Désactiver le délai d'inactivité du VPN site à site FTD avec les stratégies FlexConfig

Contenu

Introduction

Ce document décrit comment modifier l'attribut **vpn-idle-timeout** d'un VPN avec des stratégies FlexConfig dans Cisco Firepower Management Center (FMC) afin d'empêcher les temps d'arrêt du tunnel dus à l'inactivité ou au délai d'inactivité.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- FMC
- Stratégies FlexConfig
- Topologies VPN site à site

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

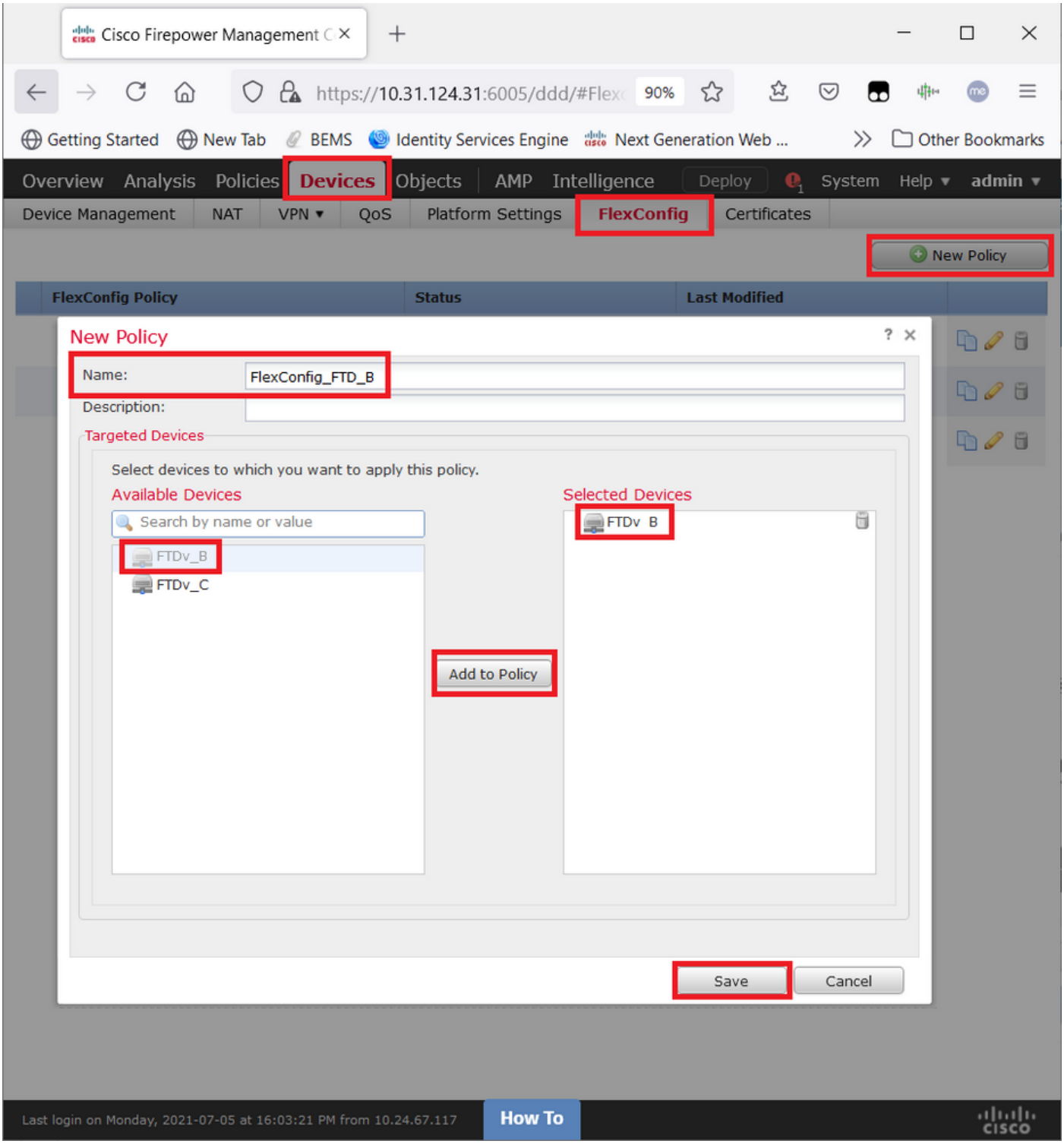
Informations générales

