Time-out bij inactiviteitstimer van FTD Site-to-Site VPN met beleid van FlexConfig

Inhoud

Inleiding

Dit document beschrijft hoe de **VPN-**eigenschap **inactiviteitstimer** van een VPN met FlexConfig-beleid in Cisco Firepower Management Center (FMC) kan worden gewijzigd om tunneldowntime te voorkomen als gevolg van inactiviteit of inactiviteitstimer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defense (FTD)
- FMC
- FlexConfig-beleid
- Site-to-Site VPN-topologieën

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- FMCv - 6.5.0.4 (bouw 57)
- FTDv - 6.4.0.10 (bouw 95)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

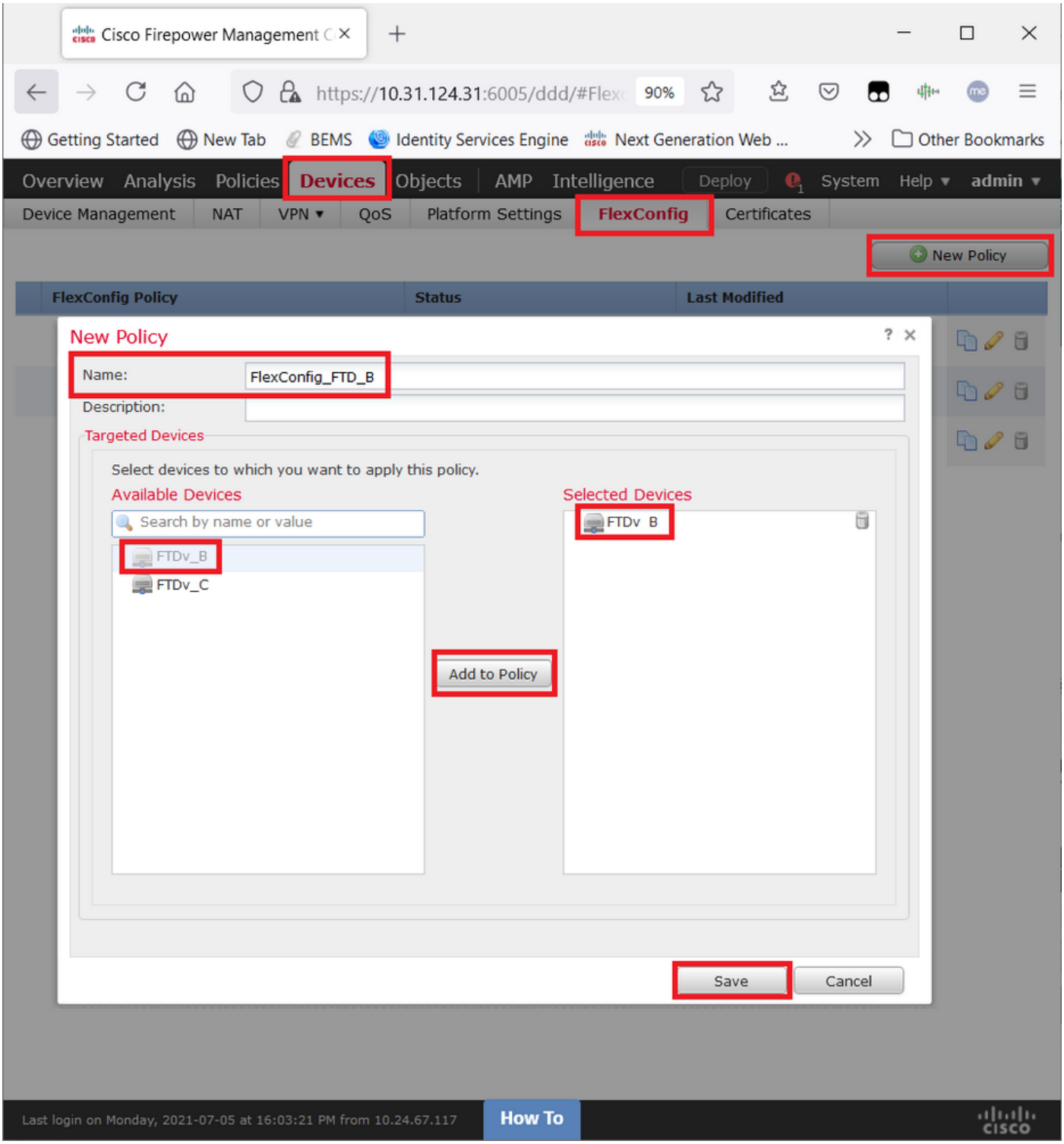
