Desactivar el tiempo de espera de inactividad de VPN de sitio a sitio de FTD con las políticas de FlexConfig

Contenido

Introducción

Este documento describe cómo modificar el atributo **vpn-idle-timeout** de una VPN con políticas FlexConfig en Cisco Firepower Management Center (FMC) para evitar el tiempo de inactividad del túnel debido a la inactividad o el tiempo de espera inactivo.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense (FTD)
- FMC
- Políticas de FlexConfig
- Topologías VPN de sitio a sitio

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- FMCv - 6.5.0.4 (compilación 57)
- FTDv - 6.4.0.10 (compilación 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

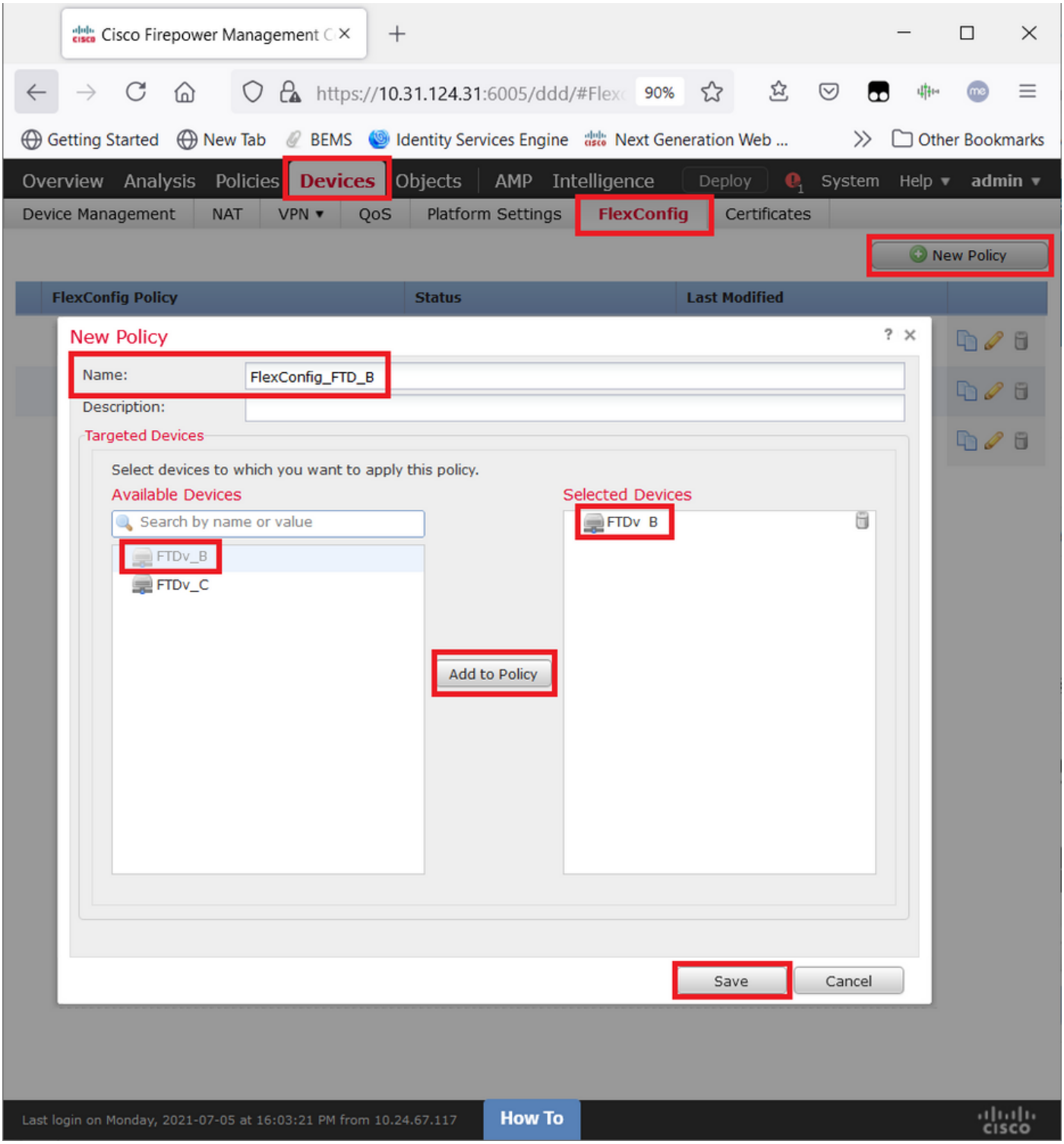