Les VPN de site à site basés sur une stratégie (Crypto map) d'échange de clés Internet version 1 (IKEv1) et de clé Internet version 2 (IKEv2) sont tous deux des tunnels à la demande. Par défaut, le FTD met fin à la connexion VPN s'il n'y a aucune activité de communication sur le tunnel dans une certaine période appelée **vpn-idle-timeout**. Ce compteur est défini sur 30 minutes par défaut.

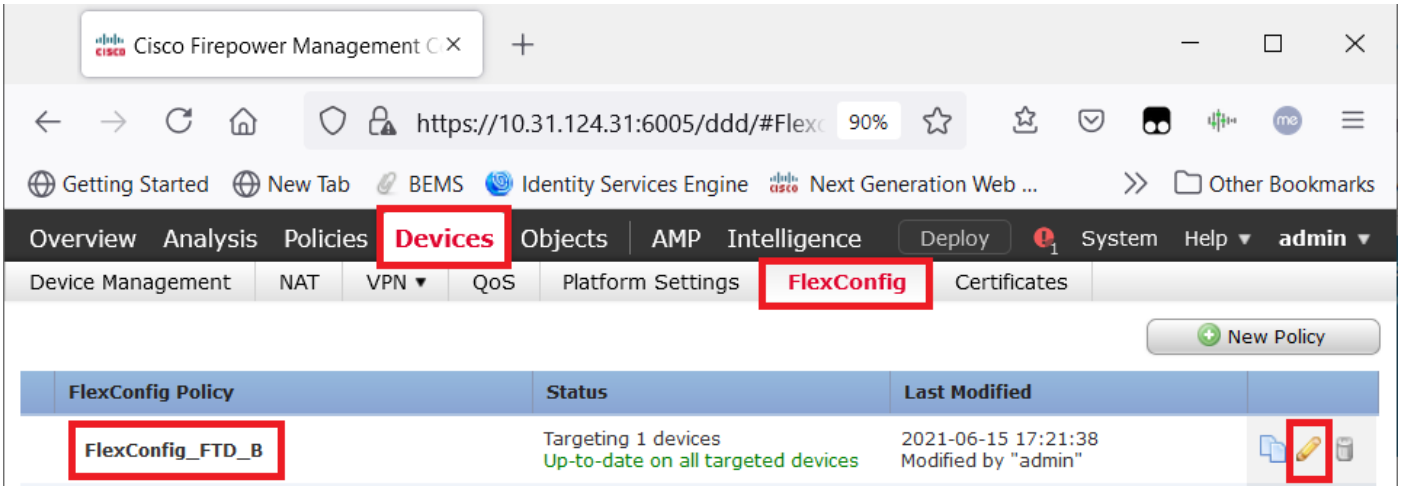
Configuration

Configurer la stratégie FlexConfig et l'objet FlexConfig

Étape 1. Sous **Devices > FlexConfig**, créez une nouvelle stratégie FlexConfig (si elle n'existe pas déjà) et associez-la au FTD où le VPN site à site est configuré.