Achtergrondinformatie

Zowel site-to-site VPN's zijn op bestelling gebaseerde tunnels, versie 1 (IKEv1) van Internet Key Exchange en versie 2 (IKEv2) van Internet Key Exchange (Crypto-kaart). Standaard beëindigt de FTD de VPN-verbinding als er geen communicatieactiviteit over de tunnel is in een bepaalde periode die **vpn-inactiviteitstimer** wordt genoemd. Deze timer wordt standaard ingesteld op 30 minuten.

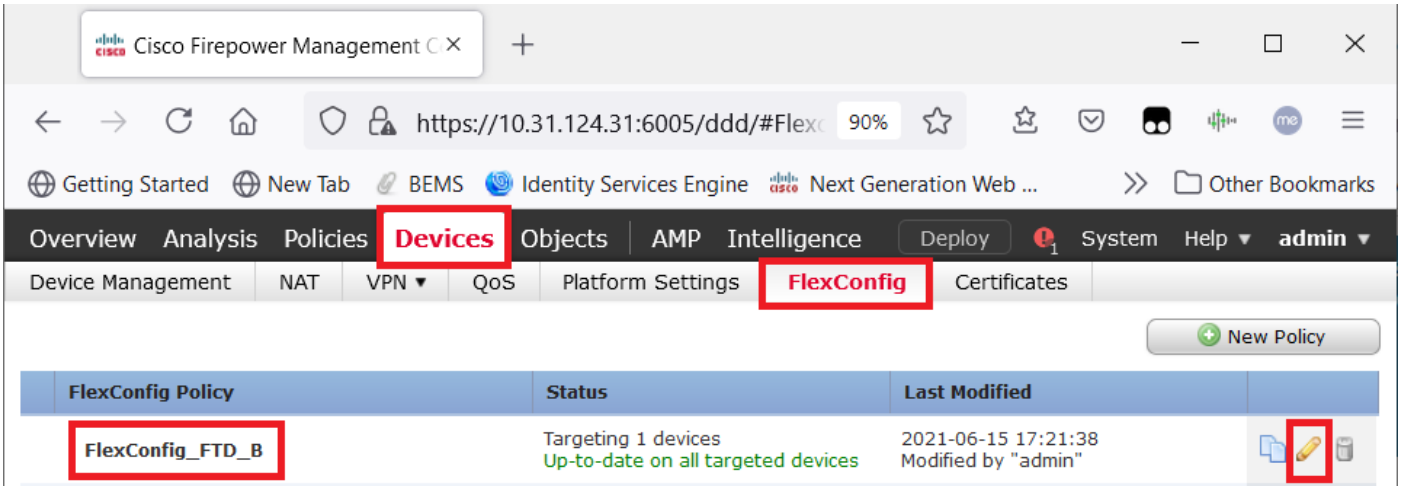
Configureren

FlexConfig-beleid en FlexConfig-object

Stap 1. Onder **Apparaten > FlexConfig** maakt u een nieuw FlexConfig-beleid (als dit niet reeds bestaat) en sluit het beleid aan op de FTD waar de Site-to-Site VPN is geconfigureerd.


