Desative o tempo limite ocioso de VPN site a site do FTD com políticas FlexConfig

Contents

Introduction

Este documento descreve como modificar o atributo **vpn-idle-timeout** de uma VPN com Políticas FlexConfig no Cisco Firepower Management Center (FMC) para evitar o tempo de inatividade do túnel devido ao tempo limite de inatividade ou ociosidade.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD)
- FMC
- Políticas FlexConfig
- Topologias de VPN site a site

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

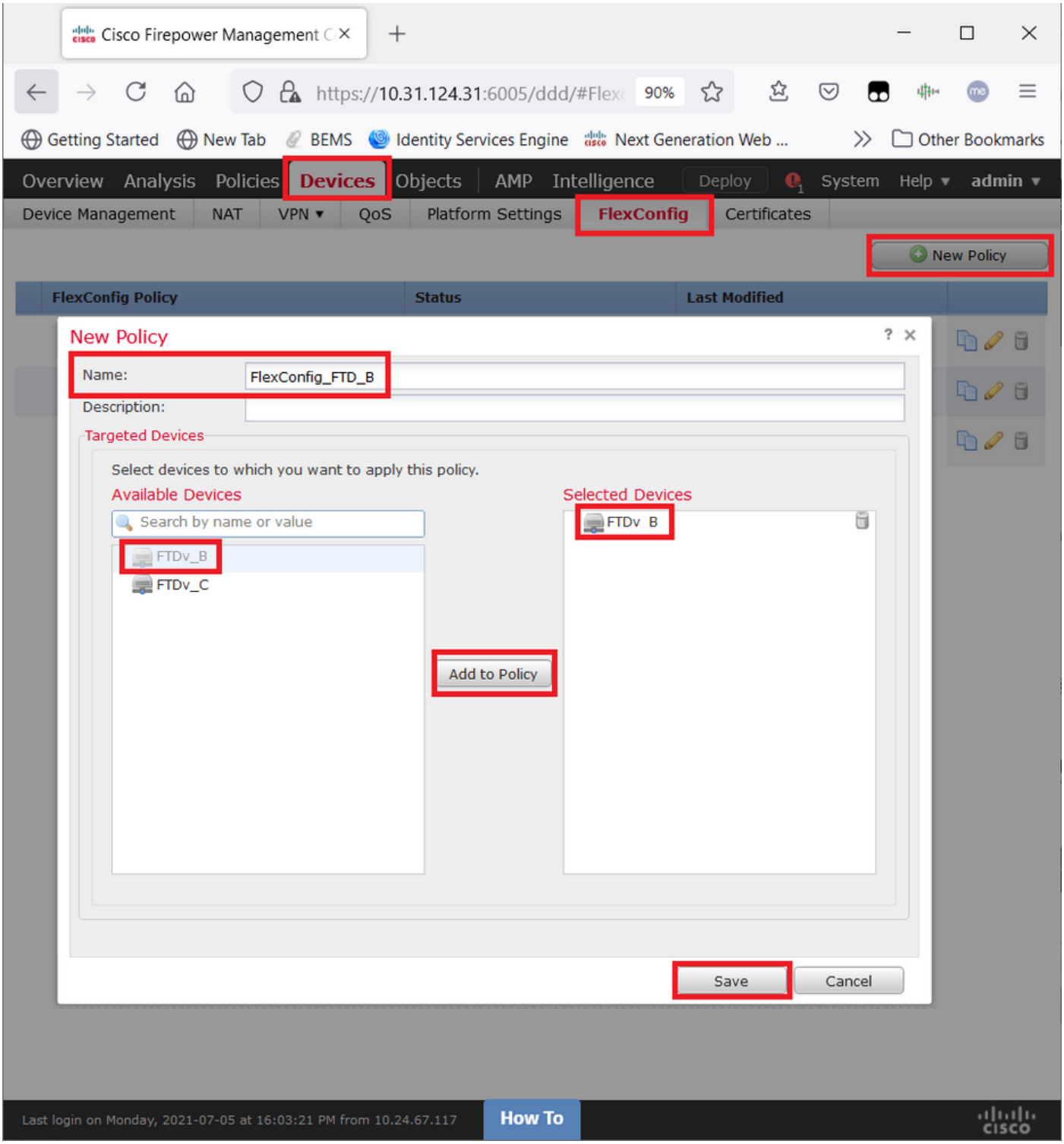
Informações de Apoio