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

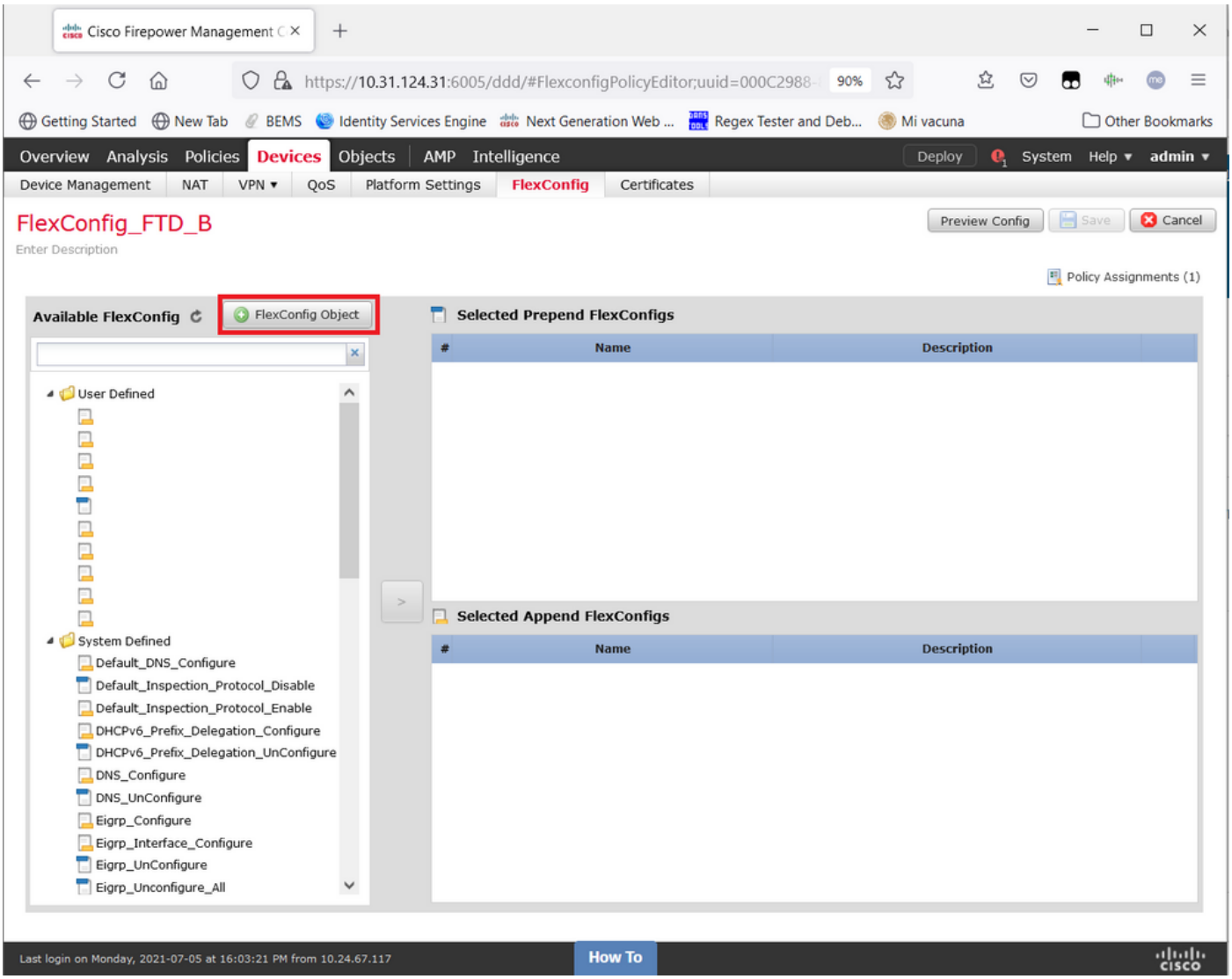
ou

