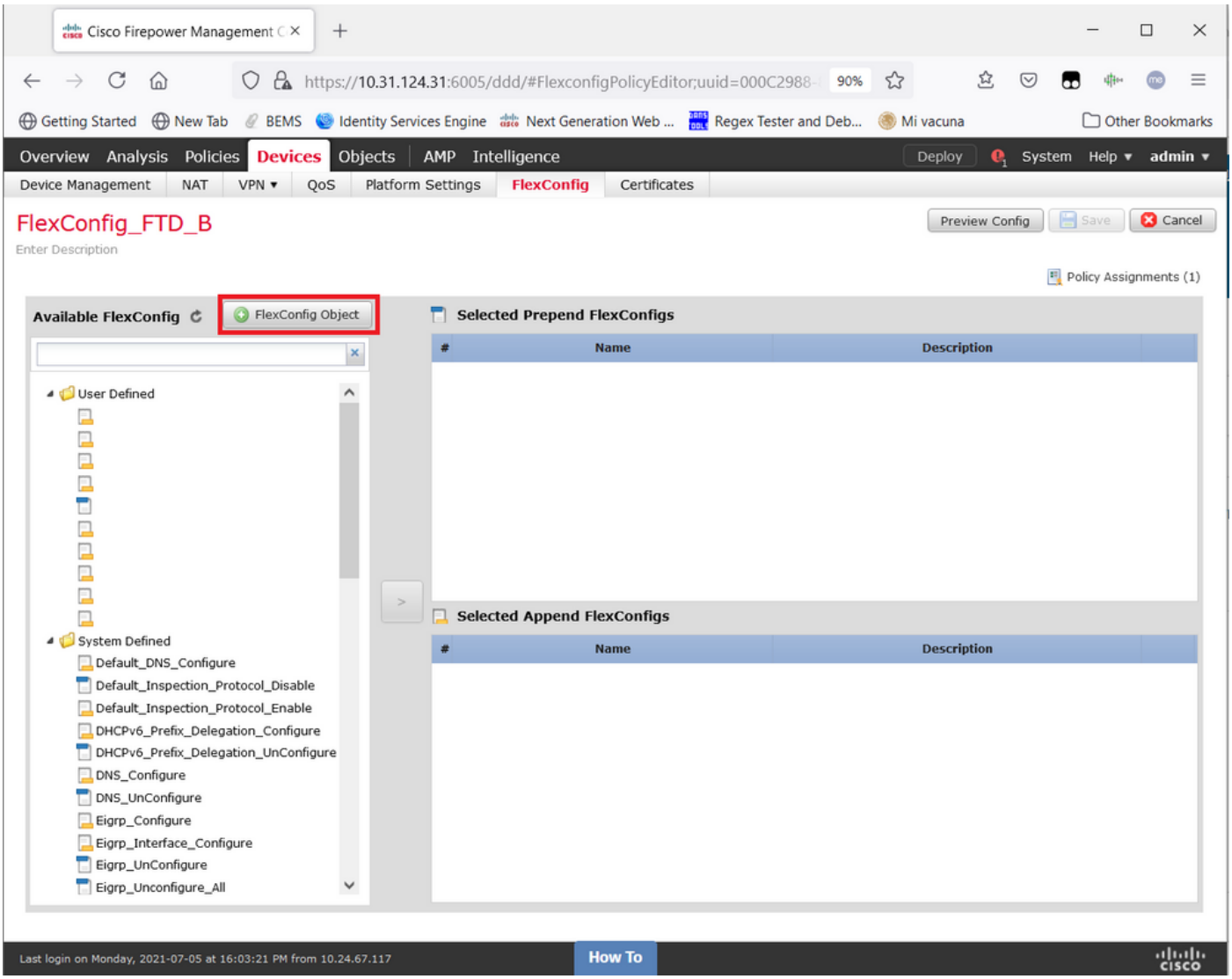
or

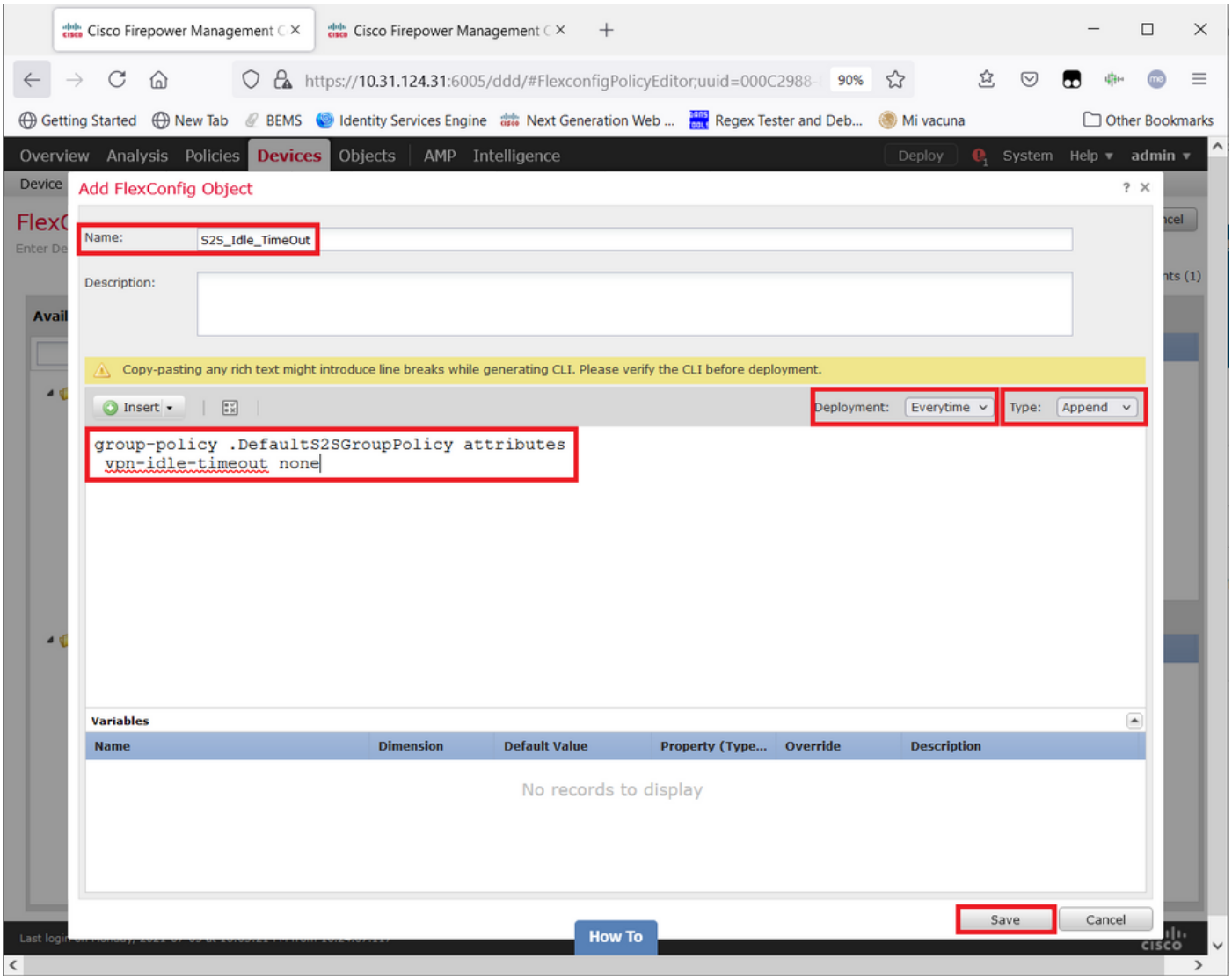


Step 2. Inside that policy create a **FlexConfig object** as follows:

Name: S2S_Idle_TimeOut
Deployment: Everytime
Type: Append

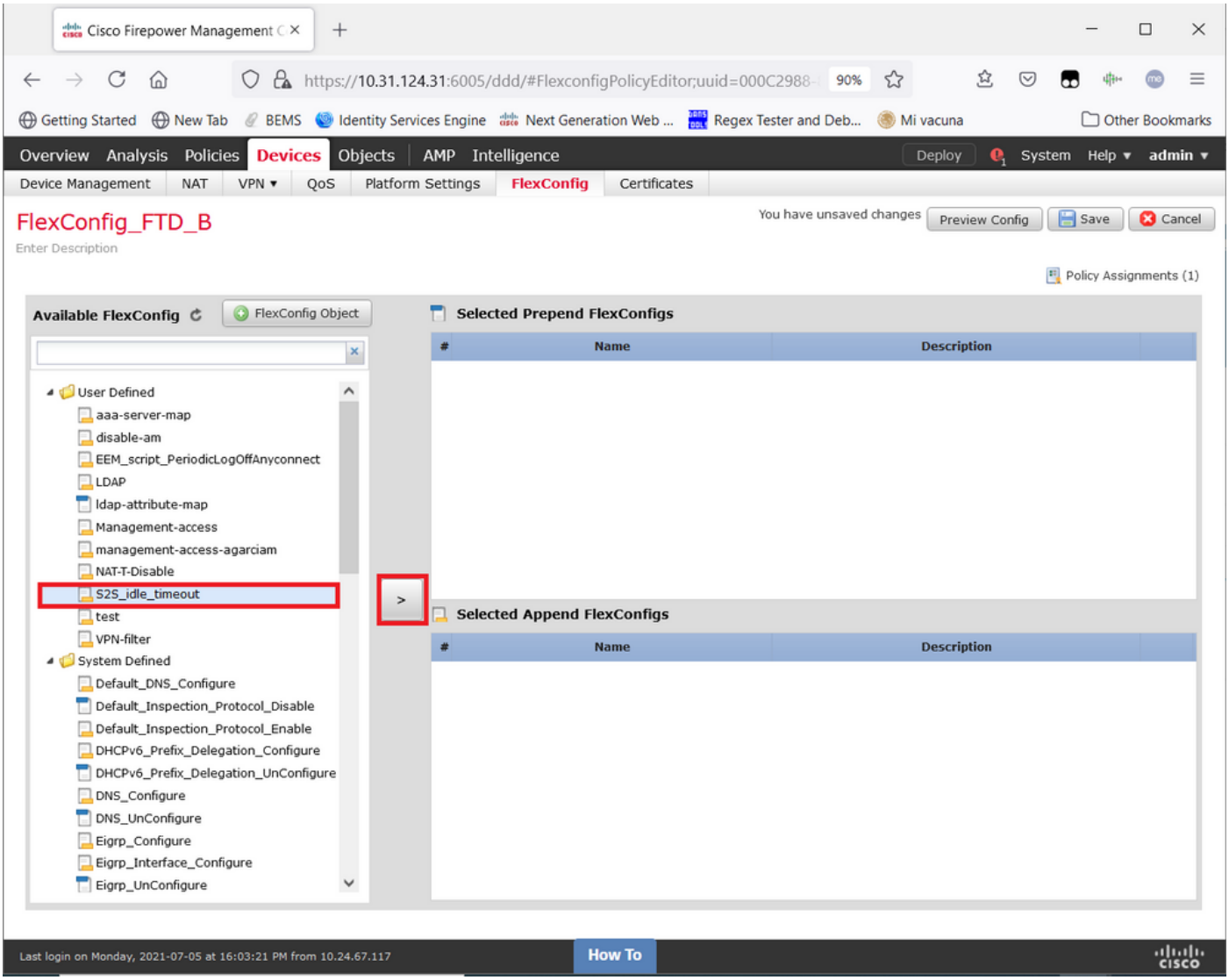
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout none

