使用FlexConfig策略禁用FTD站点到站点VPN空闲超时

目录

简介

本文档介绍如何在Cisco Firepower管理中心(FMC)中修改具有FlexConfig策略的VPN的vpn-idle-timeout属性，以防止因非活动或空闲超时而导致隧道停机。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower威胁防御(FTD)
- FMC
- FlexConfig策略
- 站点到站点VPN拓扑

使用的组件

本文档中的信息基于以下软件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

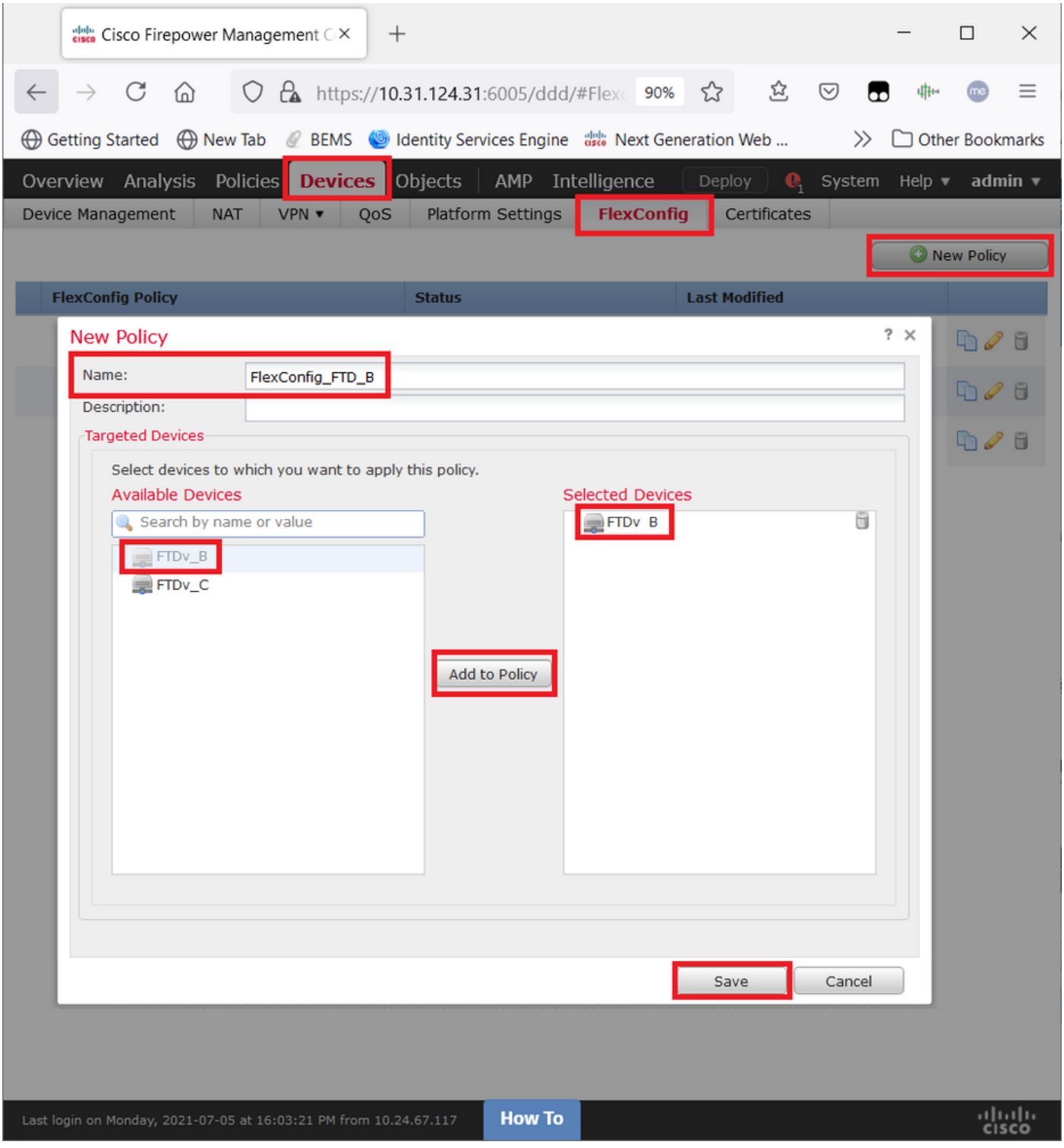
背景信息

互联网密钥交换版本1(IKEv1)和互联网密钥交换版本2(IKEv2)策略（加密映射）站点到站点VPN都是按需隧道。默认情况下，如果隧道在称为vpn-idle-timeout的特定时间段内没有通信活动，则FTD会终止VPN连**接。**此计时器默认设置为30分钟。