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

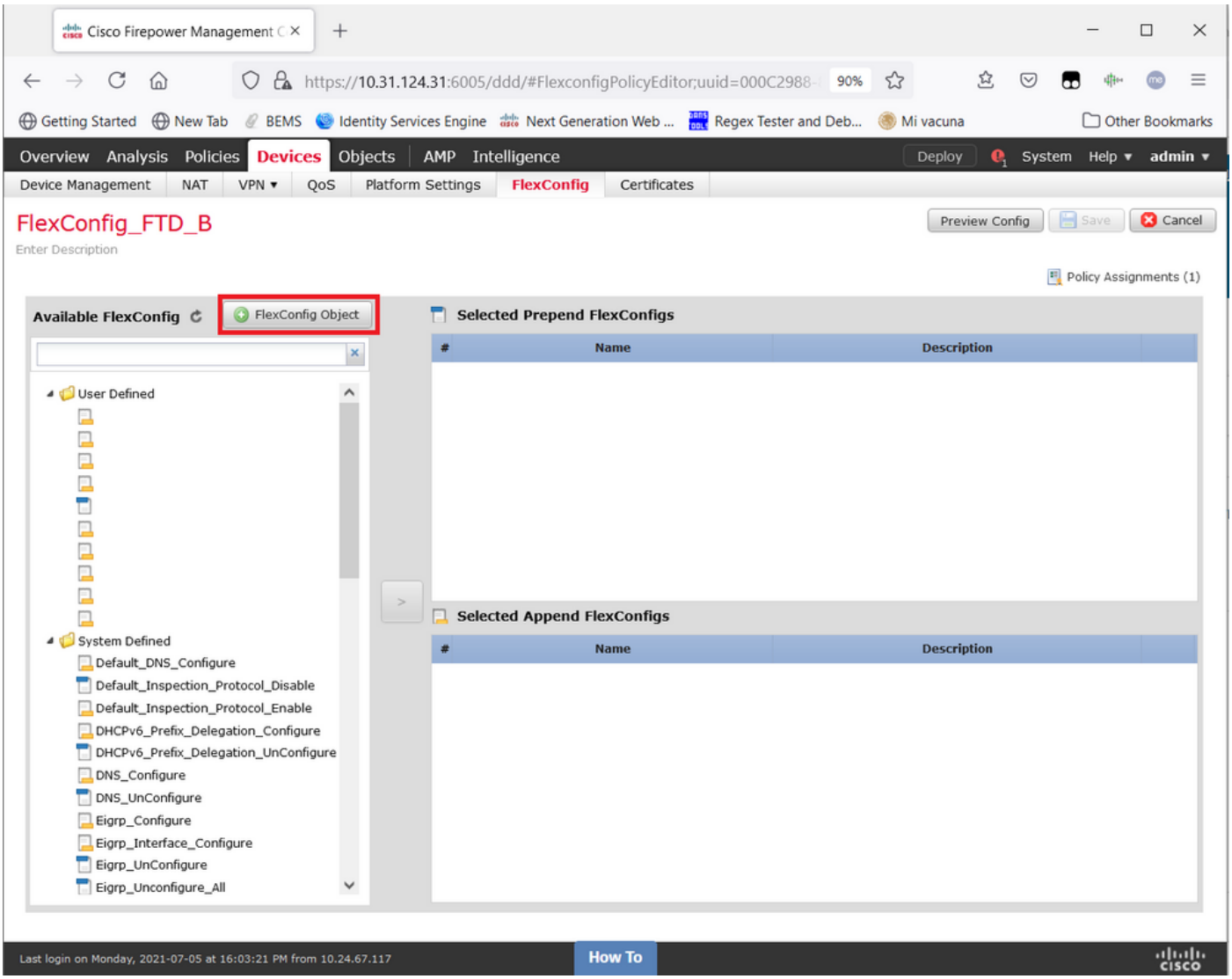
of