Antecedentes

Tanto las VPN basadas en políticas (mapa criptográfico) basadas en el intercambio de claves de Internet versión 1 (IKEv1) como las de la versión 2 del intercambio de claves de Internet (IKEv2) son túneles a demanda. De forma predeterminada, el FTD finaliza la conexión VPN si no hay actividad de comunicación sobre el túnel en un período determinado llamado **vpn-idle-timeout**. Este temporizador se establece en 30 minutos de forma predeterminada.

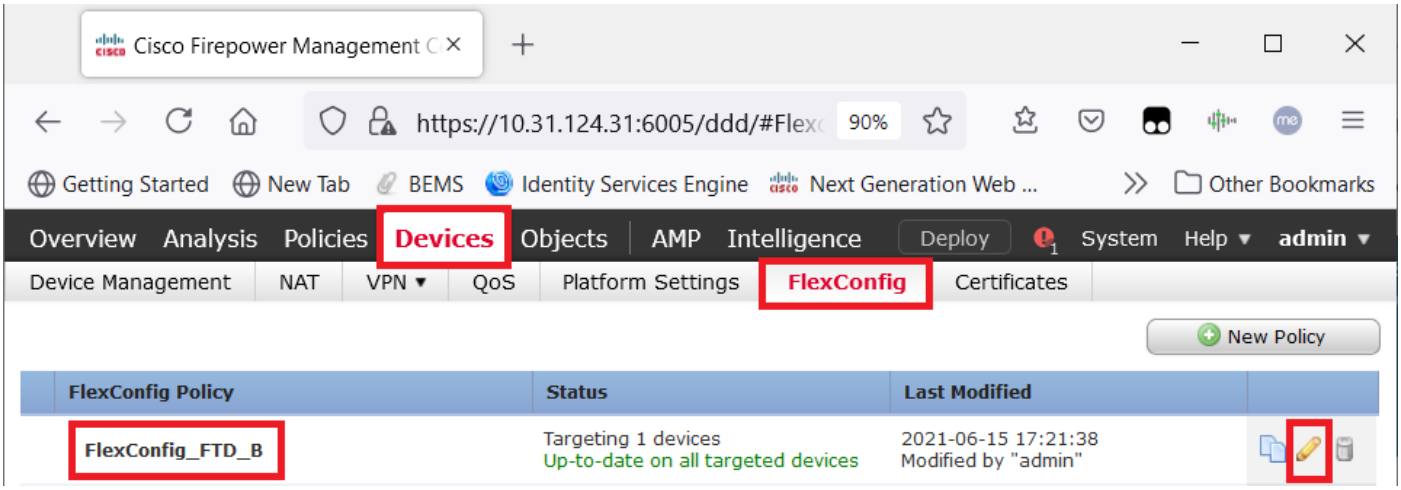
Configurar

Configurar la política FlexConfig y el objeto FlexConfig

Paso 1. En **Devices > FlexConfig**, cree una nueva política FlexConfig (si aún no existe) y adáptela al FTD donde se configura la VPN de sitio a sitio.