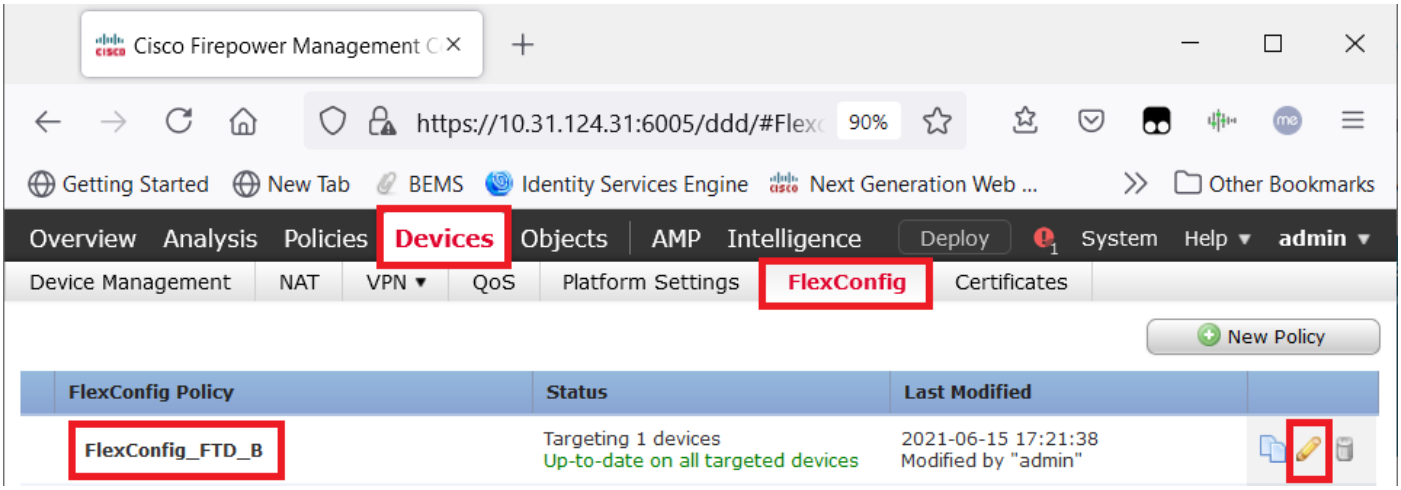
配置

配置FlexConfig策略和FlexConfig对象

步骤1.在**Devices > FlexConfig**下创建新的FlexConfig策略（如果尚不存在），并将其连接到配置了站点到站点VPN的FTD。



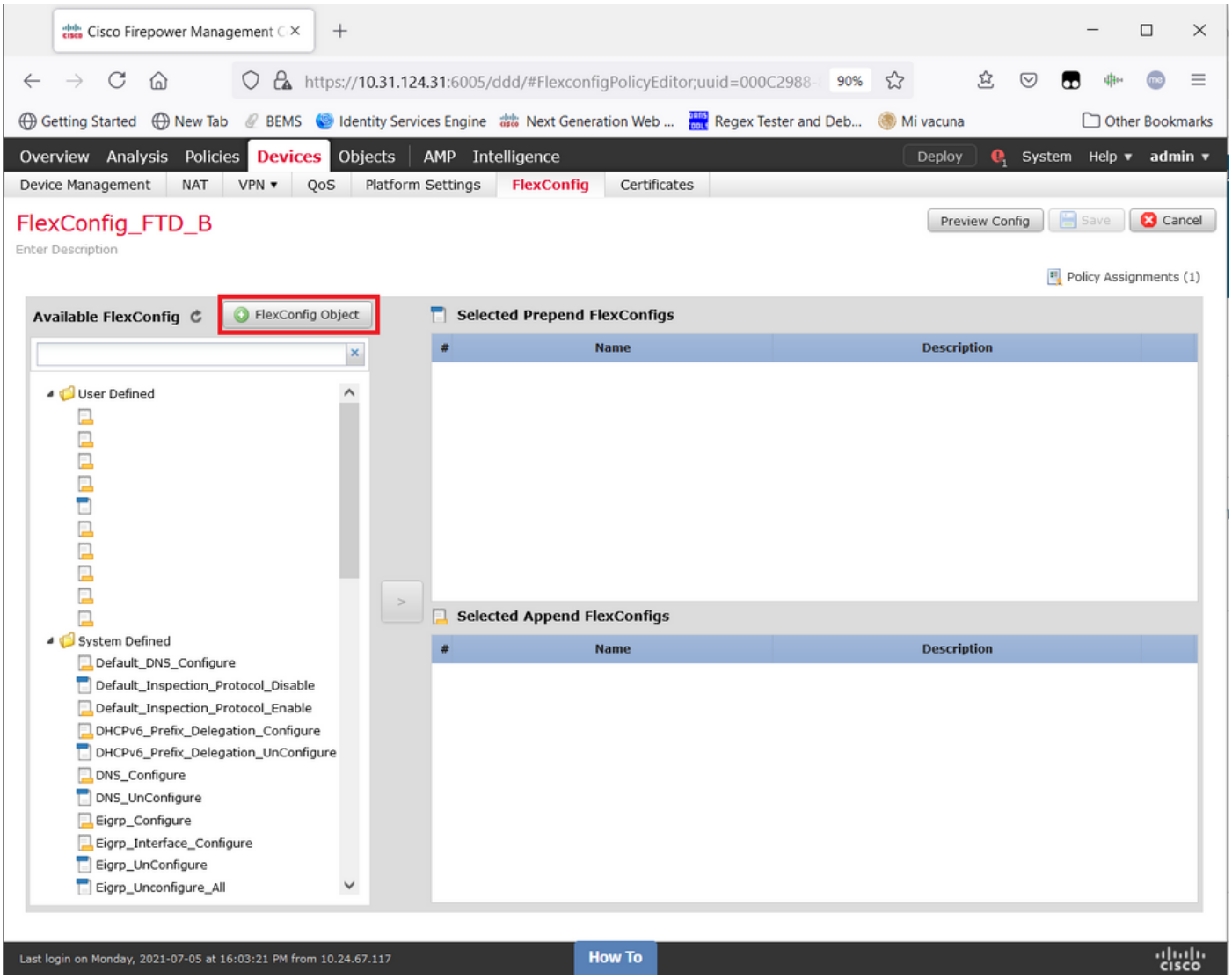
或