Tanto o Internet Key Exchange versão 1 (IKEv1) como o Internet Key Exchange versão 2 (IKEv2) Policy Based (mapa de criptografia) VPNs site a site são túneis sob demanda. Por padrão, o FTD encerra a conexão VPN se não houver nenhuma atividade de comunicação no túnel em um determinado período chamado **vpn-idle-timeout**. Esse temporizador é definido como 30 minutos por padrão.

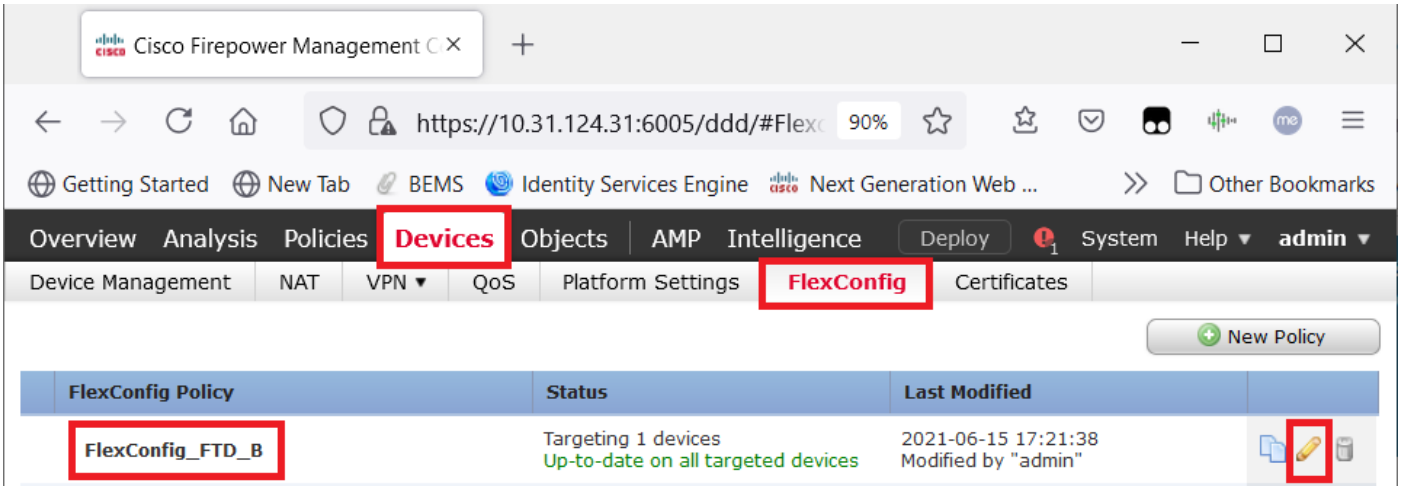
Configurar

Configurar a política FlexConfig e o objeto FlexConfig

Etapa 1. Em **Dispositivos > FlexConfig** crie uma nova política FlexConfig (se ainda não existir) e a anexe ao FTD onde a VPN de site a site está configurada.