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

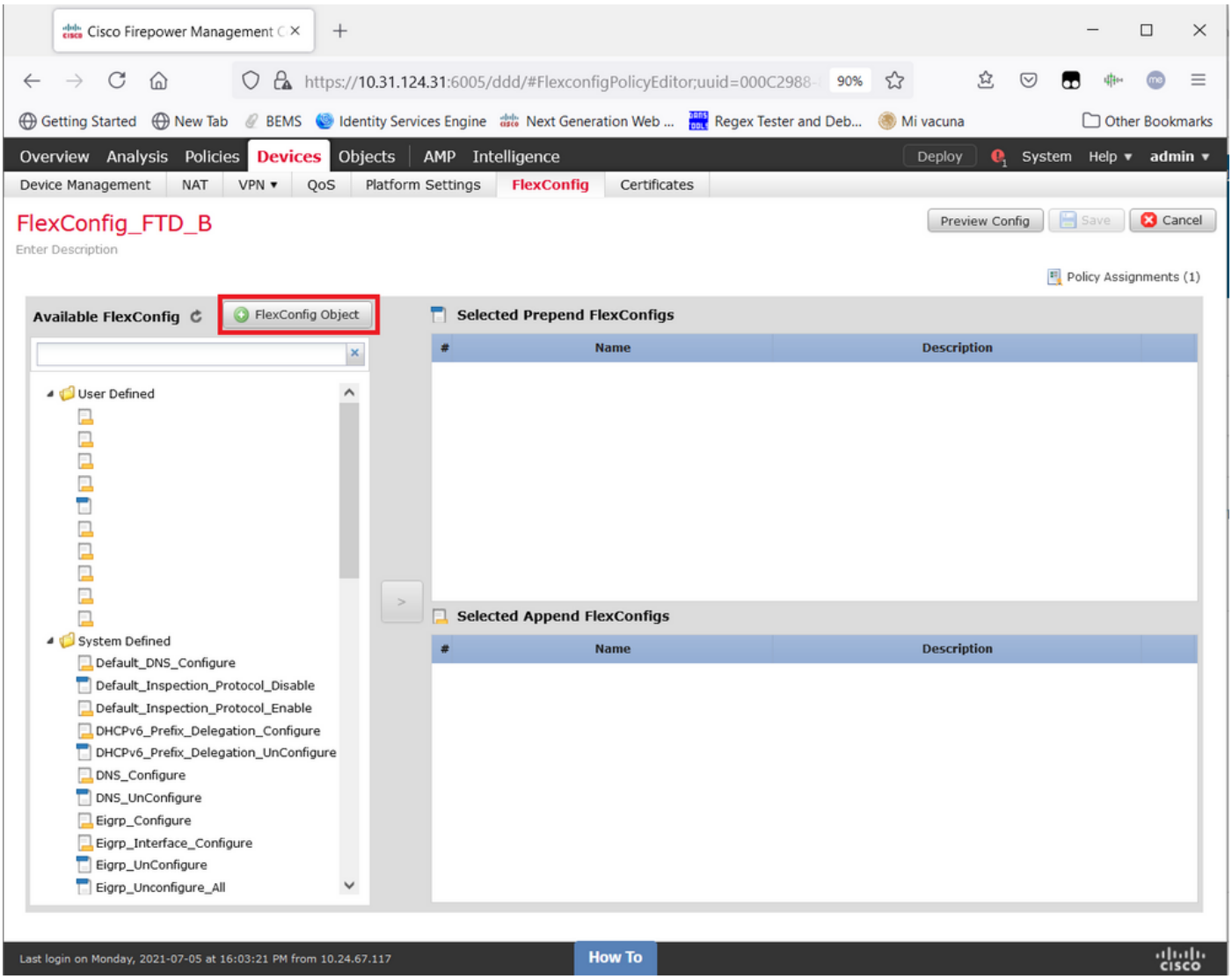
or