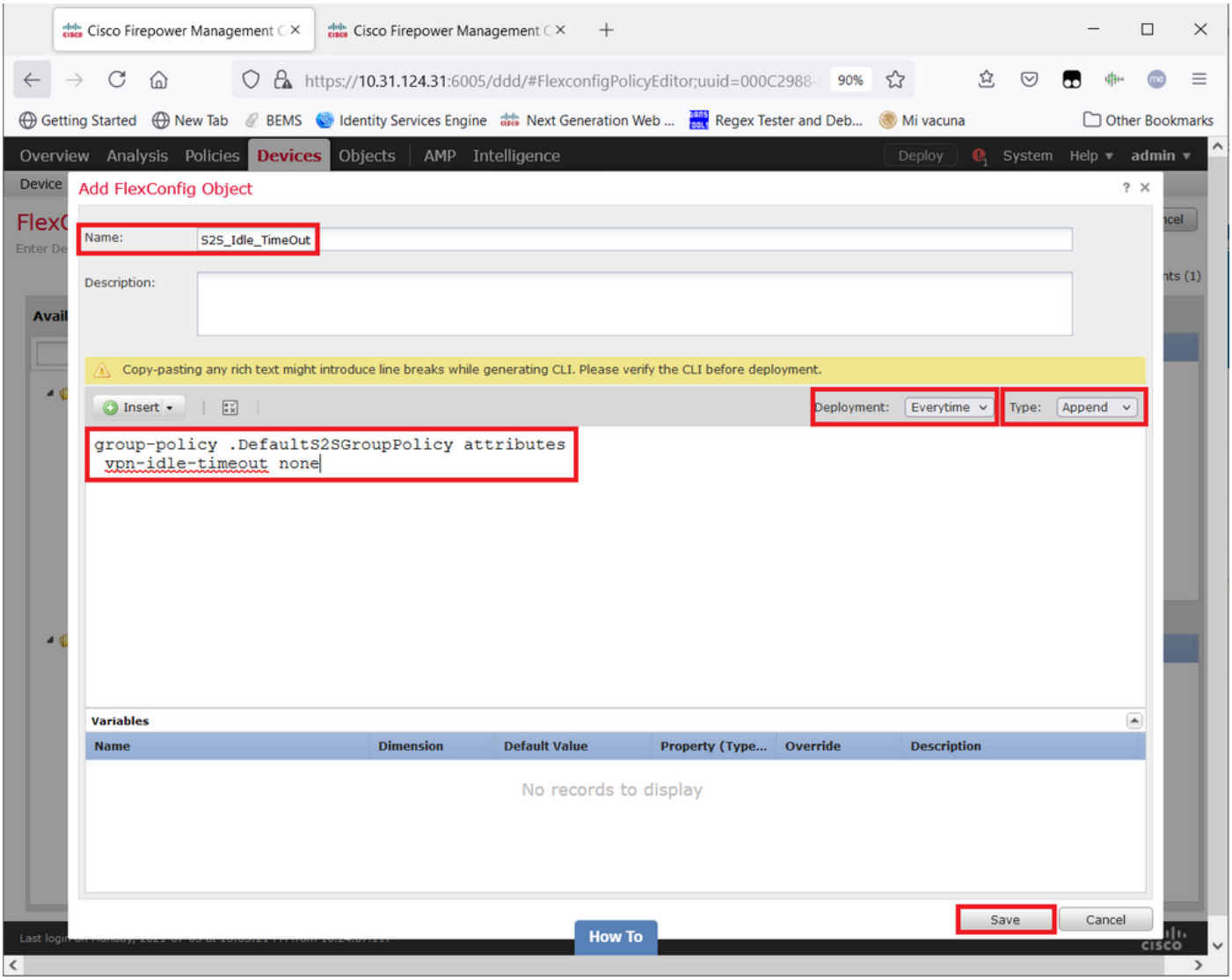


Étape 2. Dans cette stratégie, créez un **objet FlexConfig** comme suit :