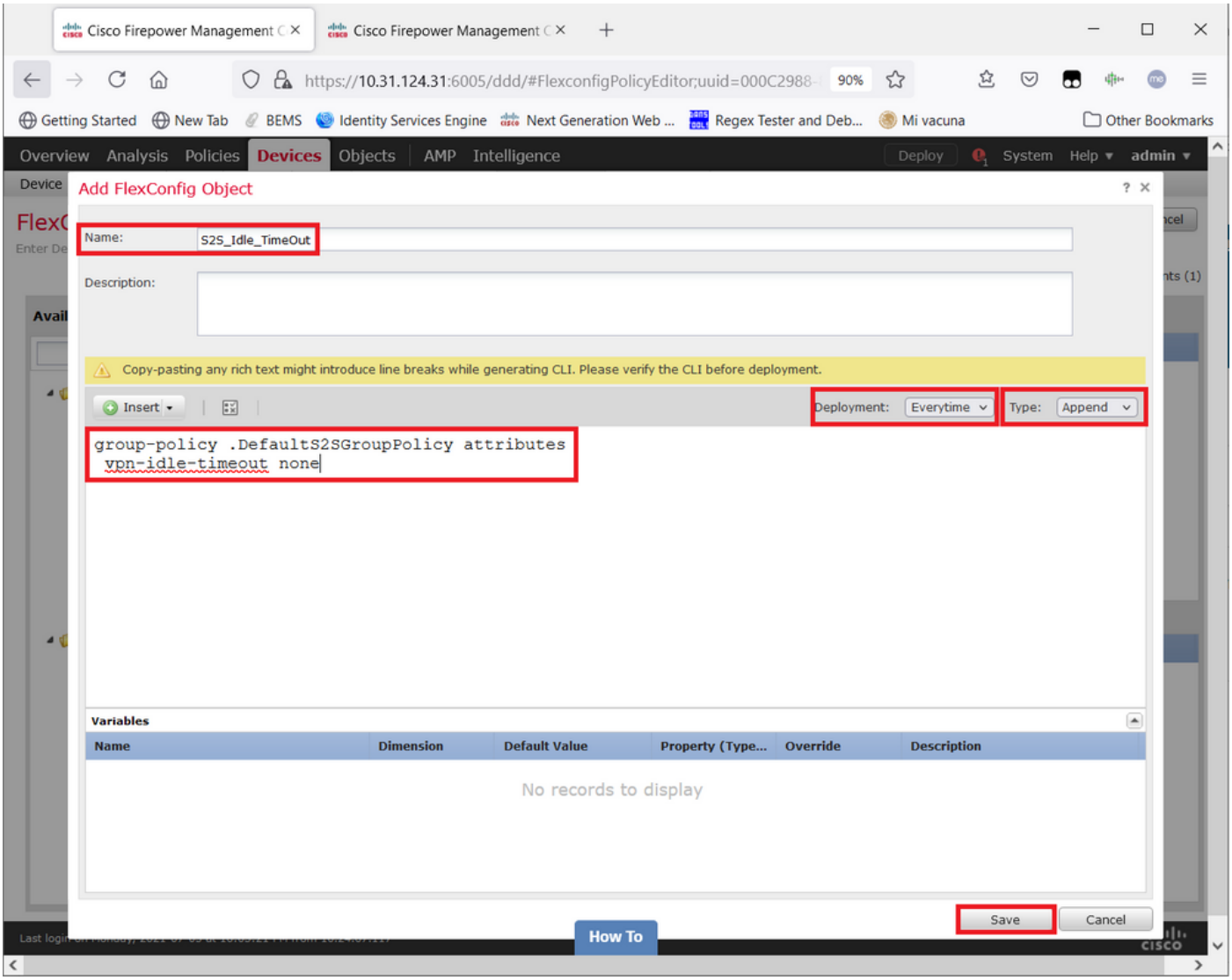


Stap 2. In dat beleid wordt als volgt een **FlexConfig-object** gemaakt:

Name: S2S_inactiviteitstimer_time-out
Inzet: alledaags
Type: toevoegen

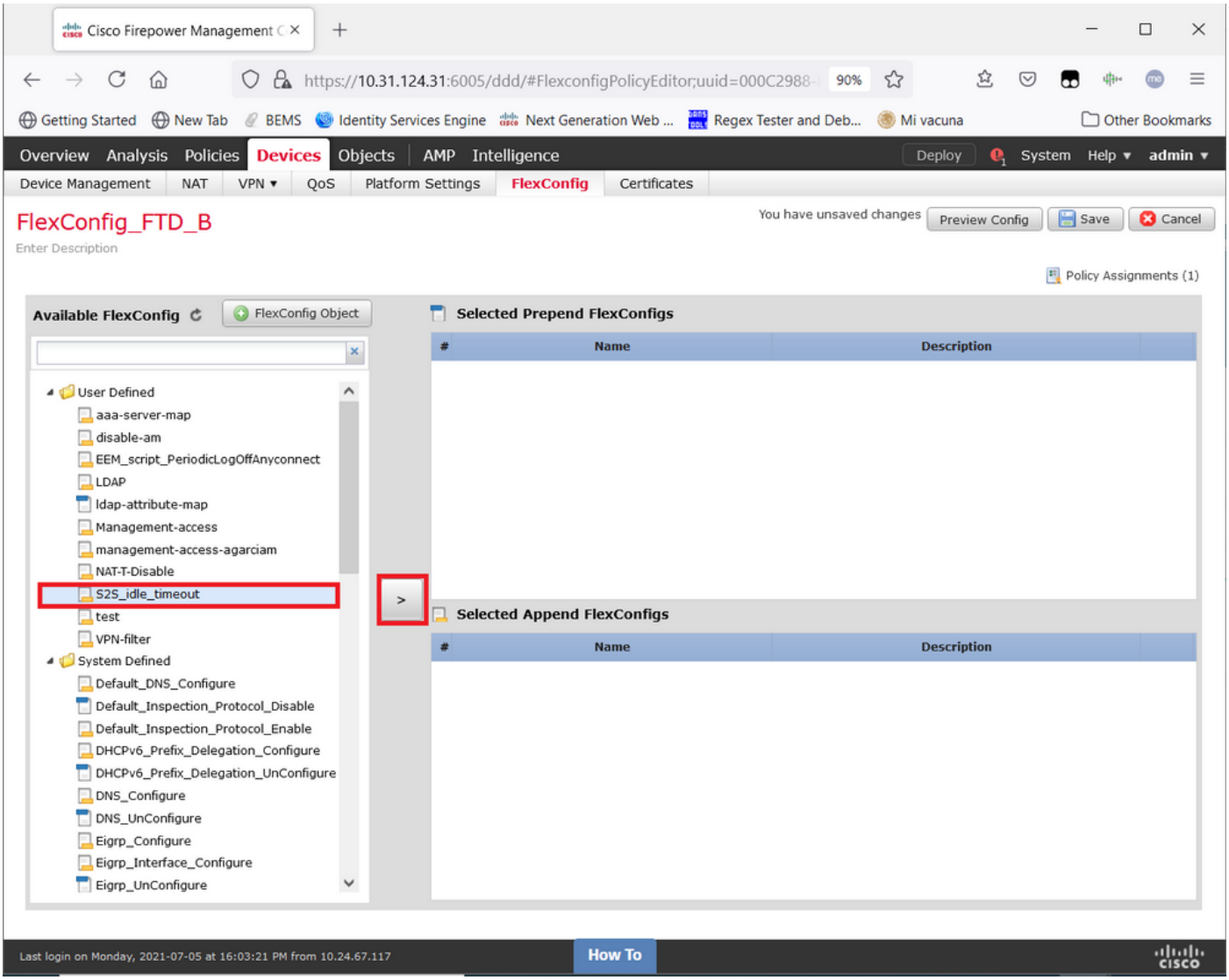
groepsbeleid .DefaultS2SGroupPolicy-eigenschappen
VPN zonder tussenkomst