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

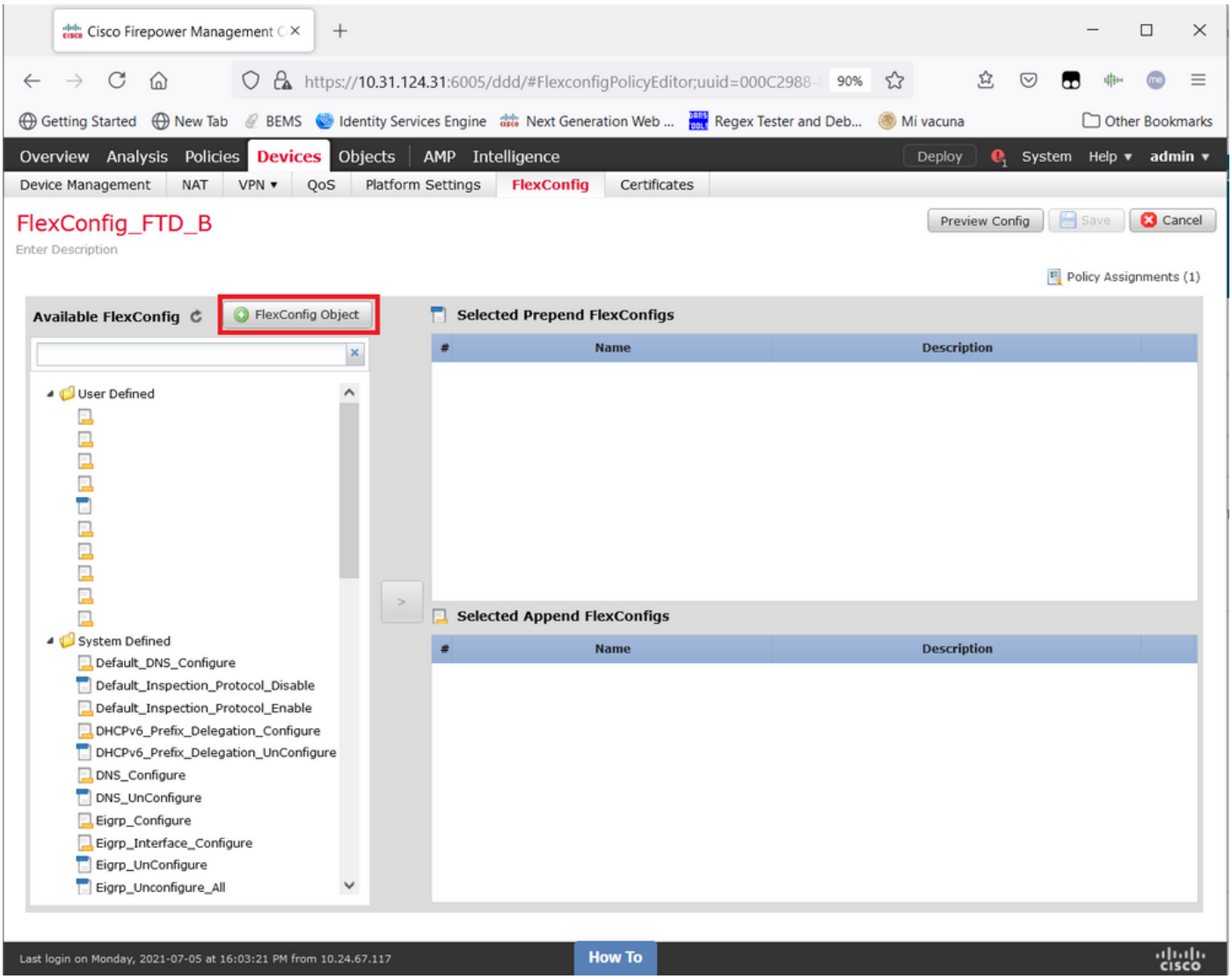
or

