FlexConfigポリシーによるFTDサイト間VPNアイドルタイムアウトの無効化

内容

概要

このドキュメントでは、非アクティブまたはアイドルタイムアウトによるトンネルのダウンタイムを防ぐために、Cisco Firepower Management Center(FMC)のFlexConfigポリシーを使用してVPNの**vpn-idle-timeout属性を変更する方法について説明します**。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Threat Defense(FTD)
- FMC
- FlexConfigポリシー
- サイト間VPNトポロジ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMCv - 6.5.0.4（ビルド57）
- FTDv - 6.4.0.10（ビルド95）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

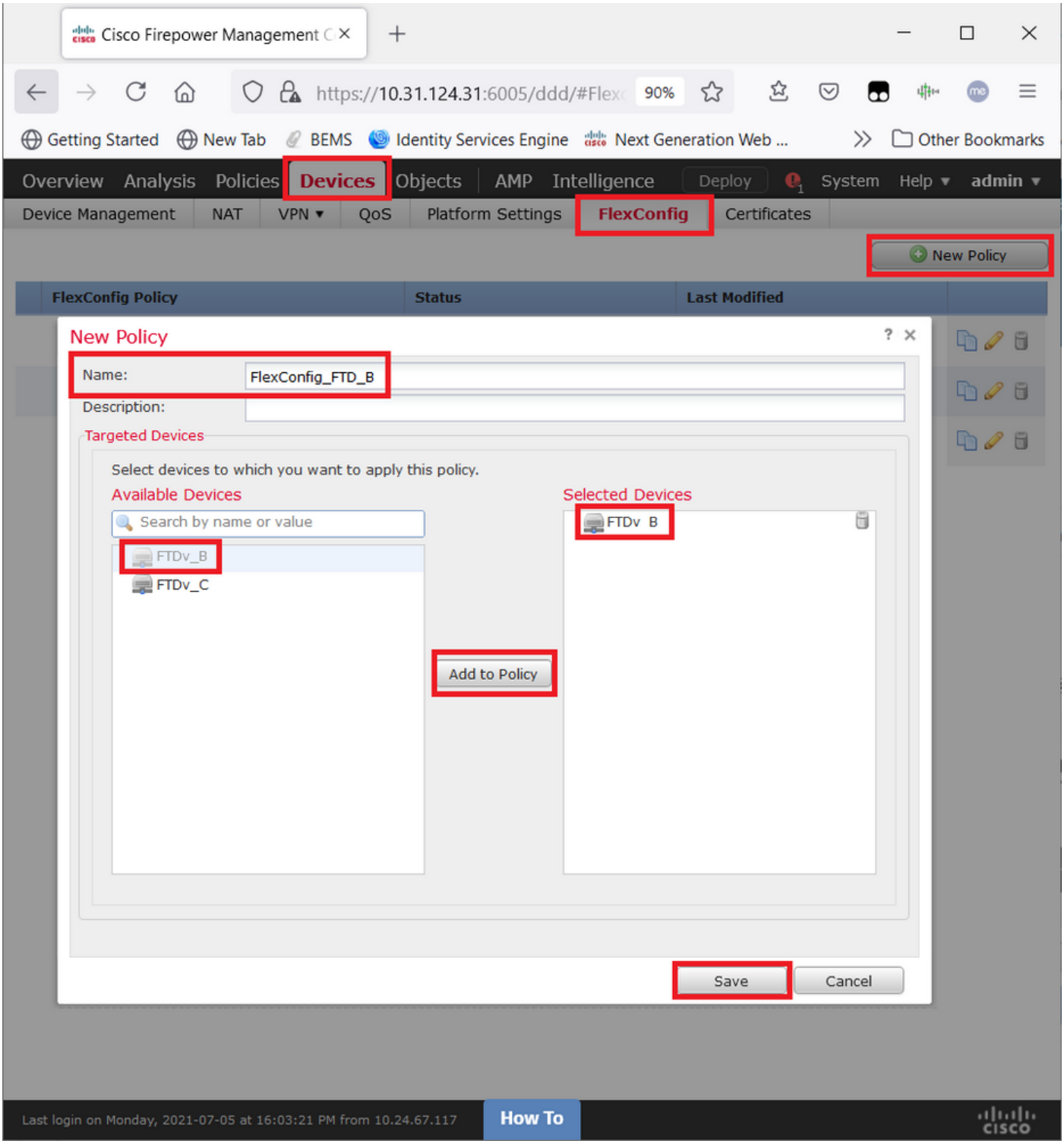
背景説明

インターネットキーエクスチェンジバージョン1(IKEv1)とインターネットキーエクスチェンジバージョン2(IKEv2)のポリシーベース（クリプトマップ）サイト間VPNは、どちらもオンデマンドトンネルです。デフォルトでは、**vpn-idle-timeout**と呼ばれる特定の時間内にトンネル上で通信アクティビティがない場合、FTDはVPN接続を終了します。このタイマーは、デフォルトで30分に設定されています。

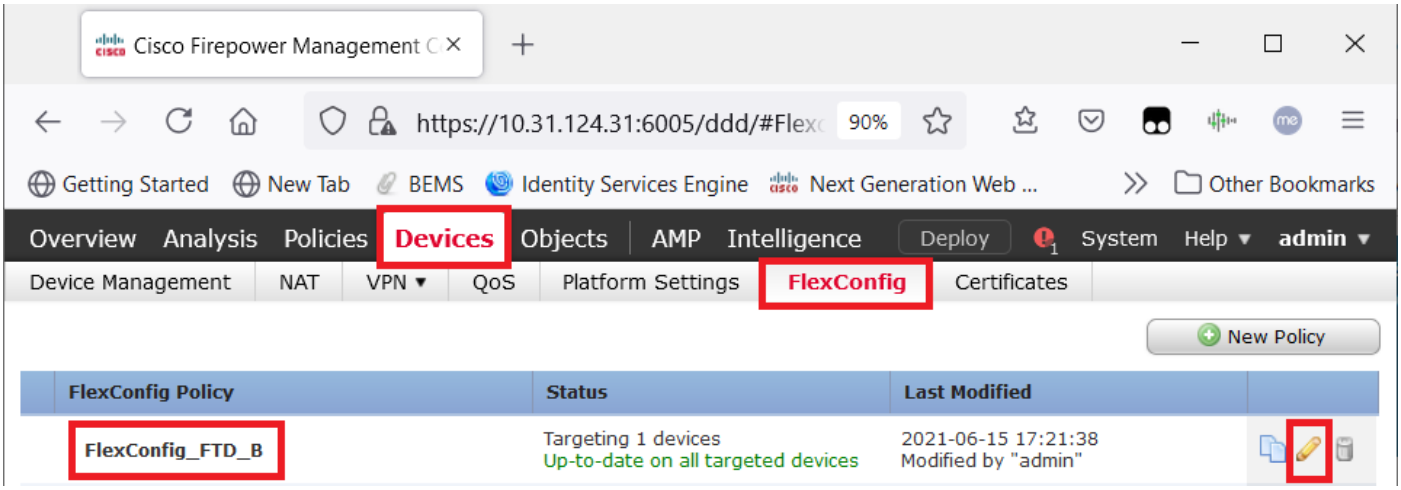
設定

FlexConfigポリシーとFlexConfigオブジェクトの設定

ステップ1:[Devices] > [FlexConfig] で、新しいFlexConfigポリシー（存在しない場合）を作成し、それをサイト間VPNが設定されているFTDに接続します。


