Disabilita timeout di inattività VPN da sito a sito FTD con criteri FlexConfig

Sommario

Introduzione

In questo documento viene descritto come modificare l'attributo **vpn-idle-timeout** di una VPN con criteri FlexConfig in Cisco Firepower Management Center (FMC) per evitare il downtime del tunnel dovuto a inattività o timeout di inattività.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense (FTD)
- CCP
- Criteri FlexConfig
- Topologie VPN da sito a sito

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

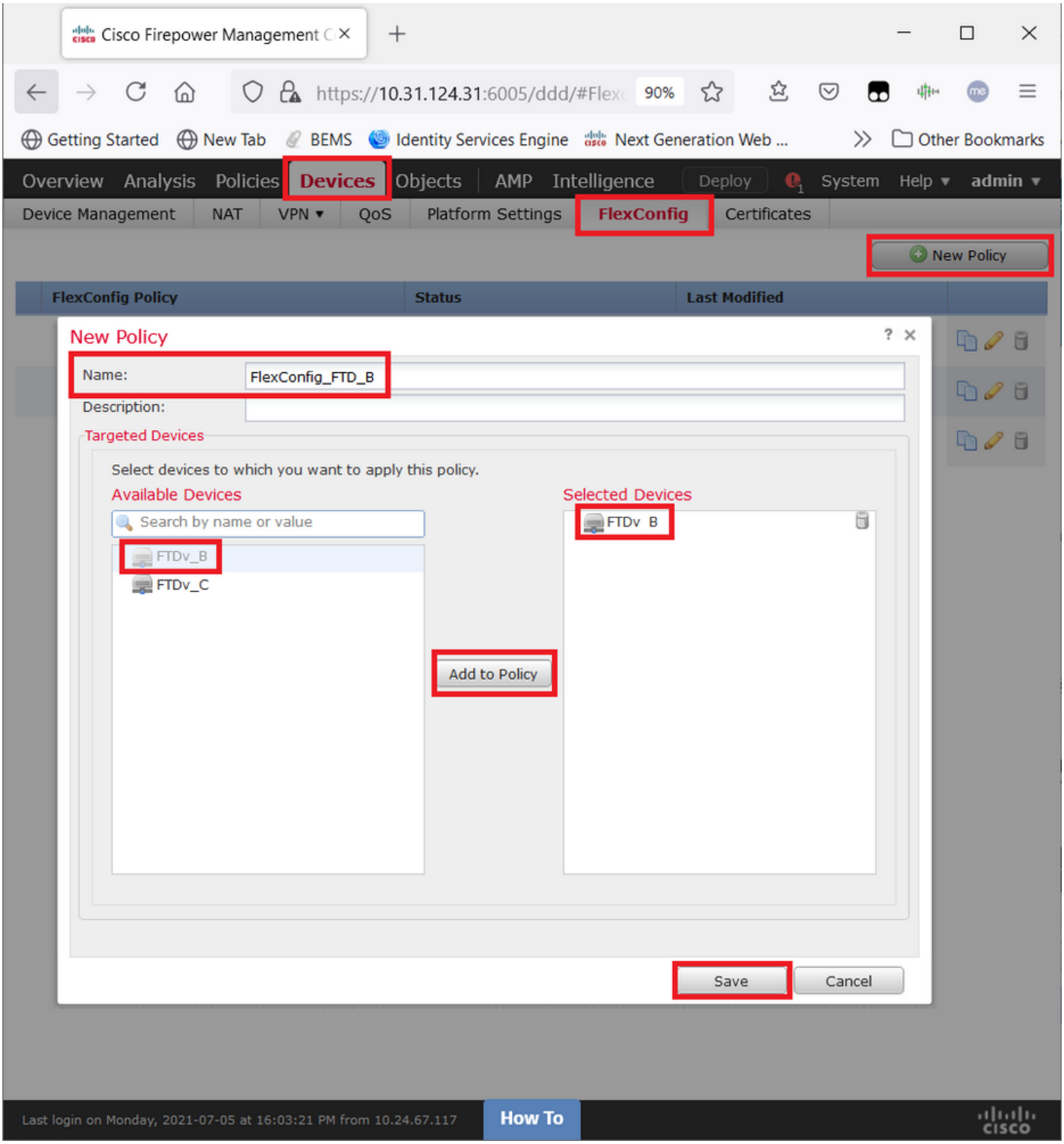
Premesse