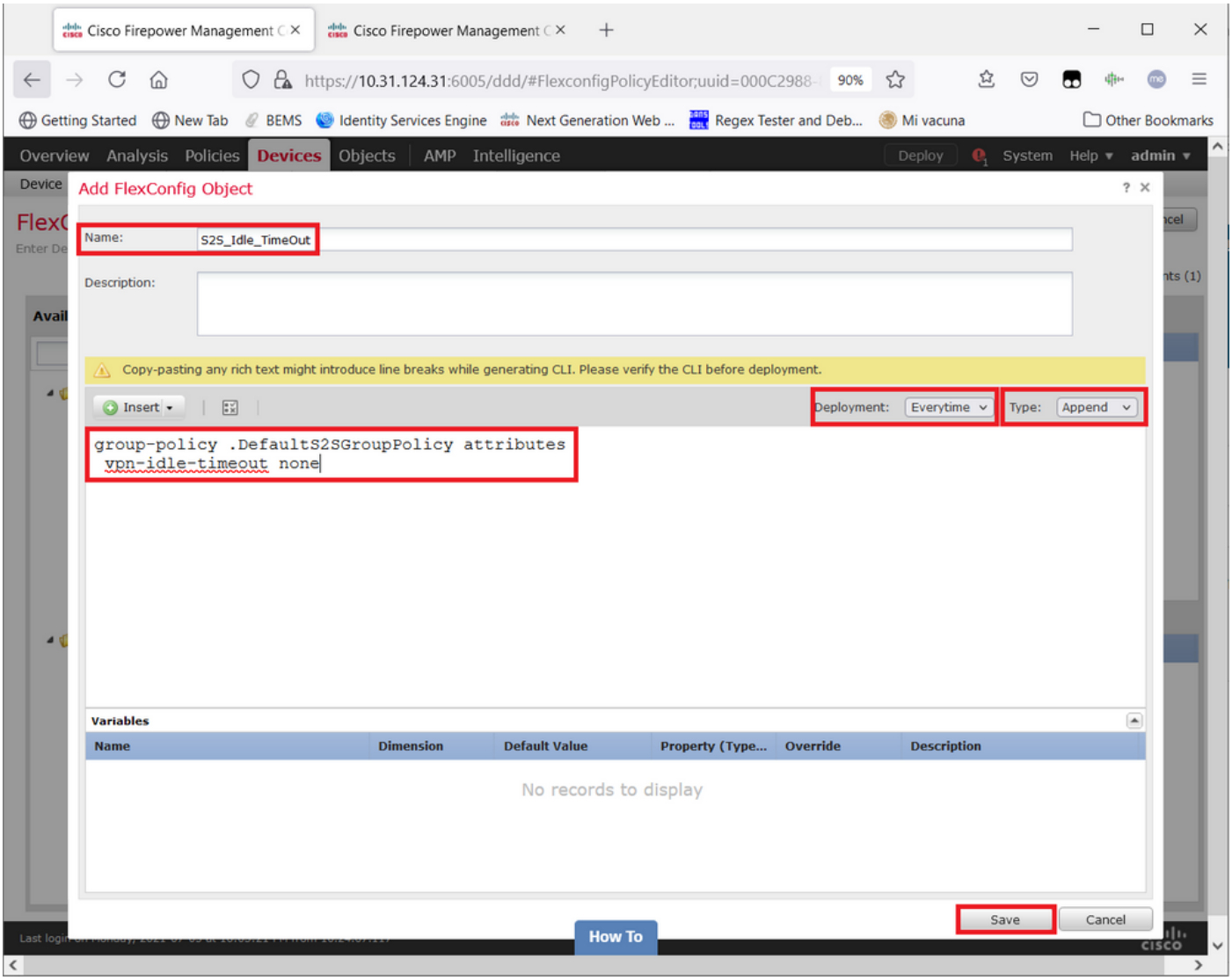


Paso 2. Dentro de esa política, cree un **objeto FlexConfig** de la siguiente manera:

Nombre: S2S_Idle_TimeOut
Implementación: En cualquier momento
Tipo: Anexar

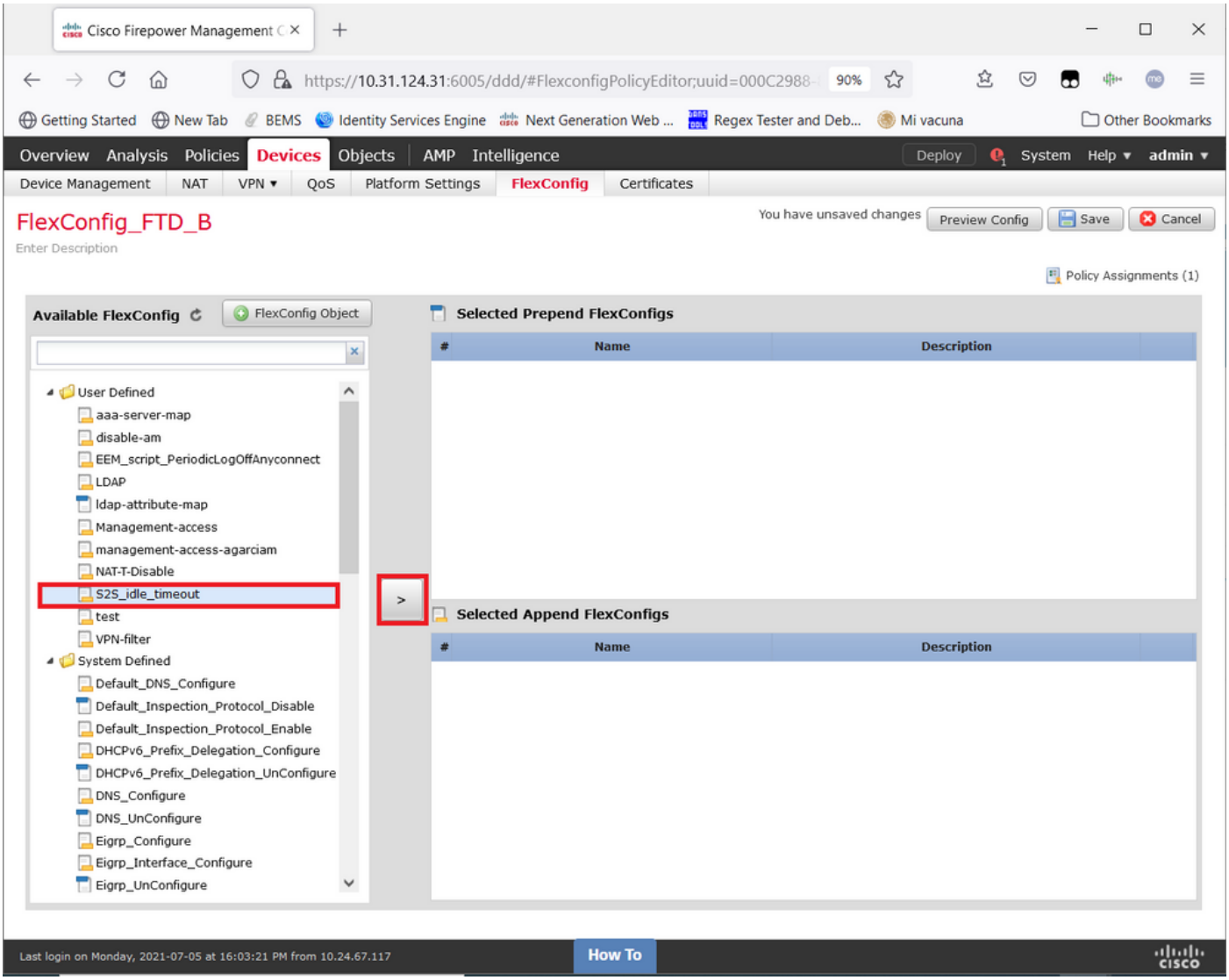
atributos de política de grupo .DefaultS2SGroupPolicy
vpn-idle-timeout none