Cisco Firepower Management
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

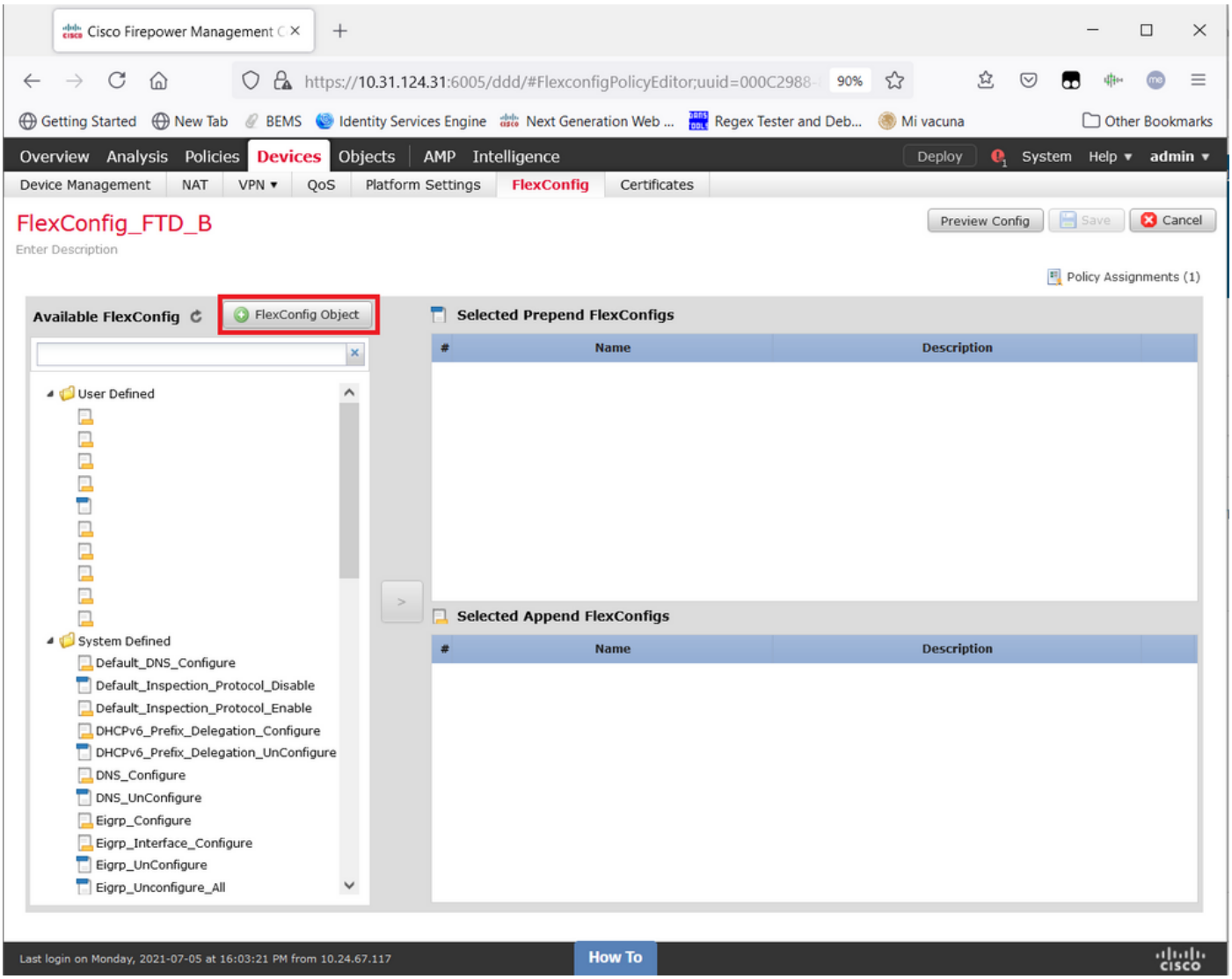