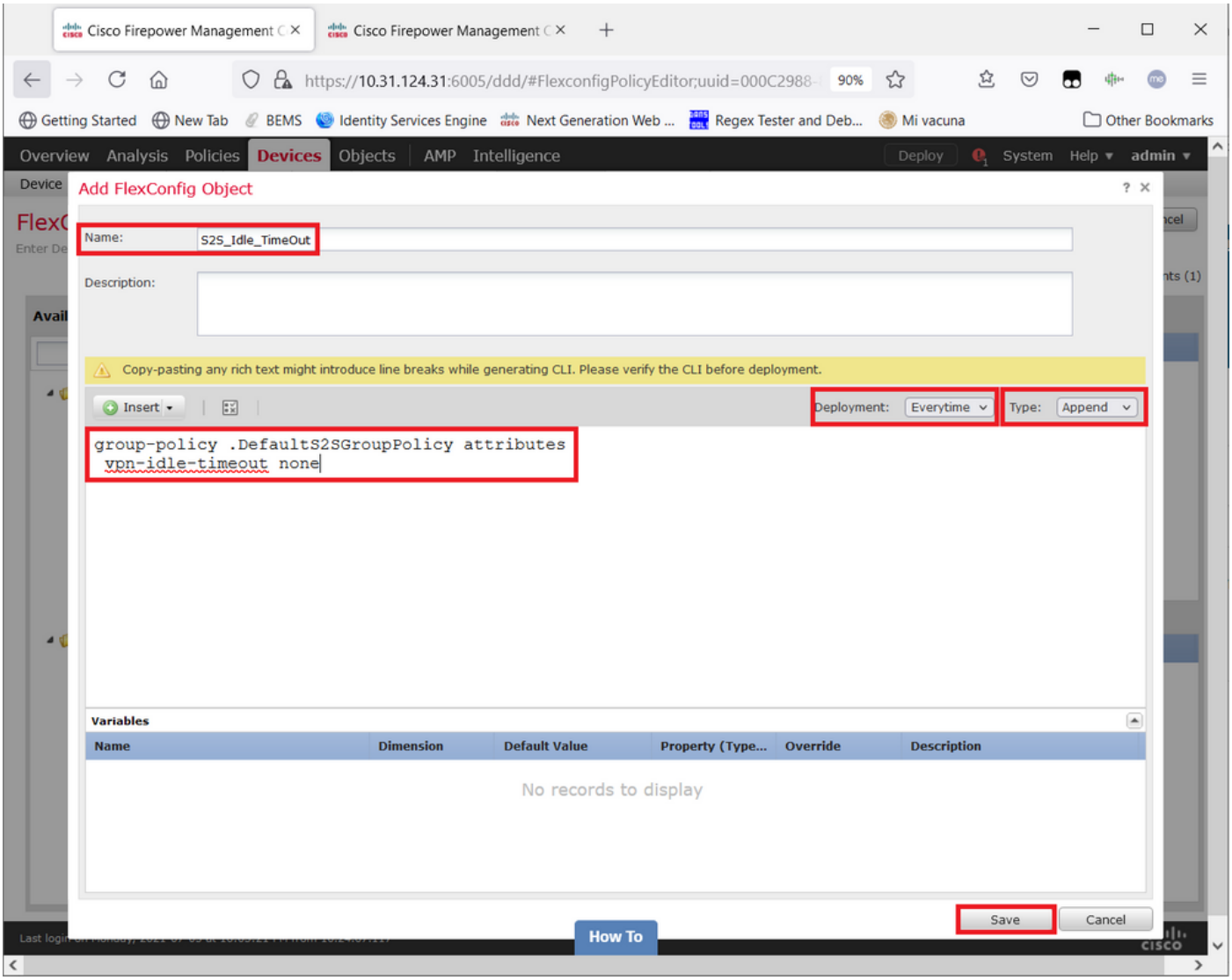


步骤2.在该策略内创建FlexConfig**对象**，如下所示：

名称：S2S_Idle_TimeOut
部署：每次
type：附加