Name : S2S_Délai_InactifSortant
Déploiement : Partout
type : Ajouter

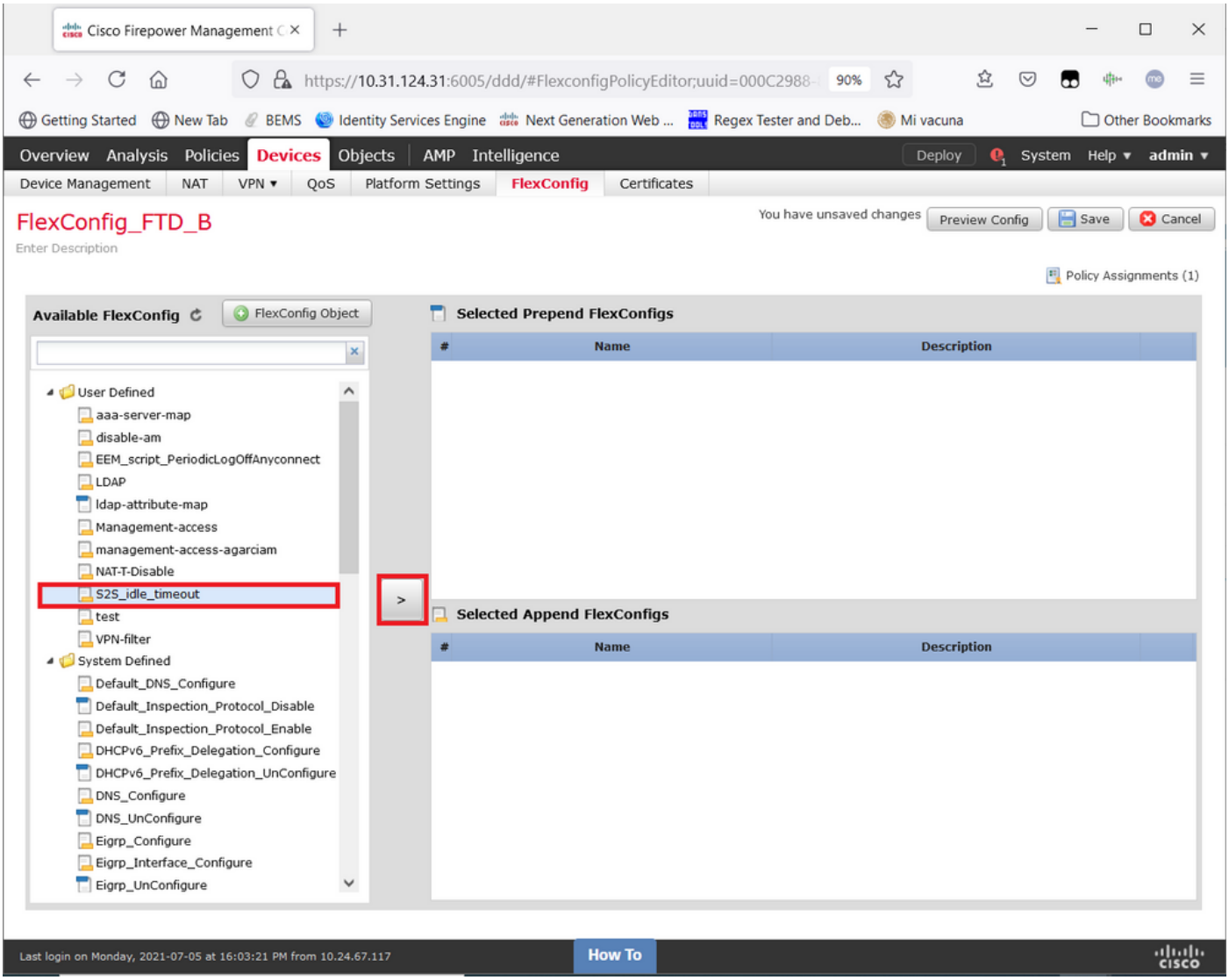
group-policy .DefaultS2SGroupPolicy attributs
vpn-idle-timeout none