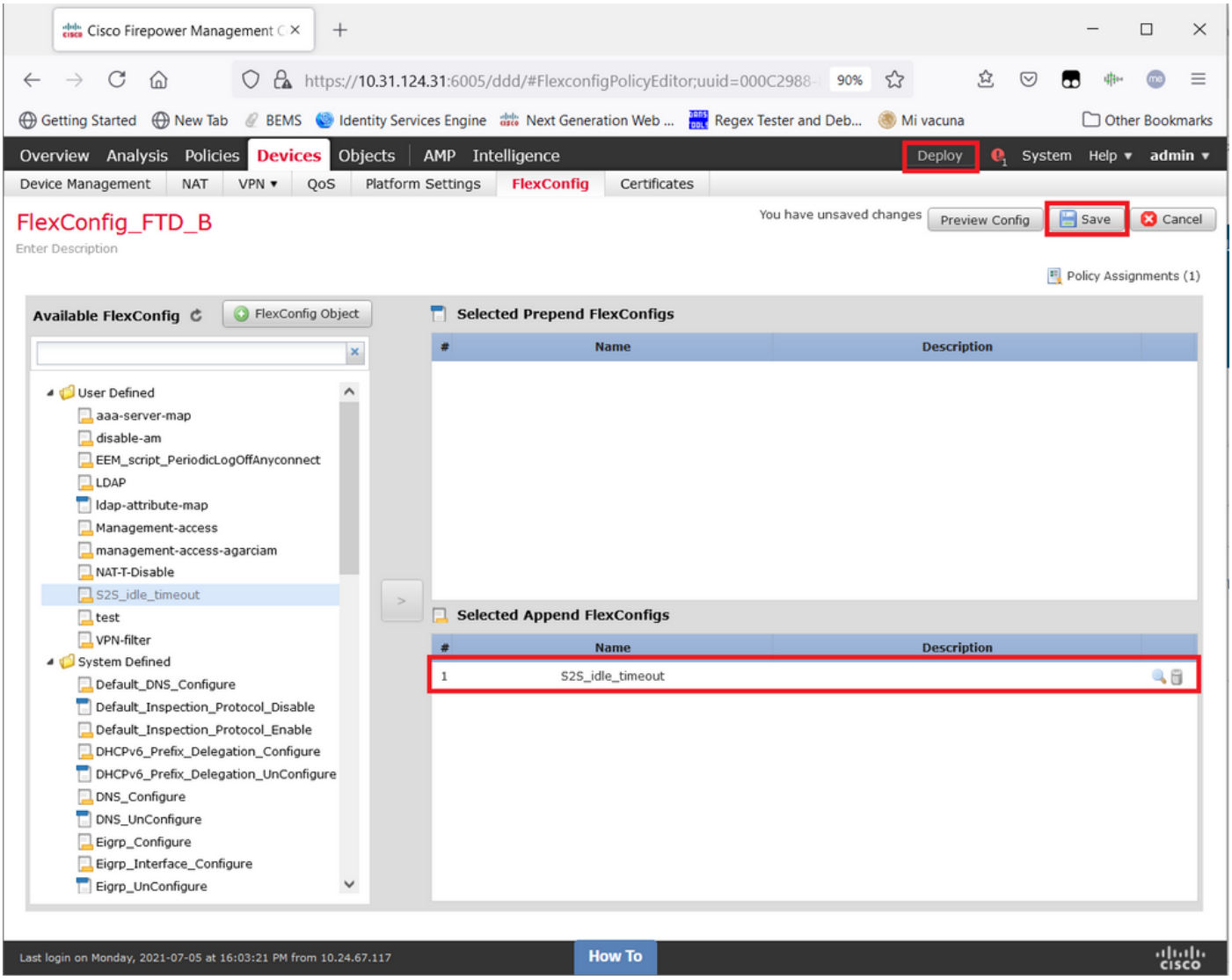




en **red** het.