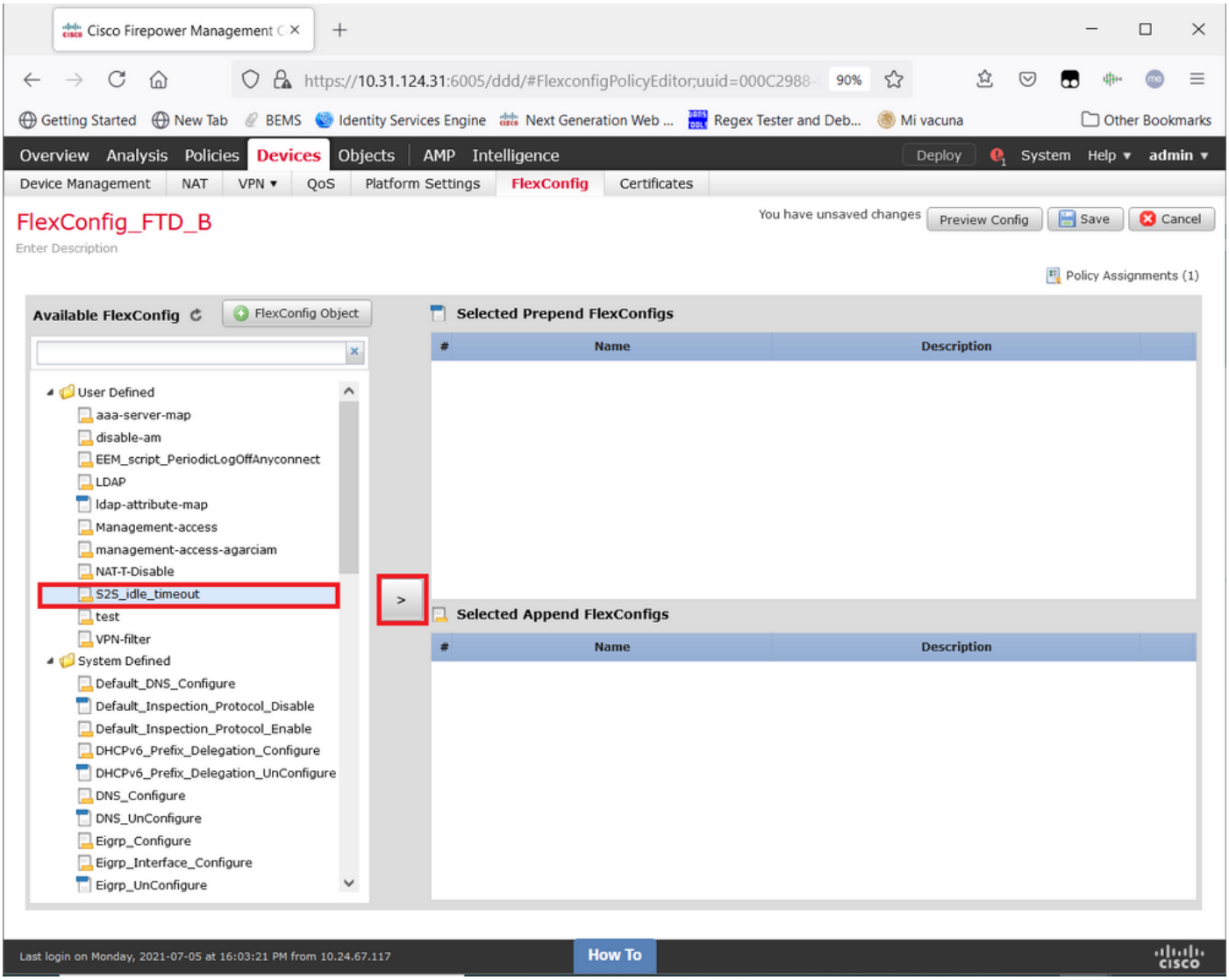
group-policy .DefaultS2SGroupPolicy属性
vpn-idle-timeout none