Le VPN da sito a sito basate su policy (mappa crittografica) di Internet Key Exchange versione 1 (IKEv1) e Internet Key Exchange versione 2 (IKEv2) sono entrambe tunnel su richiesta. Per impostazione predefinita, l'FTD termina la connessione VPN se non vi è attività di comunicazione sul tunnel in un determinato periodo di tempo chiamato **vpn-idle-timeout**. Per impostazione predefinita, questo timer è impostato su 30 minuti.

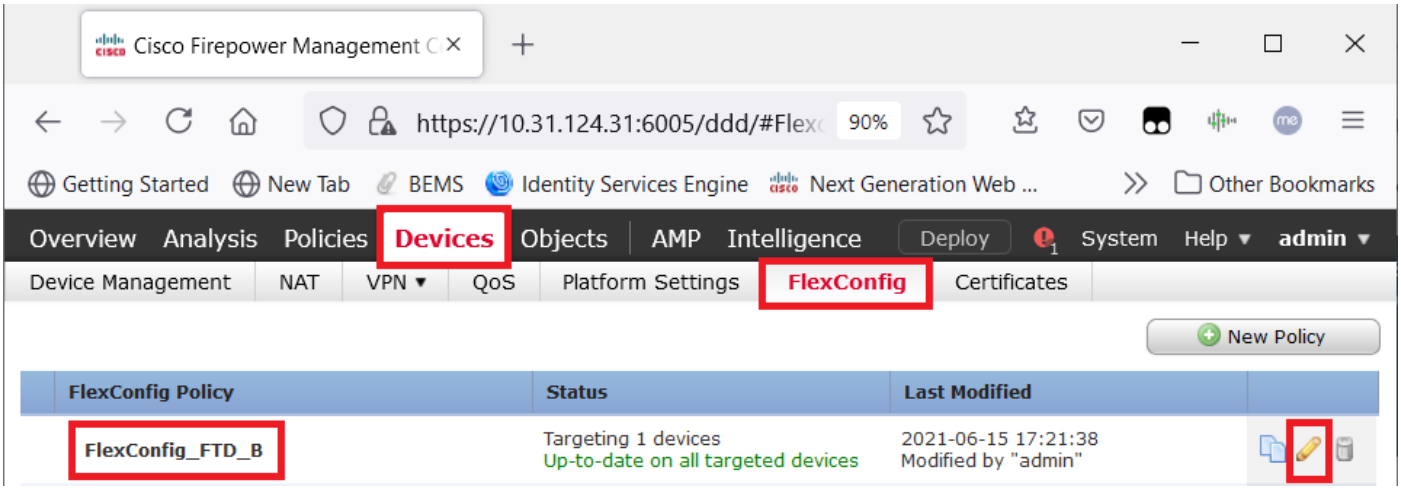
Configurazione

Configura criteri FlexConfig e oggetto FlexConfig

Passaggio 1. In **Dispositivi > FlexConfig** creare un nuovo criterio FlexConfig (se non ne esiste già uno) e collegarlo all'FTD in cui è configurata la VPN da sito a sito.