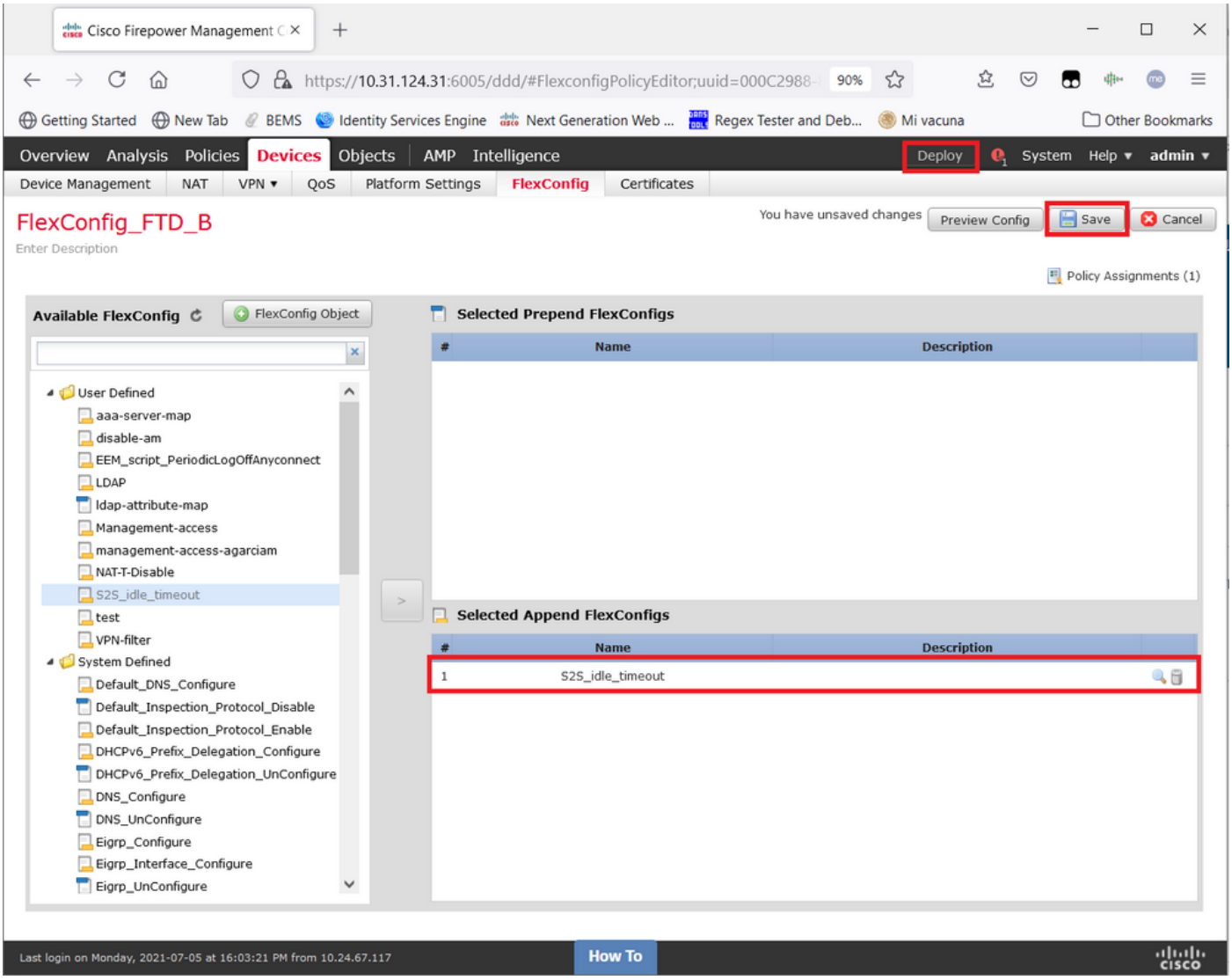




and **Save** it.