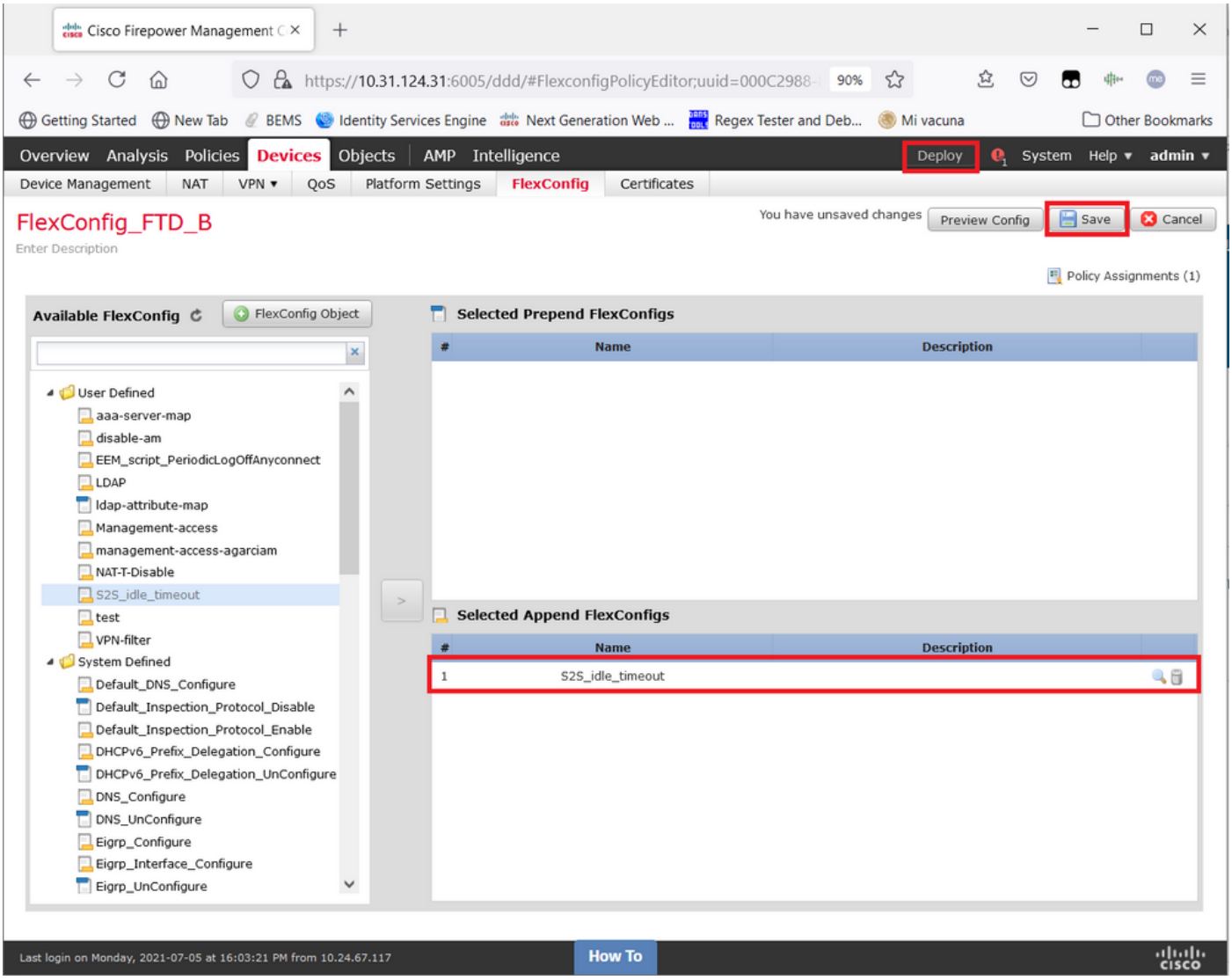




然后保存。

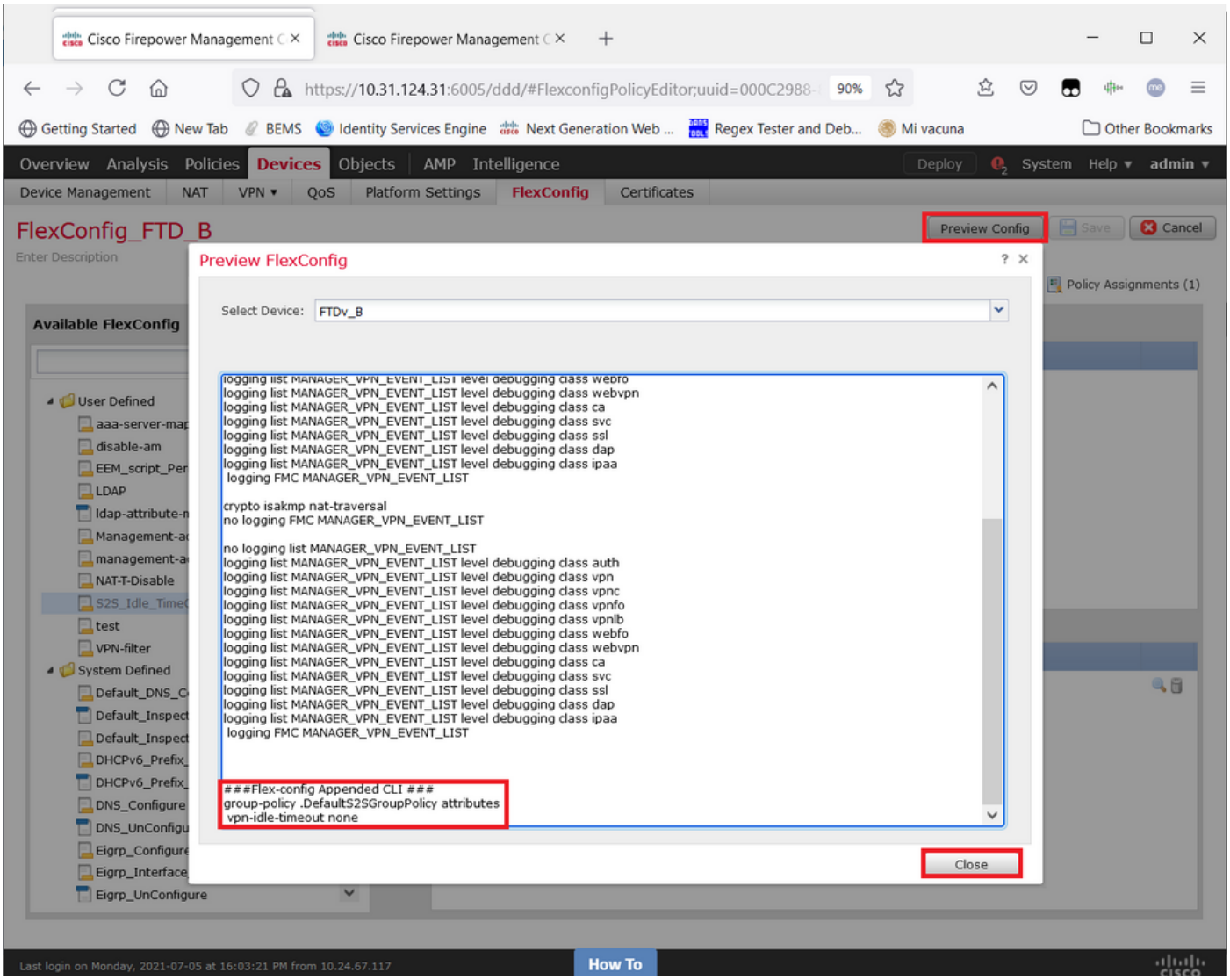
步骤3.在左窗格中搜索并用按钮>将其拖到右窗格中。


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



保存更改并**部署**。

第3.1步（可选）作为中间步骤，在保存配置更改后，您可以选择**预览配置**，以确保FlexConfig命令已准备好在配置末尾推送。



验证

部署完成后，您可以在LINA(> system support diagnostic-cli)**中运行此命令**，以确认新配置是否存在：

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

> **警告**：请记住，此更改会影响FTD上的所有S2S VPN。它不是每个隧道设置，而是全局设置。

即使存在配置，活动隧道也需要退回(**clear crypto ipsec sa peer** *<Remote_Peer_IP_Address>*)，以便在再次建立隧道时更改生效。您可以通过以下命令确认更改生效：

```
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
```

*Idle Time Out计*数器必须设置为0分钟而不是30分钟，并且VPN必须保持活动状态，无论其上运行的活动/流量如何。

> **注意：**在撰写本文时，存在增强错误，可集成直接在FMC上修改此设置的功能，而无需Flexconfig。请参阅Cisco Bug ID CSCvr82274 — 增强版：使vpn-idle-timeout可配置

故障排除

目前没有可用于故障排除的特定信息。

相关信息

- Firepower管理中心配置指南，版本7.0 — 第章：Firepower威胁防御的FlexConfig策略
- Firepower管理中心配置指南，版本7.0 — 第章：用于Firepower威胁防御的站点到站点VPN
- 技术支持和文档 - Cisco Systems