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

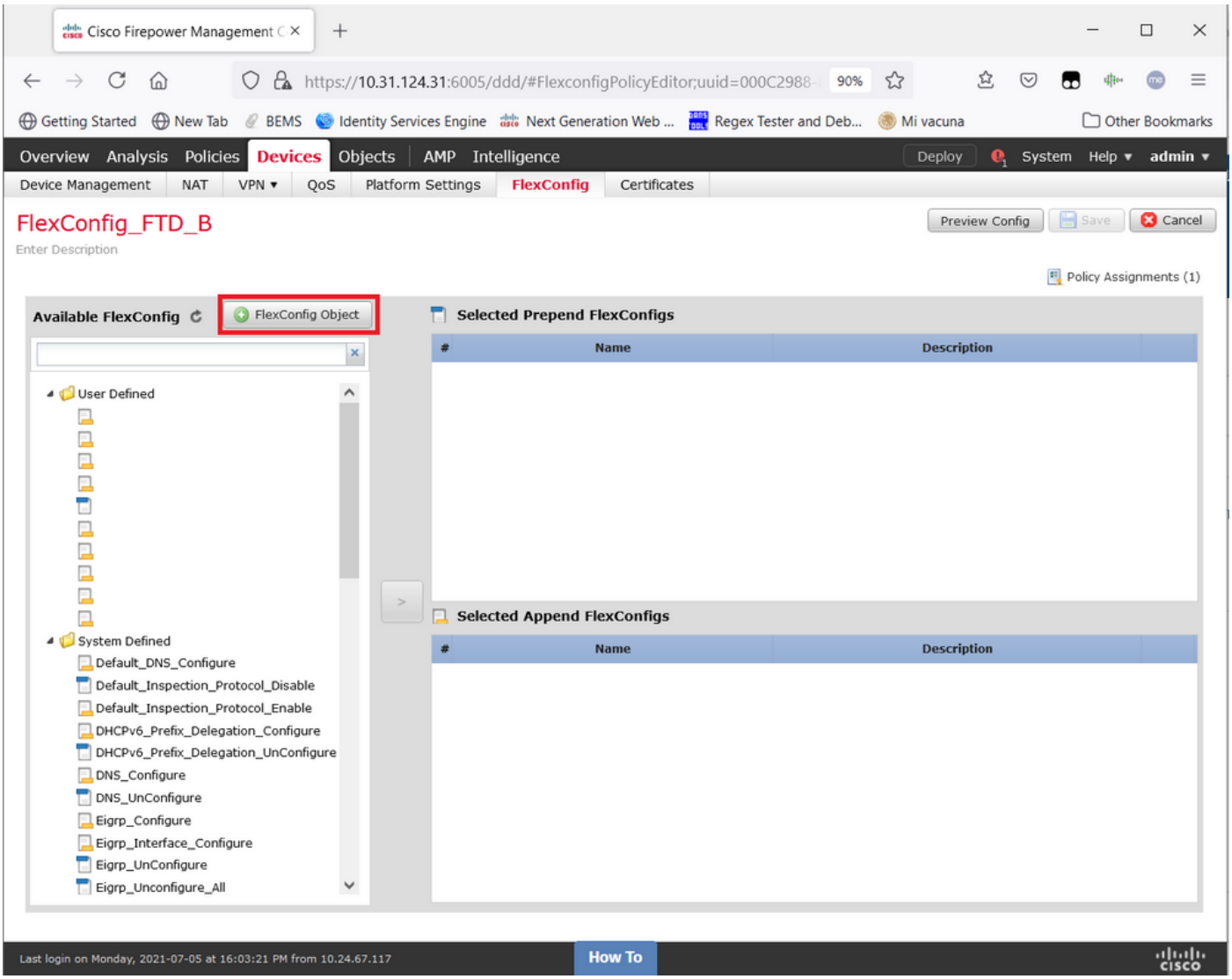
o