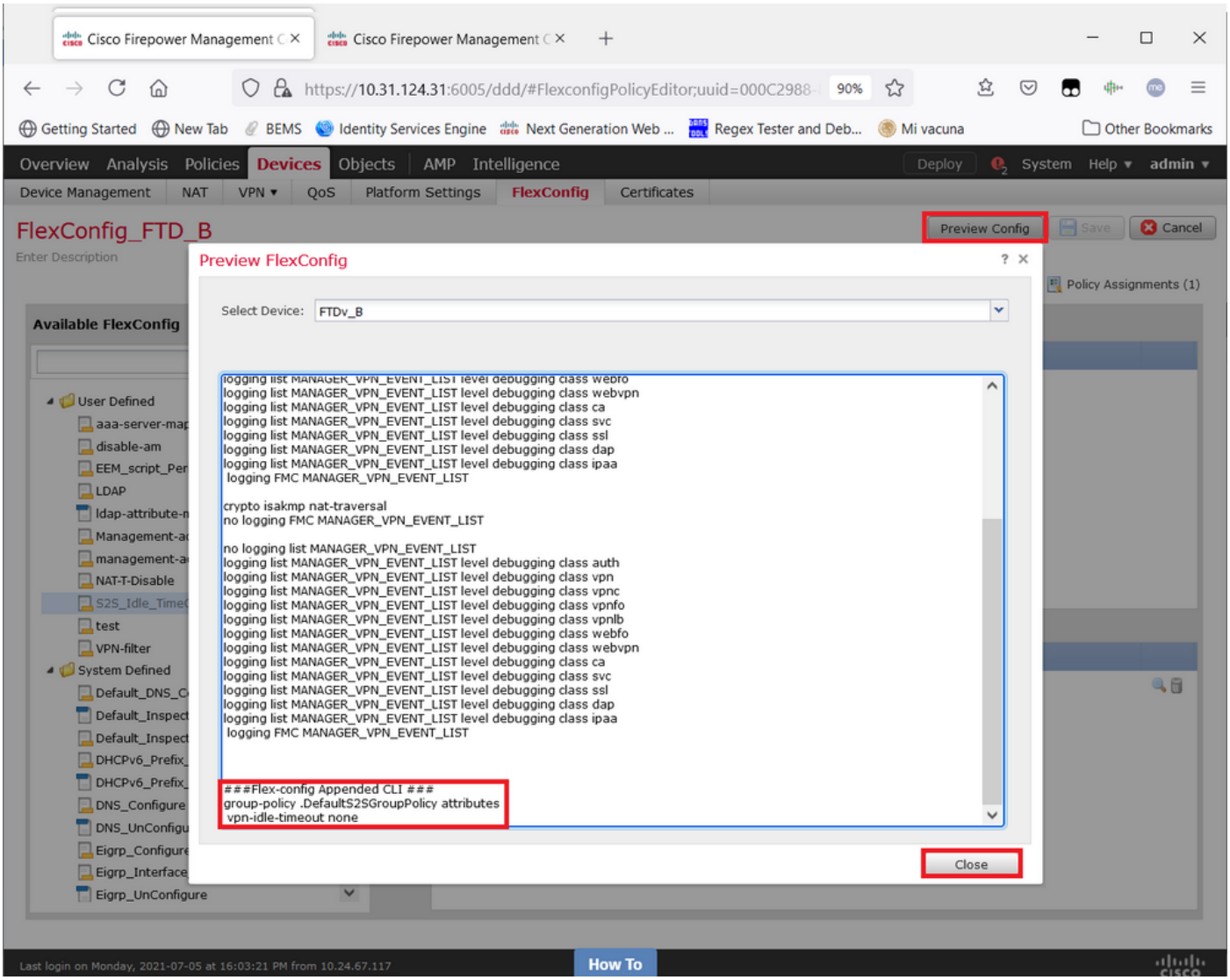
Step 3. In the left pane search for it and drag it to the right pane with the button **>**.


Cisco Firepower Management C
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



Save the changes and **Deploy**.

Step 3.1 (Optional) As an intermediate step, after configuration changes have been saved, you could choose **Preview Config** in order to ensure the FlexConfig commands are ready to be pushed at the end of the configuration.



Verify

Once deployment is complete, you can run this command in LINA (**> system support diagnostic-cli**) in order to confirm the new configuration is there:

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

> **Caution**: Keep in mind that this change affects all of the S2S VPNs on the FTD. It is NOT a per-tunnel setting but a global one.

Even though the configuration is there, the active tunnel needs to be bounced (**clear crypto ipsec sa peer** <*Remote_Peer_IP_Address*>) so the change takes effect when the tunnel gets established back again. You can confirm that the change is in effect with this command:

```
firepower# show vpn-sessiondb detail l2l filter ipaddress <Remote_Peer_IP_Address>

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
```

Idle Time Out counter must be set to 0 Minutes instead of 30 minutes and the VPN must remain active regardless of the activity/traffic running over it.

> **Note**: At the time of writing, there exists an Enhancement Bug to integrate the ability to modify this setting directly on FMC without the need of Flexconfig. See Cisco bug ID CSCvr82274 - ENH: make the vpn-idle-timeout configurable

Troubleshoot

There is currently no specific information to troubleshoot available.

Related Information

- **Firepower Management Center Configuration Guide, Version 7.0 - Chapter: FlexConfig Policies for Firepower Threat Defense**
- **Firepower Management Center Configuration Guide, Version 7.0 - Chapter: Site-to-Site VPNs for Firepower Threat Defense**
- **Technical Support & Documentation - Cisco Systems**