または

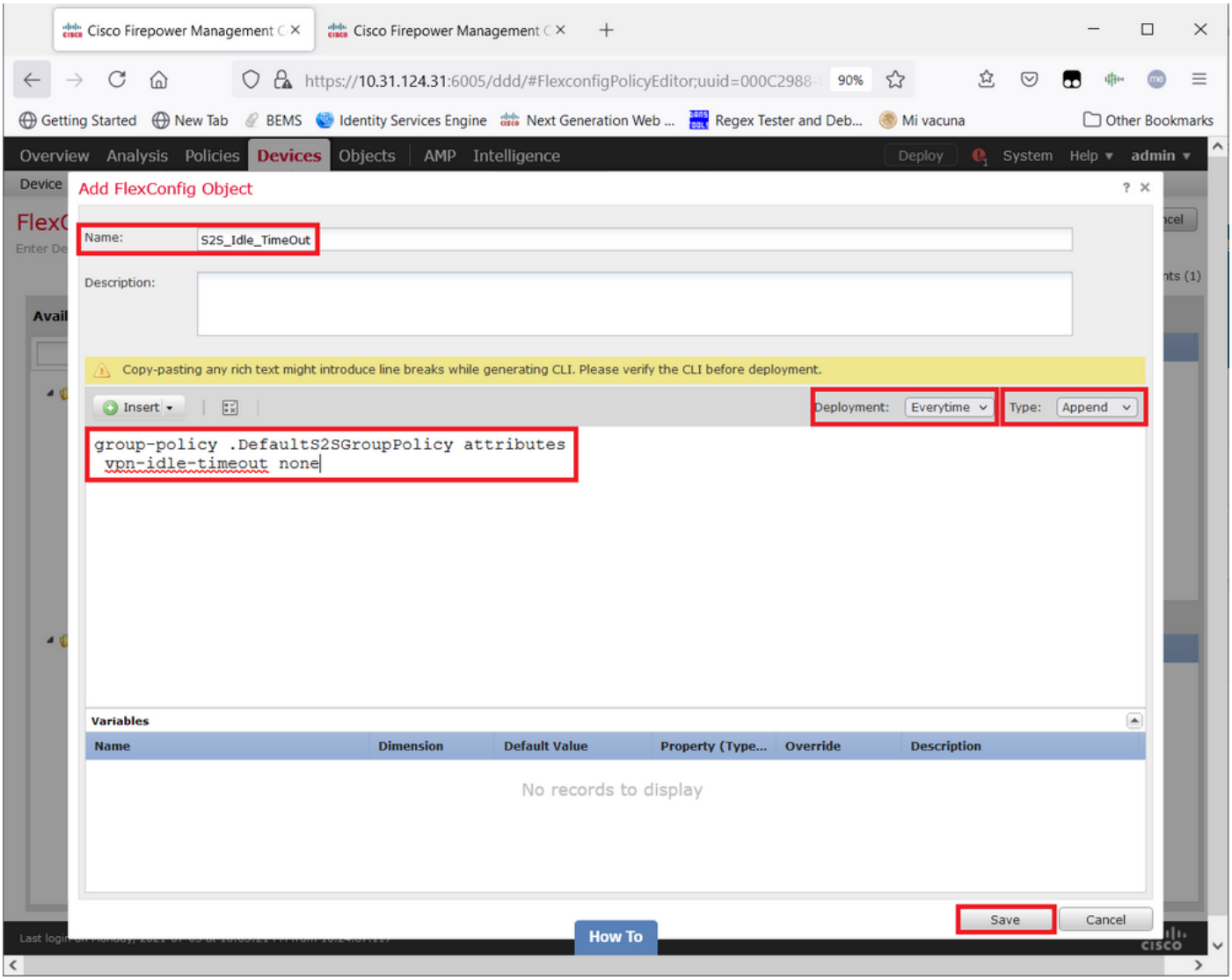


ステップ2：このポリシー内で、次のように**FlexConfigオブジェクト**を作成します。

[Name]：S2S_Idle_TimeOut