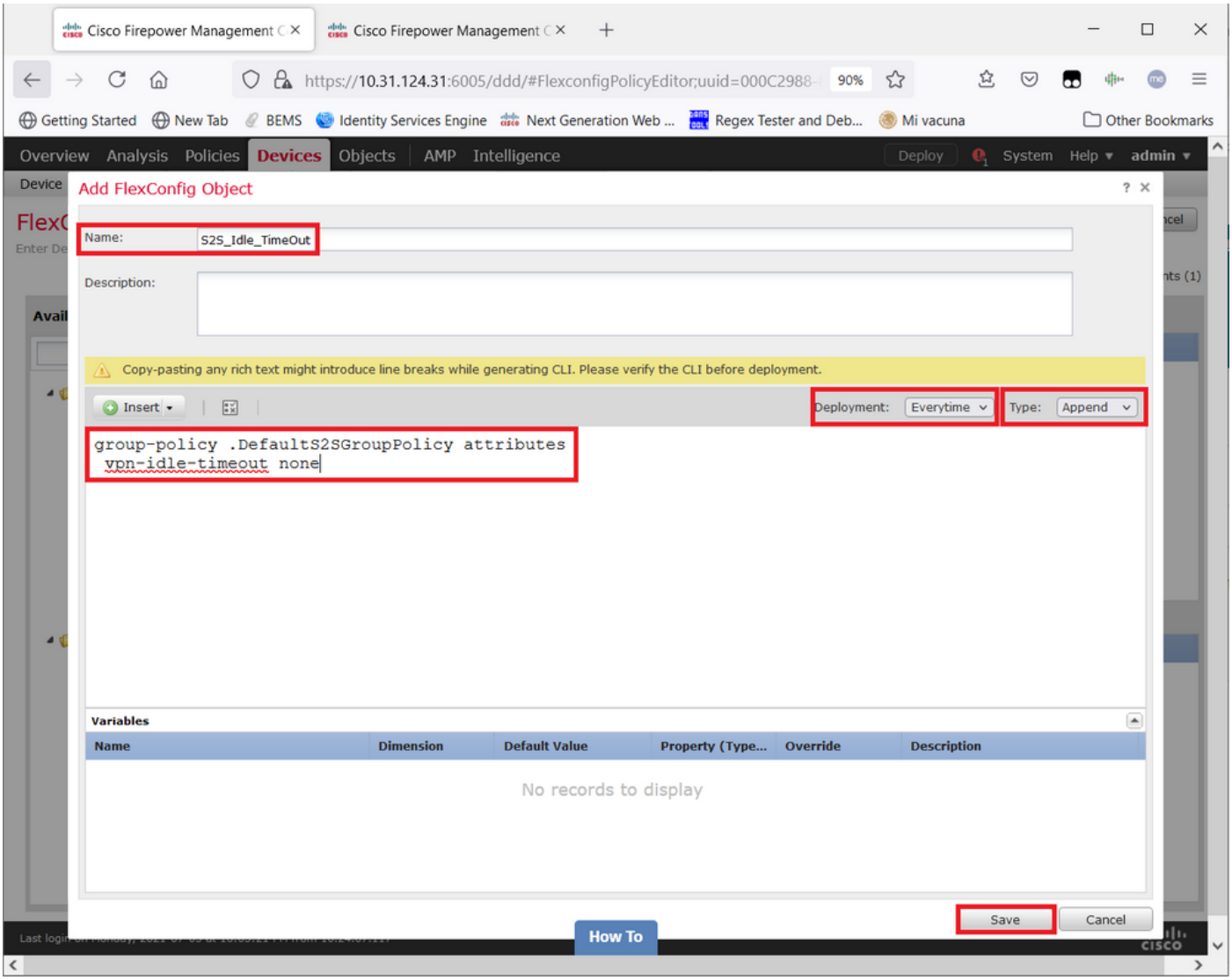


Etapa 2. Dentro dessa política, crie um **objeto FlexConfig** da seguinte maneira:

Nome: S2S_Idle_TimeOut
Implantação: Sempre
Digite: Acrescentar

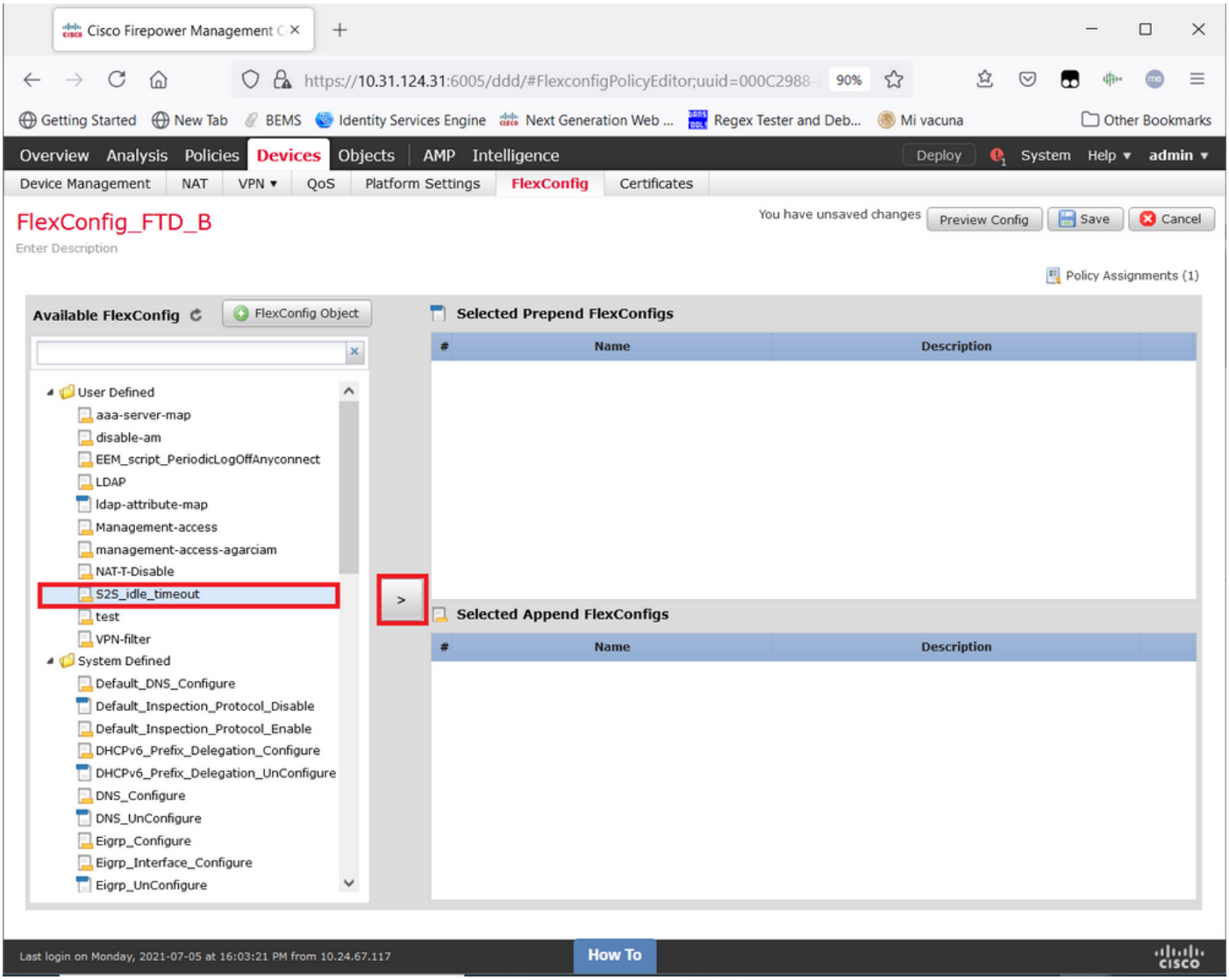
group-policy .DefaultS2SGroupPolicy atributos
vpn-idle-timeout none