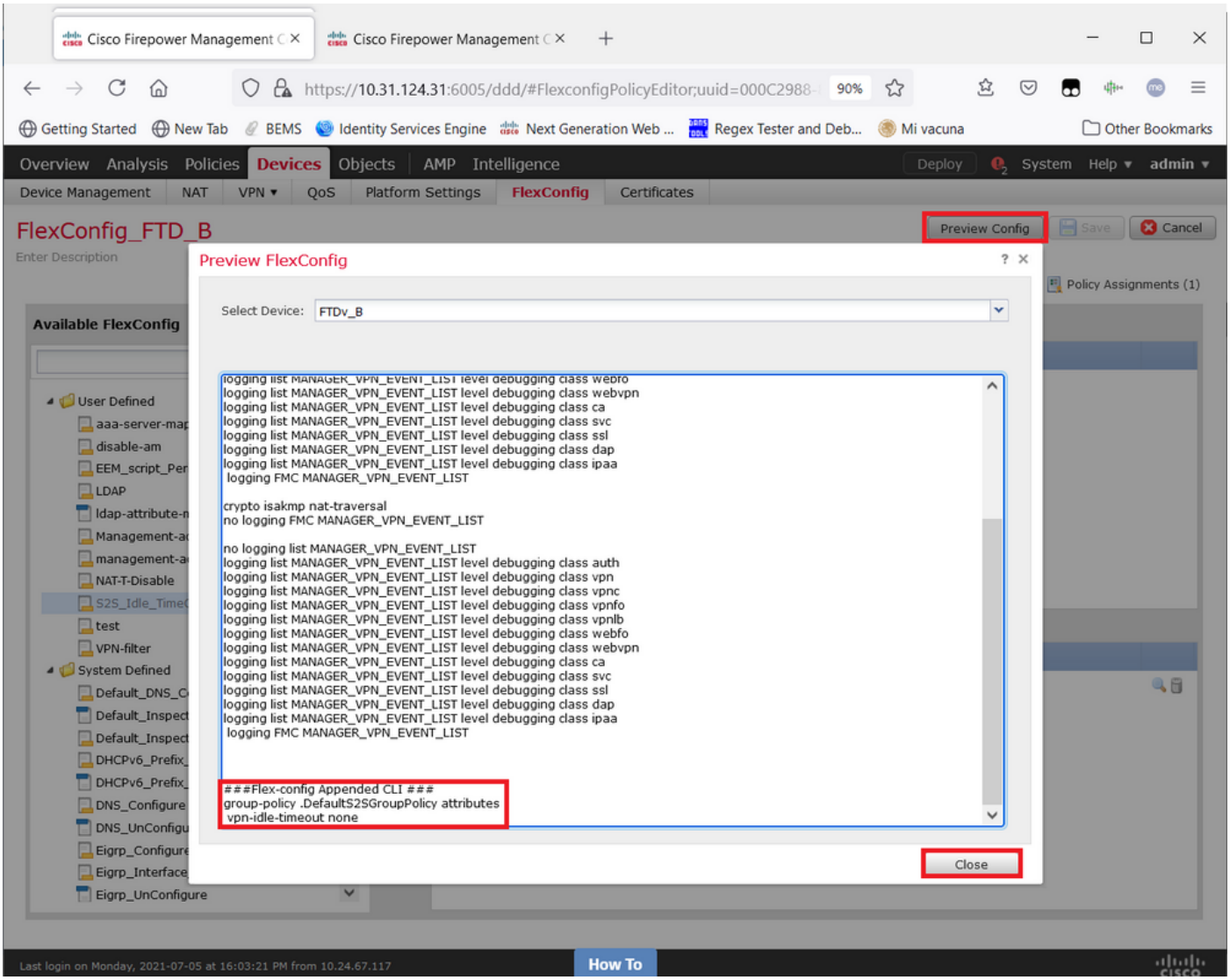
Stap 3. Zoek in het linker deelvenster naar deze en sleep deze met de knop naar het rechter deelvenster **>**.


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



Sla de wijzigingen **op** en **implementeer**.

Stap 3.1 (optioneel) Als tussenstap, nadat de configuratiewijzigingen zijn opgeslagen, kunt u **Preview Config** kiezen om er zeker van te zijn dat de opdrachten FlexConfig klaar zijn om aan het eind van de configuratie te worden geduwd.



Verifiëren

Nadat de implementatie is voltooid, kunt u deze opdracht in LINA (**> systeemondersteuning voor diagnostische CLI**) uitvoeren om te bevestigen dat de nieuwe configuratie er is:

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

> **Voorzichtig:** Houd in gedachten dat deze verandering alle S2S VPN's op de FTD beïnvloedt. Het is GEEN instelling per tunnel maar een mondiale.

Ook al is de configuratie er, de actieve tunnel moet worden uitgezet (**duidelijke crypto ipsec als peer**<Remote_Peer_IP_Address>) zodat de verandering van kracht wordt wanneer de tunnel opnieuw wordt ingericht. U kunt bevestigen dat de wijziging met deze opdracht van kracht is:

```
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
```

De inactiviteitstimer van de uitloop moet op 0 minuten worden ingesteld in plaats van op 30 minuten en de VPN moet actief blijven, ongeacht de activiteit/het verkeer dat erover wordt uitgevoerd.

> **Opmerking:** Op het moment van schrijven bestaat er een Verbeteringsknuppel om het vermogen te integreren om deze instelling direct op FMC aan te passen zonder de noodzaak van Flexstack. Zie Cisco bug-ID CSCvr8274 - ENH: de vpn-tijdelijke oplossing configureerbaar maken

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar voor probleemoplossing.

Gerelateerde informatie

- Firepower Management Center Configuration Guide, versie 7.0 - hoofdstuk: FlexConfig-beleid voor FirePOWER-bedreigingsverdediging
- Firepower Management Center Configuration Guide, versie 7.0 - hoofdstuk: Site-to-Site VPN's voor FirePOWER Threat Defense
- Technische ondersteuning en documentatie – Cisco Systems