導入:毎回
Type:追加

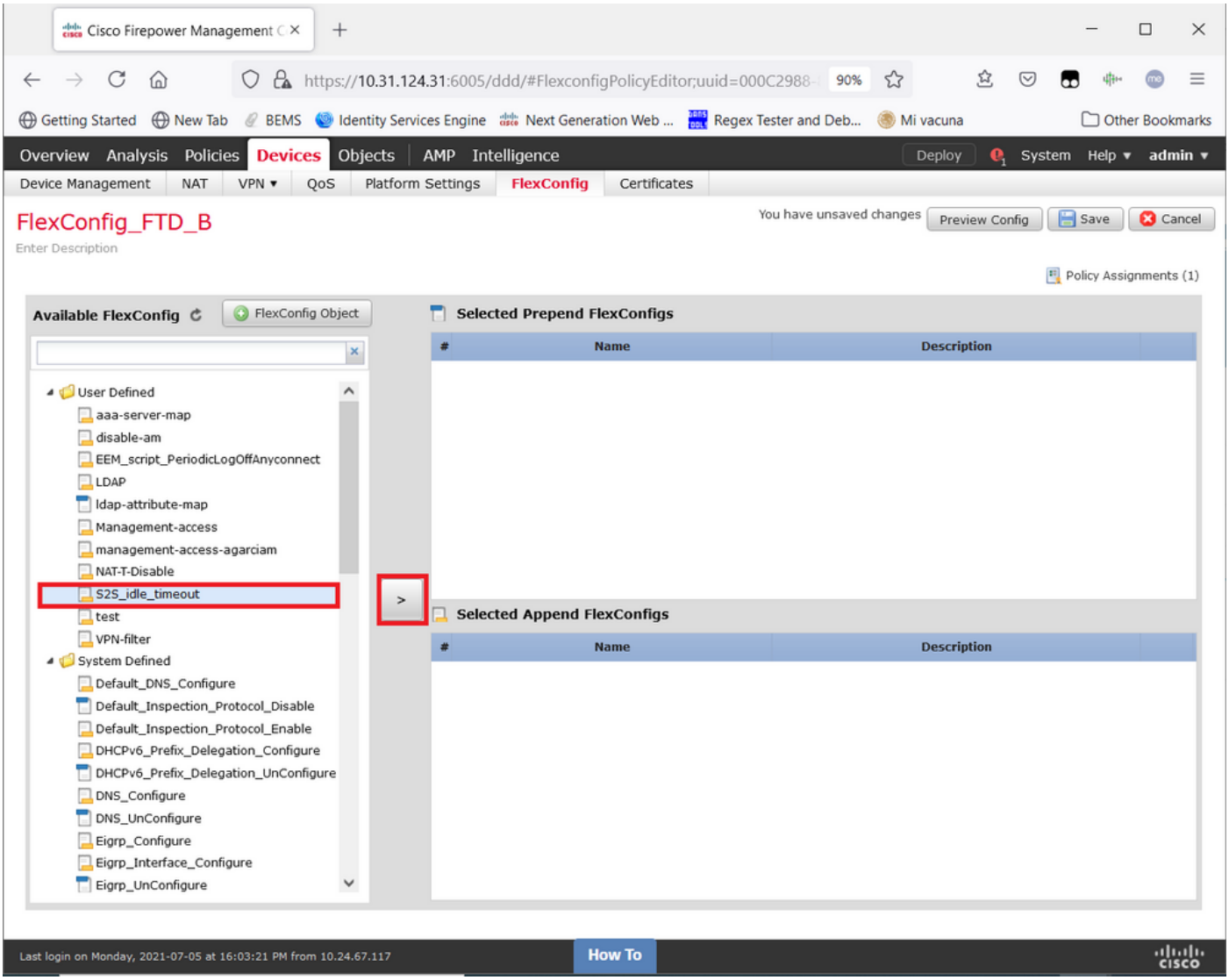
group-policy .DefaultS2SGroupPolicy属性
vpn-idle-timeout none