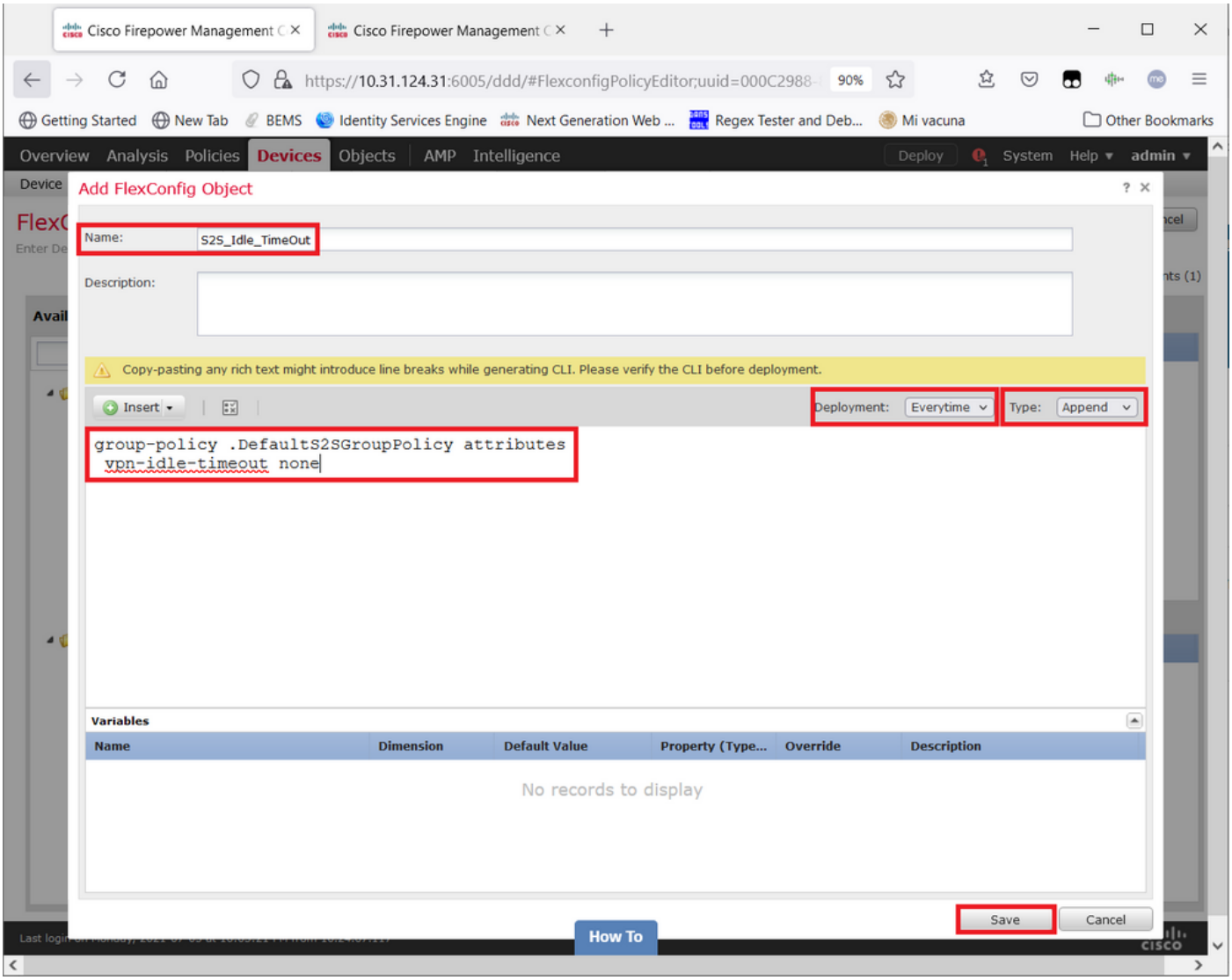


Passaggio 2. All'interno del criterio, creare un **oggetto FlexConfig** come segue:

Nome: S2S_Idle_TimeOut
Implementazione: Sempre
Tipo: Aggiungi

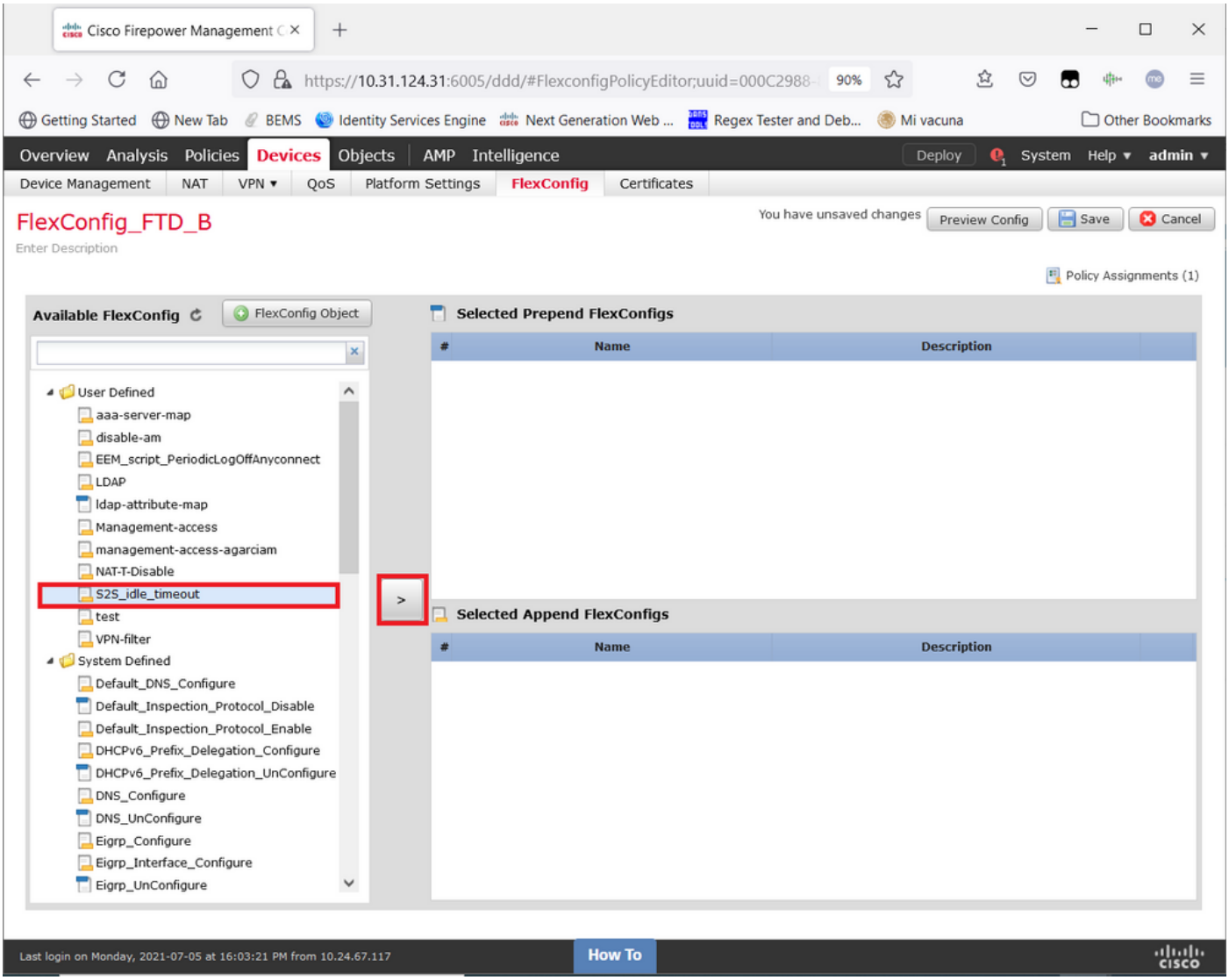
attributi .DefaultS2SGroupPolicy di criteri di gruppo
vpn-idle-timeout none