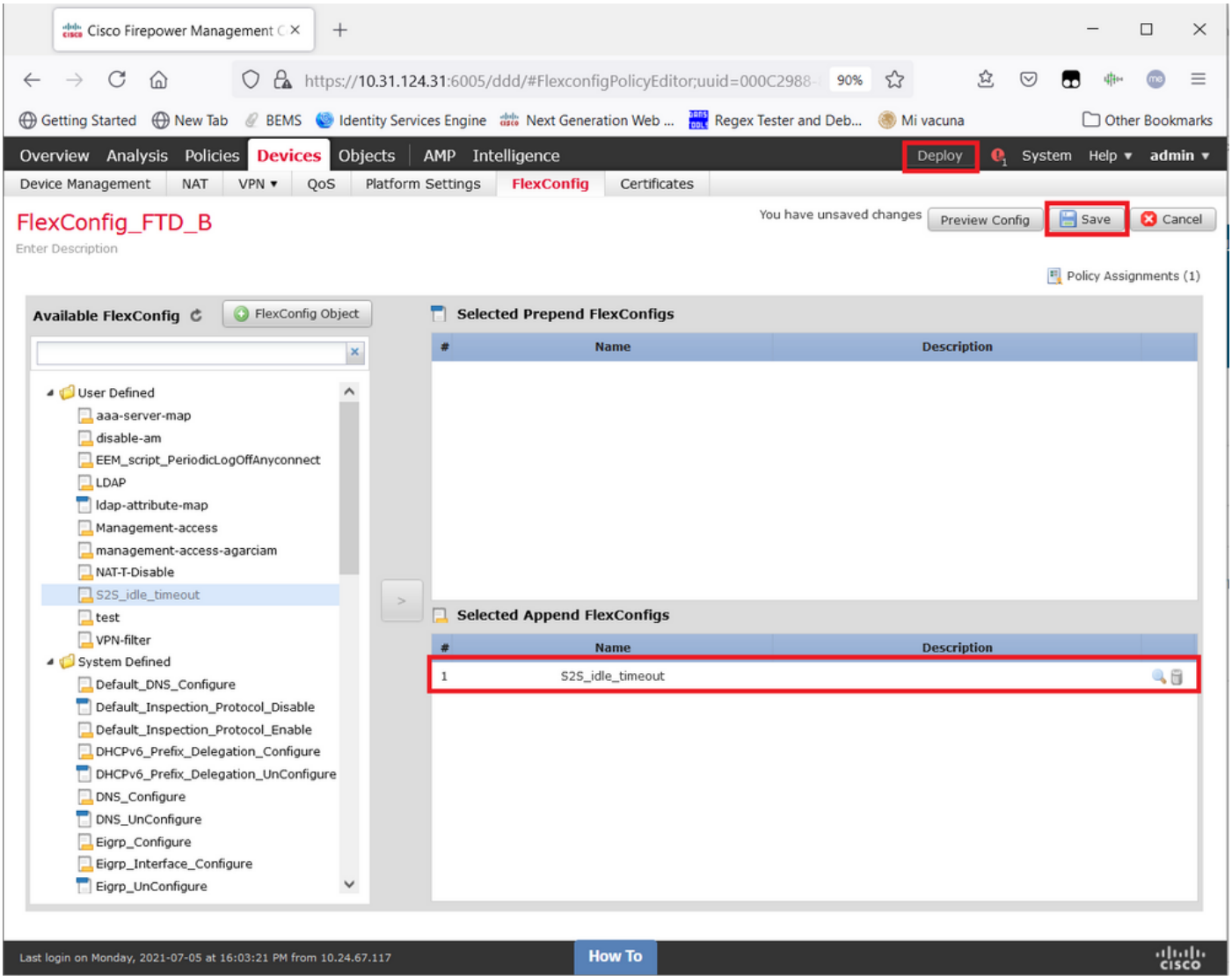




y **guárdelo**.