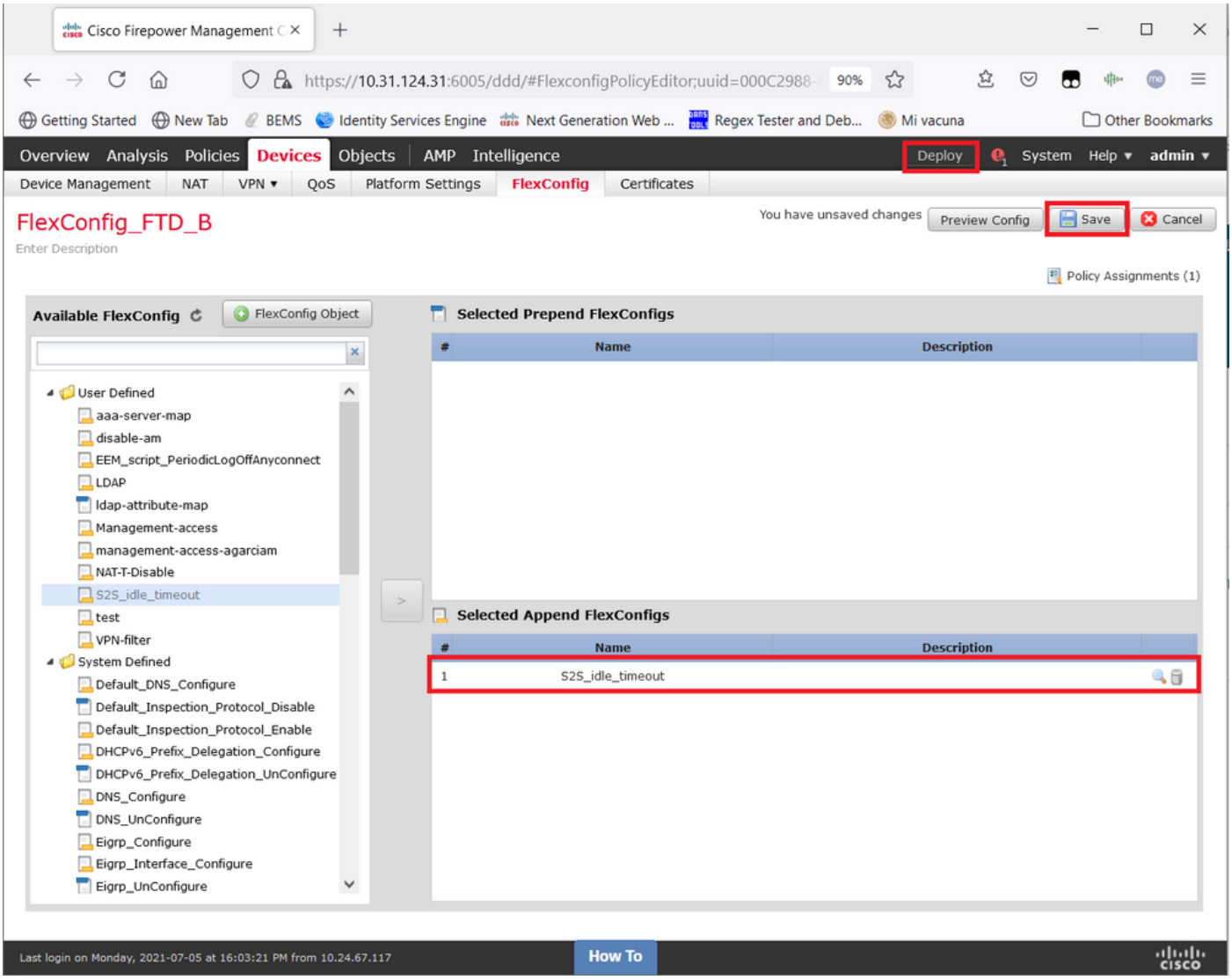




et **enregistrez**-le.