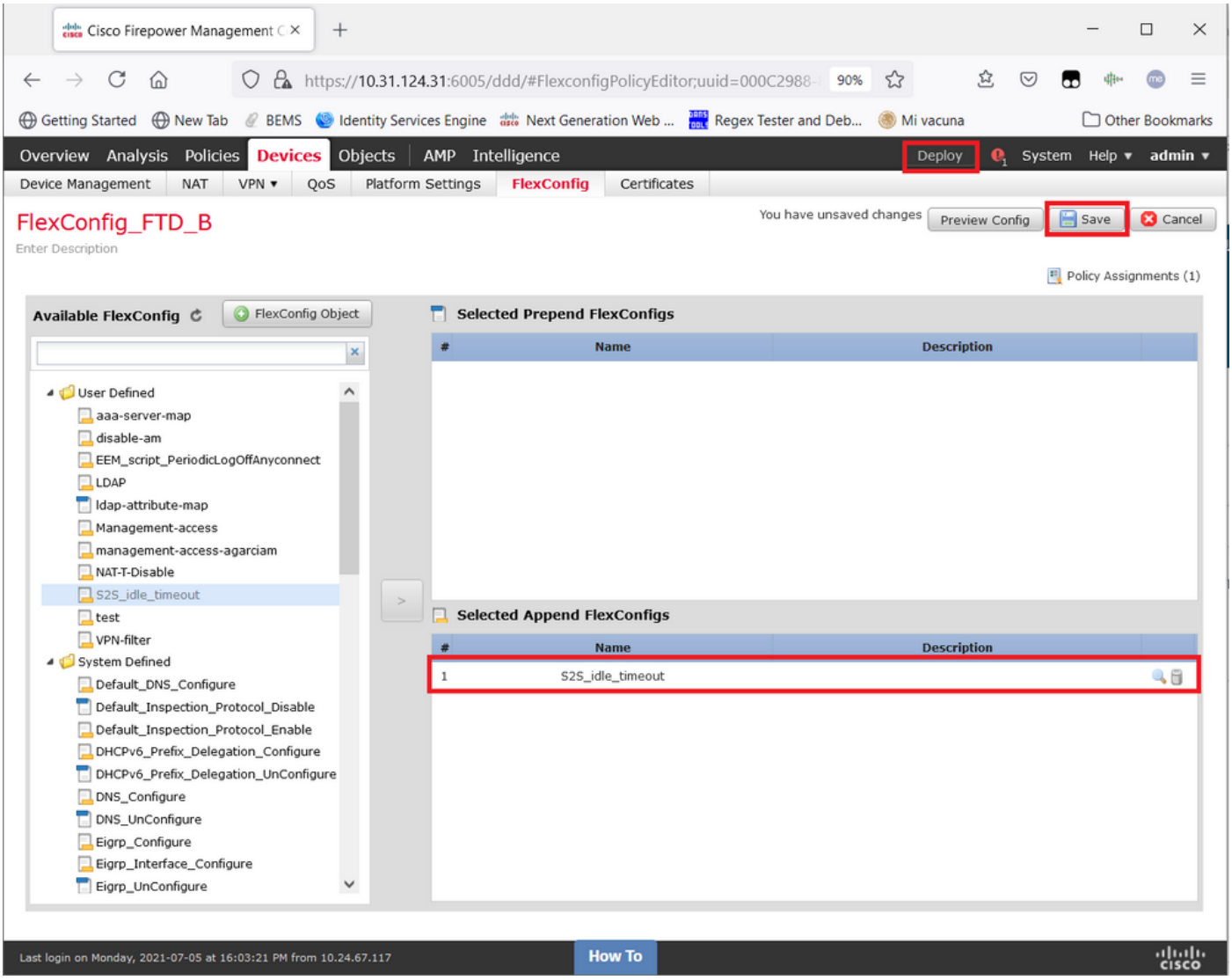




e **salvatelo**.