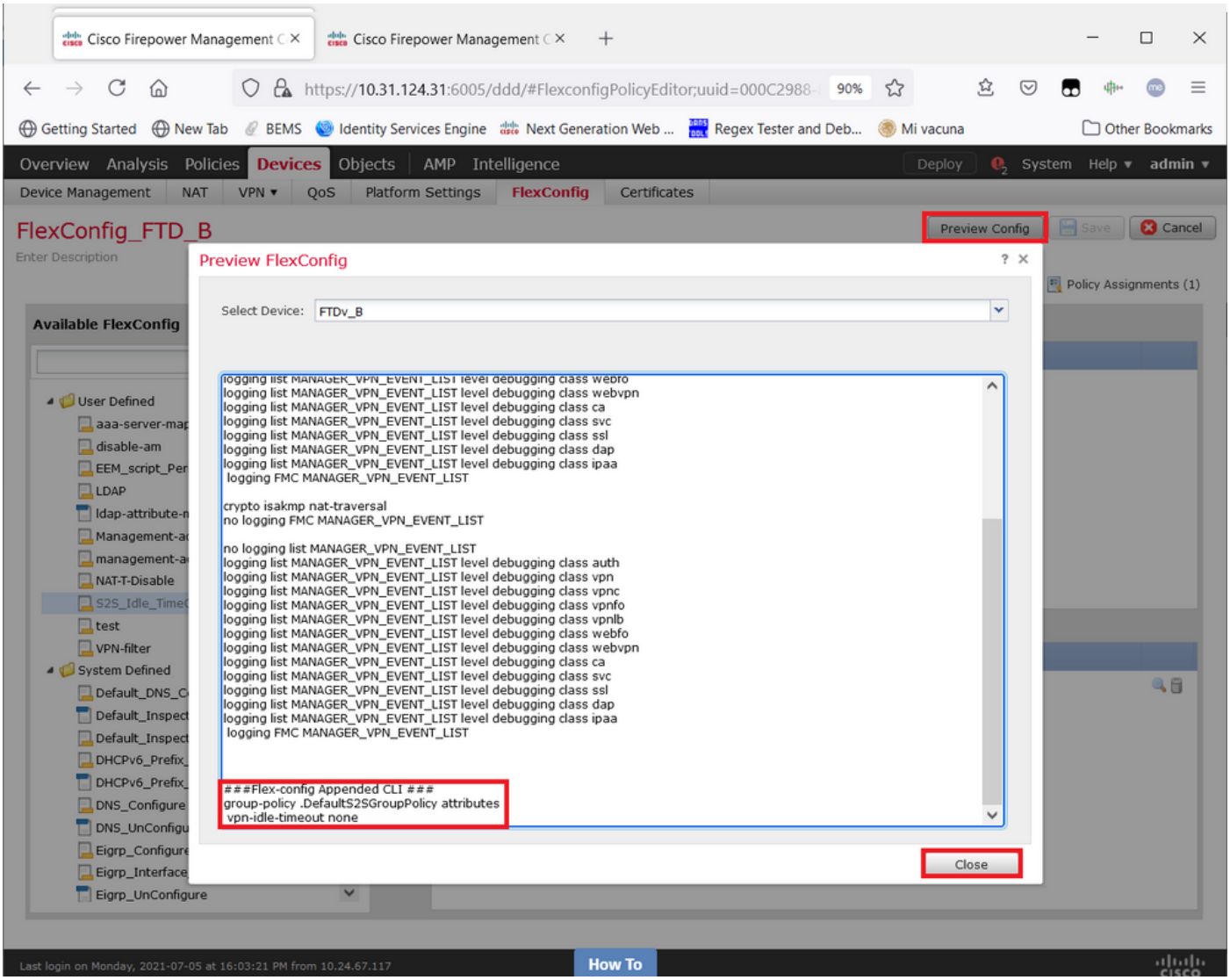
Paso 3. En el panel izquierdo, busque y arrástrelo al panel derecho con el botón **>**.


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



Guarde los cambios y **implemente**.

Paso 3.1 (Opcional) Como paso intermedio, después de haber guardado los cambios de configuración, puede elegir **Vista previa de configuración** para asegurarse de que los comandos FlexConfig estén listos para ser empujados al final de la configuración.



Verificación

Una vez que se complete la implementación, puede ejecutar este comando en LINA (**> system support diagnostic-cli**) para confirmar que la nueva configuración está ahí:

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

> **Precaución:** Tenga en cuenta que este cambio afecta a todas las VPN S2S del FTD. NO es una configuración por túnel sino una global.

Aunque la configuración está ahí, el túnel activo necesita ser rebotado (**clear crypto ipsec sa peer** *<Remote_Peer_IP_Address>*) para que el cambio surta efecto cuando el túnel se restablezca nuevamente. Puede confirmar que el cambio está en vigor con este comando:

```
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
```

El contador *de tiempo de espera inactivo* debe establecerse en 0 Minutos en lugar de 30 minutos y la VPN debe permanecer activa independientemente de la actividad/tráfico que se esté ejecutando sobre ella.

> **Nota:** Al momento de escribir este artículo, existe un Bug de mejora para integrar la capacidad de modificar esta configuración directamente en FMC sin la necesidad de Flexconfig. Consulte Cisco bug ID CSCvr82274 - ENH: haga configurable vpn-idle-timeout

Troubleshoot

Actualmente no hay información específica disponible para resolver problemas.

Información Relacionada

- Guía de Configuración de Firepower Management Center, Versión 7.0 - Capítulo: Políticas FlexConfig para Firepower Threat Defense
- Guía de Configuración de Firepower Management Center, Versión 7.0 - Capítulo: VPN de sitio a sitio para Firepower Threat Defense
- Soporte Técnico y Documentación - Cisco Systems