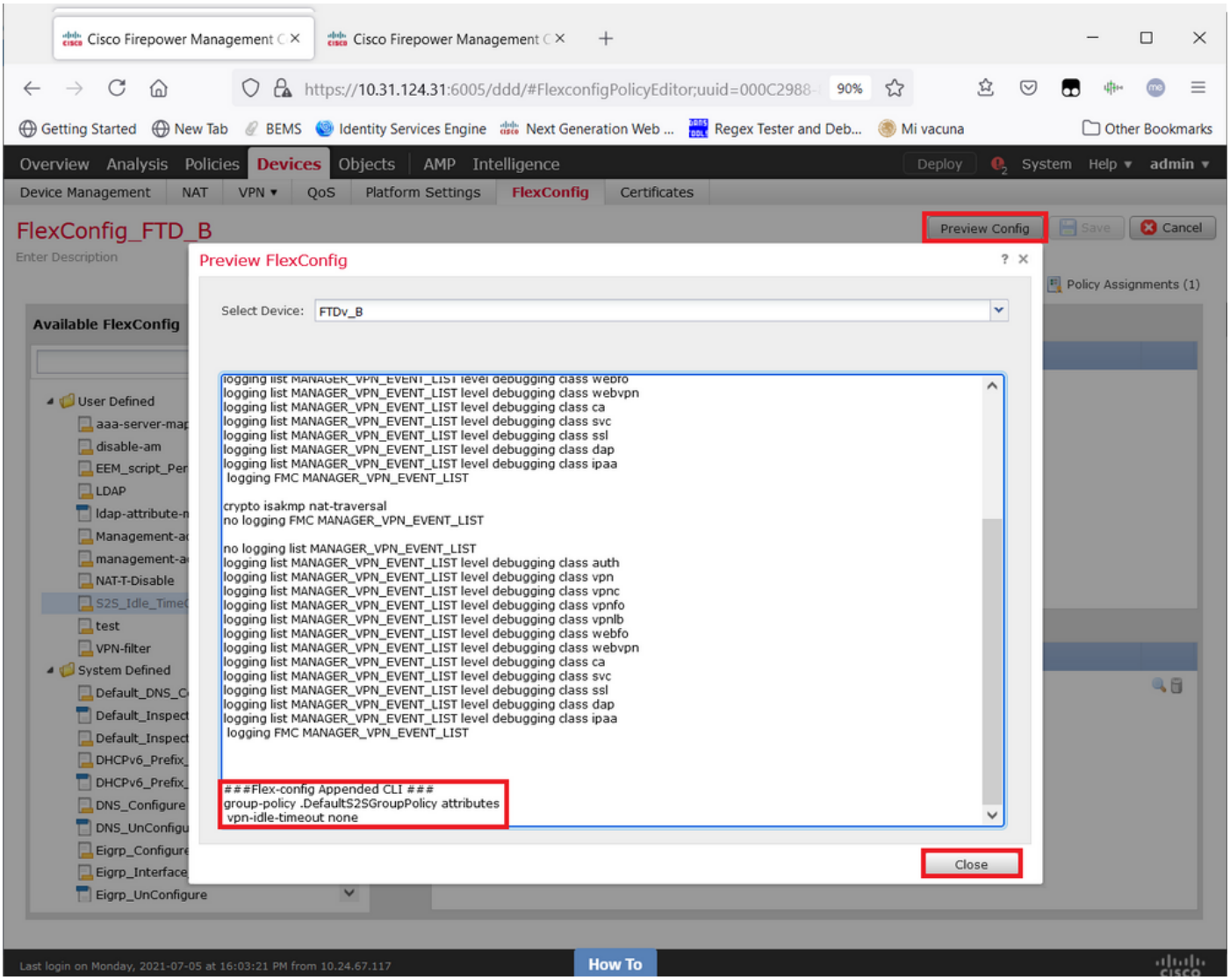
Étape 3. Dans le volet gauche, recherchez-le et faites-le glisser vers le volet droit à l'aide du bouton **>**.


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



Enregistrez les modifications et **Déployez**.

Étape 3.1 (Facultatif) En tant qu'étape intermédiaire, après avoir enregistré les modifications de configuration, vous pouvez choisir **Preview Config** afin de vous assurer que les commandes FlexConfig sont prêtes à être poussées à la fin de la configuration.



Vérification

Une fois le déploiement terminé, vous pouvez exécuter cette commande dans LINA (**> system support diagnostic-cli**) afin de confirmer la nouvelle configuration :

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

> **Attention** : Gardez à l'esprit que cette modification affecte tous les VPN S2S sur le FTD. Il ne s'agit PAS d'un paramètre par tunnel mais d'un paramètre global.

Même si la configuration est présente, le tunnel actif doit être renvoyé (**clear crypto ipsec sa peer** *<Remote_Peer_IP_Address>*) afin que la modification prenne effet lorsque le tunnel est rétabli. Vous pouvez confirmer que la modification est en vigueur avec cette commande :

```
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
```

Le compteur *de temps d'inactivité* doit être défini sur 0 minute au lieu de 30 minutes et le VPN doit rester actif indépendamment de l'activité/trafic qui le traverse.

> **Note**: Au moment de l'écriture, il existe un bogue d'amélioration pour intégrer la possibilité de modifier ce paramètre directement sur FMC sans avoir besoin de Flexconfig. Voir l'ID de bogue Cisco CSCvr82274 - ENH : rendre le vpn-idle-timeout configurable

Dépannage

Aucune information spécifique n'est actuellement disponible pour le dépannage.

Informations connexes

- Guide de configuration de Firepower Management Center, version 7.0 - Chapitre : Stratégies FlexConfig pour la défense contre les menaces Firepower
- Guide de configuration de Firepower Management Center, version 7.0 - Chapitre : VPN site à site pour la défense contre les menaces Firepower
- Support et documentation techniques - Cisco Systems