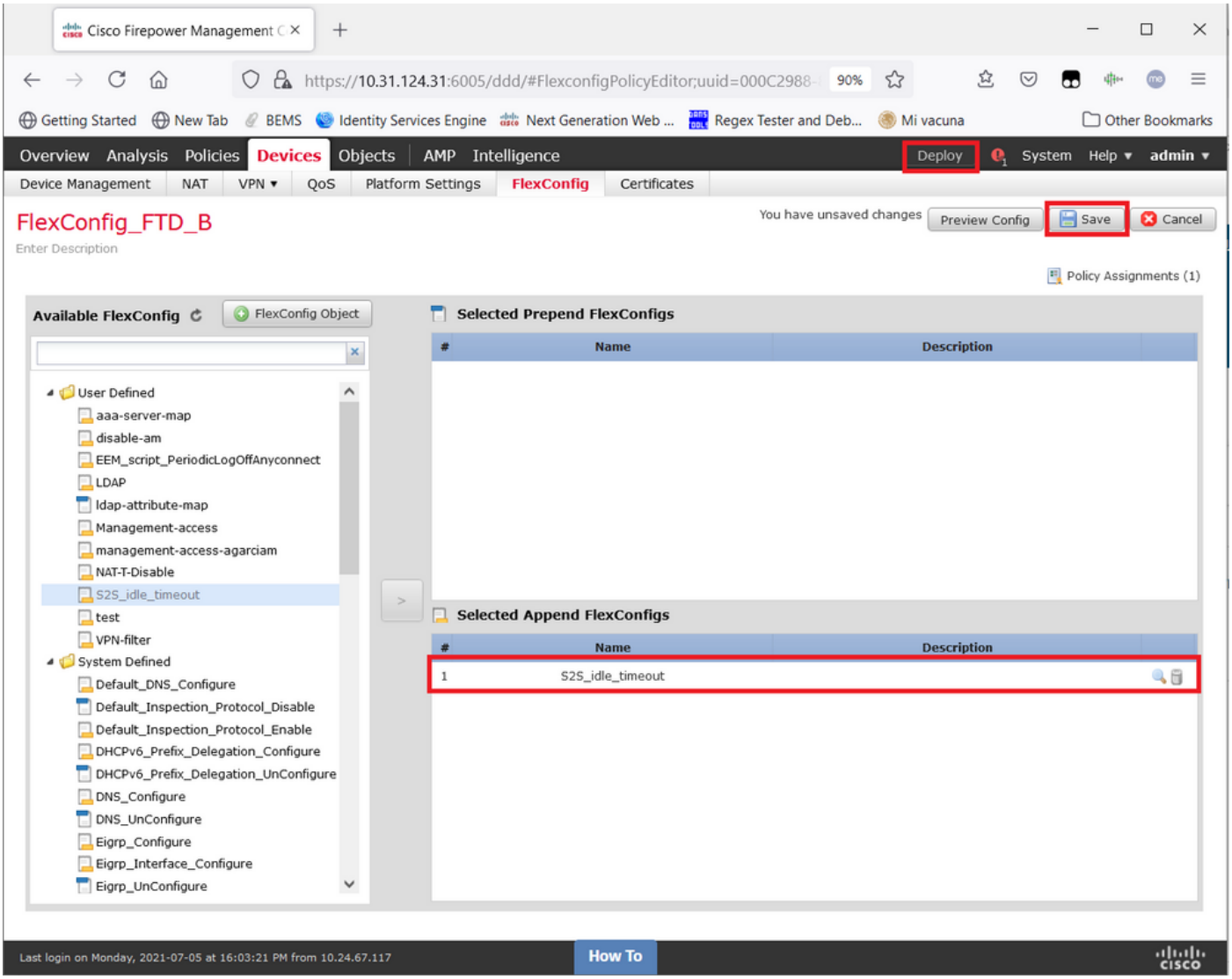




そして**保存**します。

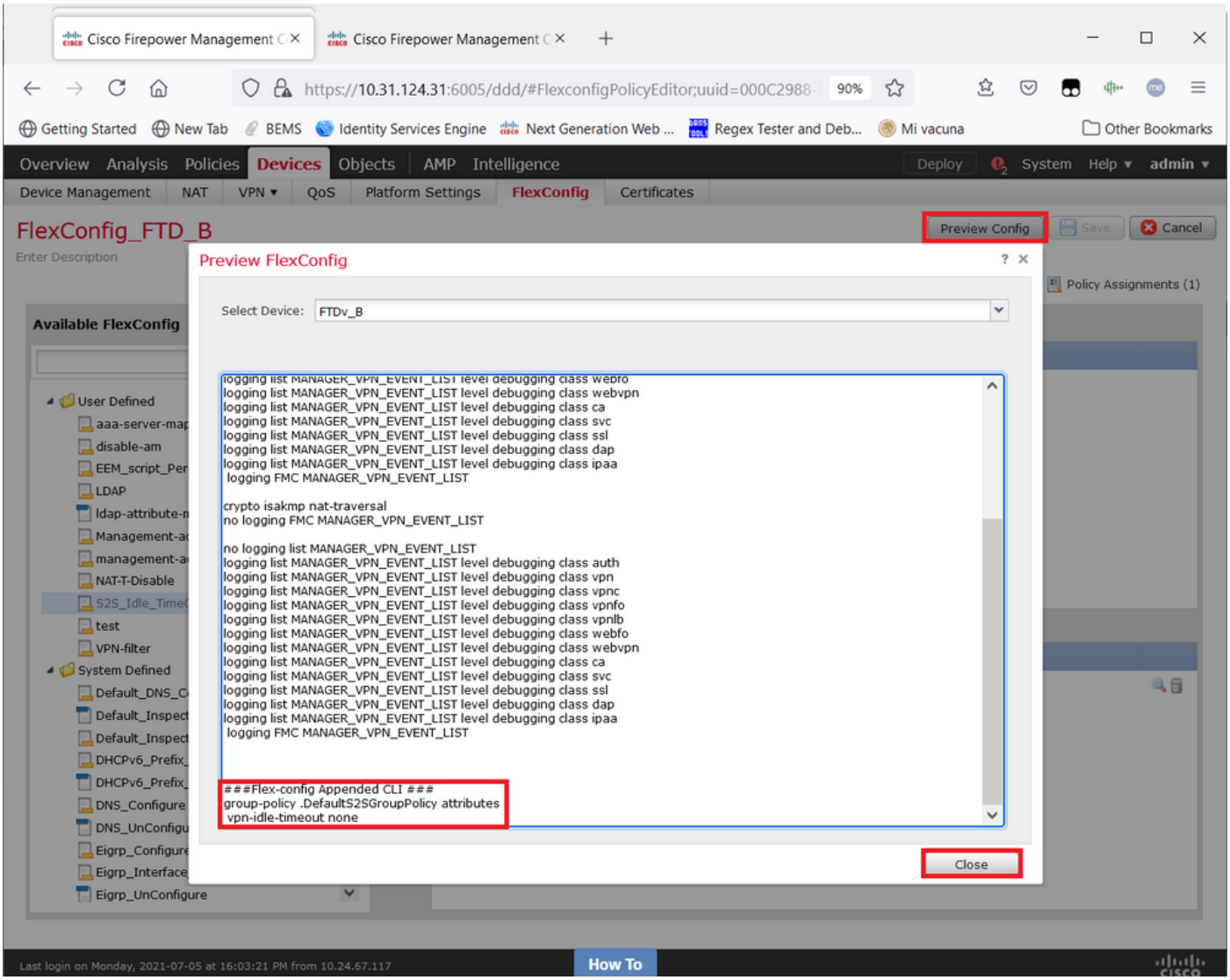
ステップ3：左側のペインで検索し、ボタン>を使用して右側のペインにドラッグ**します**。


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



変更を保存し、[Deploy]を選択します。

ステップ3.1（オプション）設定の変更を保存した後の中間ステップとして、**[Preview Config]を選択して**、FlexConfigコマンドを設定の最後にプッシュする準備ができていることを確認します。



確認

導入が完了したら、LINA(**> system support diagnostic-cli**)でこのコマンドを実行して、新しい設定があることを確認できます。

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

> **注意**：この変更は、FTD上のすべてのS2S VPNに影響することに注意してください。これはトンネル単位の設定ではなく、グローバル設定です。

設定がある場合、アクティブなトンネルをバウンスする必要があります(**clear crypto ipsec sa peer** *<Remote_Peer_IP_Address>*)。*これにより、トンネルが再確立されたときに変更が有効になります。*変更が有効であることを確認するには、次のコマンドを使用します。

```
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
```

アイドルタイムアウトカウンタは30分ではなく0分に設定する必要があり、VPN上で実行されているアクティビティやトラフィックに関係なく、VPNはアクティブなままである必要があります。

> **注：**執筆時点では、Flexconfigを使用せずにFMCでこの設定を直接変更する機能を統合する拡張バグが存在します。Cisco Bug ID CSCvr82274 - ENH:vpn-idle-timeoutを設定可能にする

トラブルシュート

現在、トラブルシューティングに必要な特定の情報はありません。

関連情報

- Firepower Management Centerコンフィギュレーションガイド、バージョン7.0 – 章：Firepower Threat DefenseのFlexConfigポリシー
- Firepower Management Centerコンフィギュレーションガイド、バージョン7.0 – 章：Firepower Threat Defenseのサイト間VPN
- テクニカル サポートとドキュメント – Cisco Systems