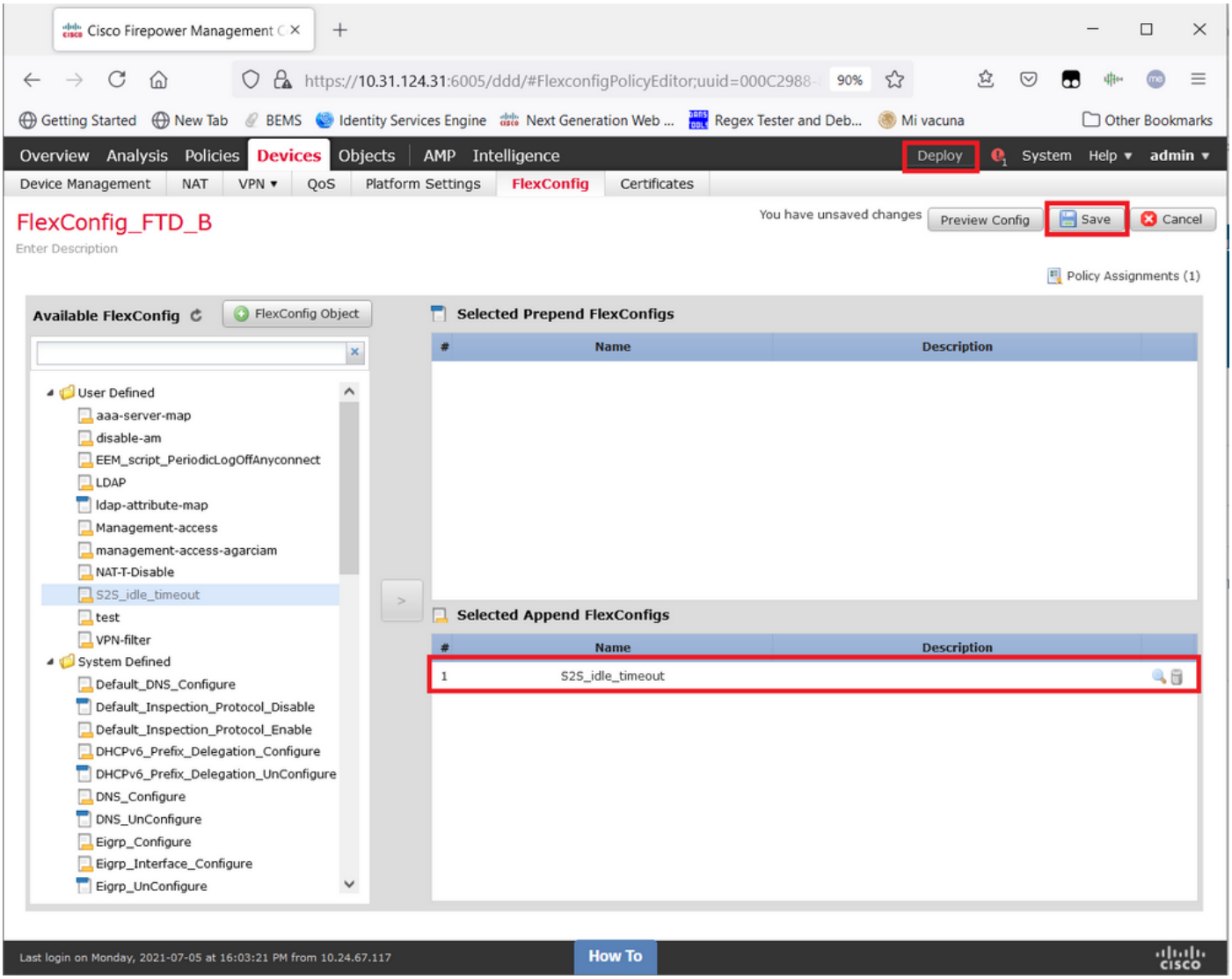




e **Salve**-o.