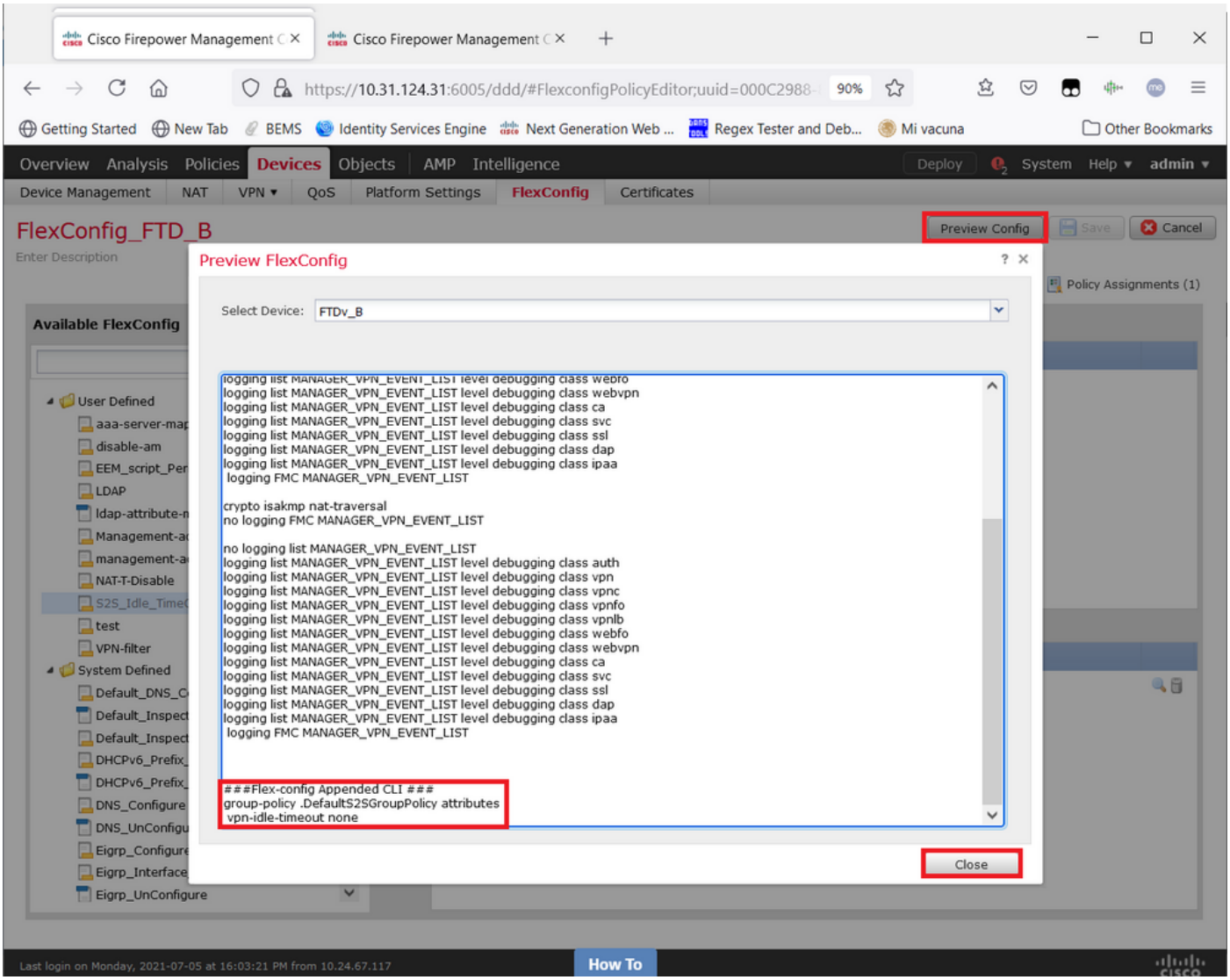
Passaggio 3. Nel riquadro di sinistra, cercarlo e trascinarlo nel riquadro di destra con il pulsante **>**.


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



Salvare le modifiche e **distribuire**.

Passaggio 3.1 (Facoltativo) Come passo intermedio, dopo aver salvato le modifiche alla configurazione, è possibile scegliere **Preview Config** per assicurarsi che i comandi FlexConfig siano pronti per essere sottoposti a push al termine della configurazione.



Verifica

Al termine della distribuzione, è possibile eseguire questo comando in LINA (**> system support diagnostic-cli**) per verificare che la nuova configurazione sia presente:

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

> **Attenzione:** Tieni presente che questa modifica interessa tutte le VPN da sito a sito sull'FTD. NON si tratta di un'impostazione per tunnel, bensì globale.

Anche se la configurazione è presente, il tunnel attivo deve essere riavviato (**cancellare ipsec sa peer** *<Indirizzo_Peer_IP_Remoto>*) in modo che la modifica abbia effetto quando il tunnel viene ristabilito. Per verificare che la modifica sia effettiva, usare questo 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
```

Il contatore del *timeout di inattività* deve essere impostato su 0 minuti anziché su 30 minuti e la VPN deve rimanere attiva indipendentemente dall'attività/traffico che la sovrasta.

> **Nota:** Al momento della stesura di questo documento, esiste un bug di miglioramento che consente di integrare la possibilità di modificare questa impostazione direttamente su FMC senza la necessità di Flexconfig. Vedere l'ID bug Cisco CSCvr82274 - ENH: rendere la vpn-idle-timeout configurabile

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi.

Informazioni correlate

- Guida alla configurazione di Firepower Management Center, versione 7.0 - Capitolo: Criteri FlexConfig per Firepower Threat Defense
- Guida alla configurazione di Firepower Management Center, versione 7.0 - Capitolo: VPN da sito a sito per Firepower Threat Defense
- Documentazione e supporto tecnico – Cisco Systems