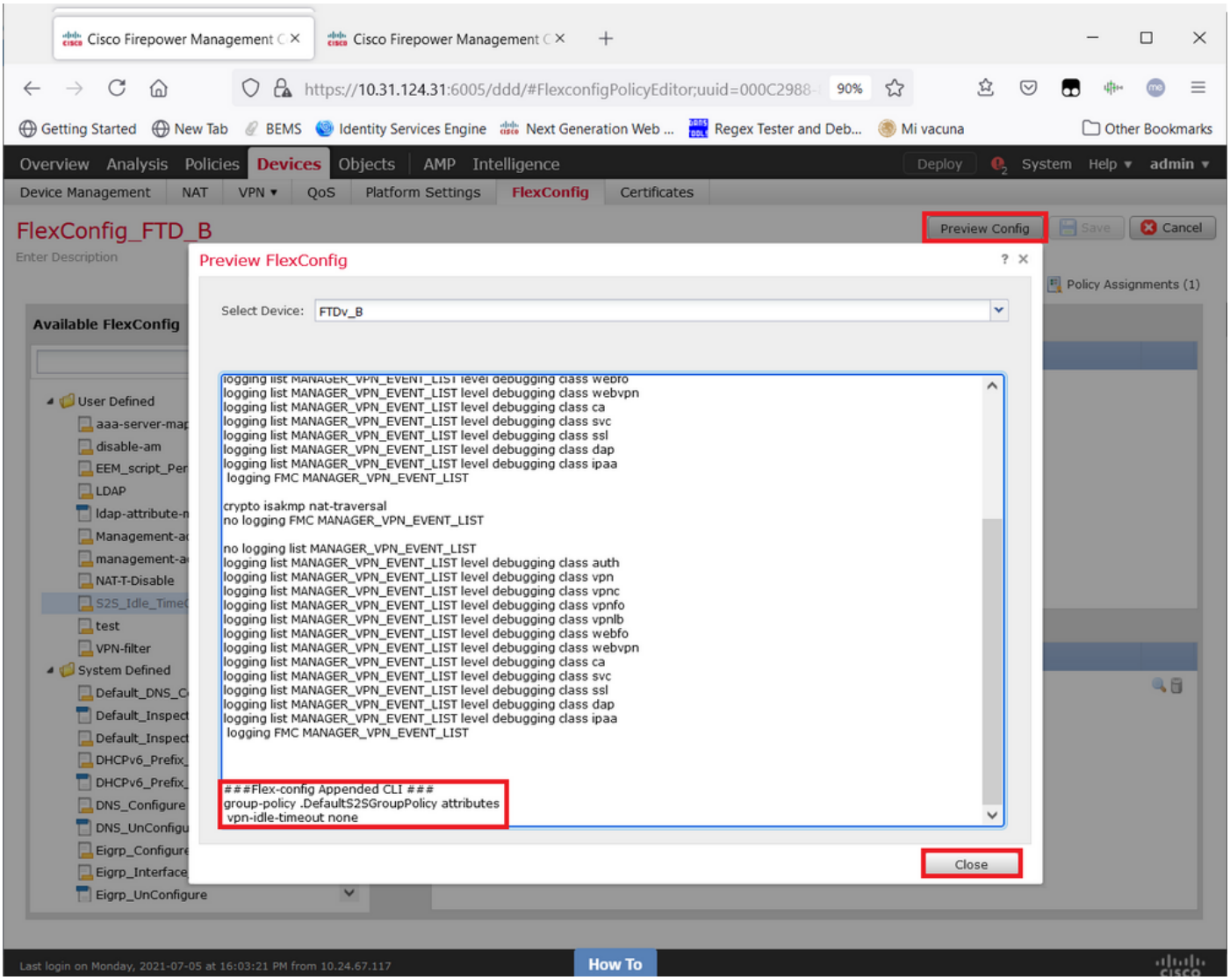
Etapa 3. No painel esquerdo, procure-o e arraste-o para o painel direito com o botão **>**.


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



Salve as alterações e **implemente**.

Etapa 3.1 (Opcional) Como etapa intermediária, depois que as alterações de configuração tiverem sido salvas, você poderá escolher **Preview Config** para garantir que os comandos FlexConfig estejam prontos para serem enviados no final da configuração.



Verificar

Quando a implantação estiver concluída, você poderá executar esse comando no LINA (**> system support diagnostic-cli**) para confirmar se a nova configuração está lá:

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

> **Caution**: Lembre-se de que essa alteração afeta todas as VPNs S2S no FTD. NÃO é uma configuração por túnel, mas global.

Mesmo que a configuração esteja lá, o túnel ativo precisa ser devolvido (**clear crypto ipsec sa peer** *<Remote_Peer_IP_Address>*) para que a alteração tenha efeito quando o túnel for estabelecido novamente. Você pode confirmar se a alteração está em vigor com 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
```

O contador *de tempo ocioso limite* deve ser definido como 0 minutos em vez de 30 minutos e a VPN deve permanecer ativa independentemente da atividade/tráfego sendo executado sobre ela.

> **Note**: No momento da escrita, existe um bug de aprimoramento para integrar a capacidade de modificar essa configuração diretamente no FMC sem a necessidade do Flexconfig. Consulte o bug da Cisco ID CSCvr82274 - ENH: torne o vpn-idle-timeout configurável

Troubleshoot

No momento, não há informações específicas disponíveis para solucionar problemas.

Informações Relacionadas

- Guia de Configuração do Firepower Management Center, Versão 7.0 - Capítulo: Políticas FlexConfig para Firepower Threat Defense
- Guia de Configuração do Firepower Management Center, Versão 7.0 - Capítulo: VPNs de site a site para Firepower Threat Defense
- Suporte Técnico e Documentação - Cisco Systems