FlexConfig 정책으로 FTD 사이트 대 사이트 VPN 유휴 시간 제한 비활성화

목차

소개

이 문서에서는 비활성 또는 유휴 시간 초과로 인한 터널 다운타임을 방지하기 위해 Cisco FMC(Firepower Management Center)에서 FlexConfig 정책을 사용하는 VPN의 vpn-idle-timeout 특성을 수정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(Firepower Threat Defense)
- FMC
- FlexConfig 정책
- Site-to-Site VPN 토폴로지

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

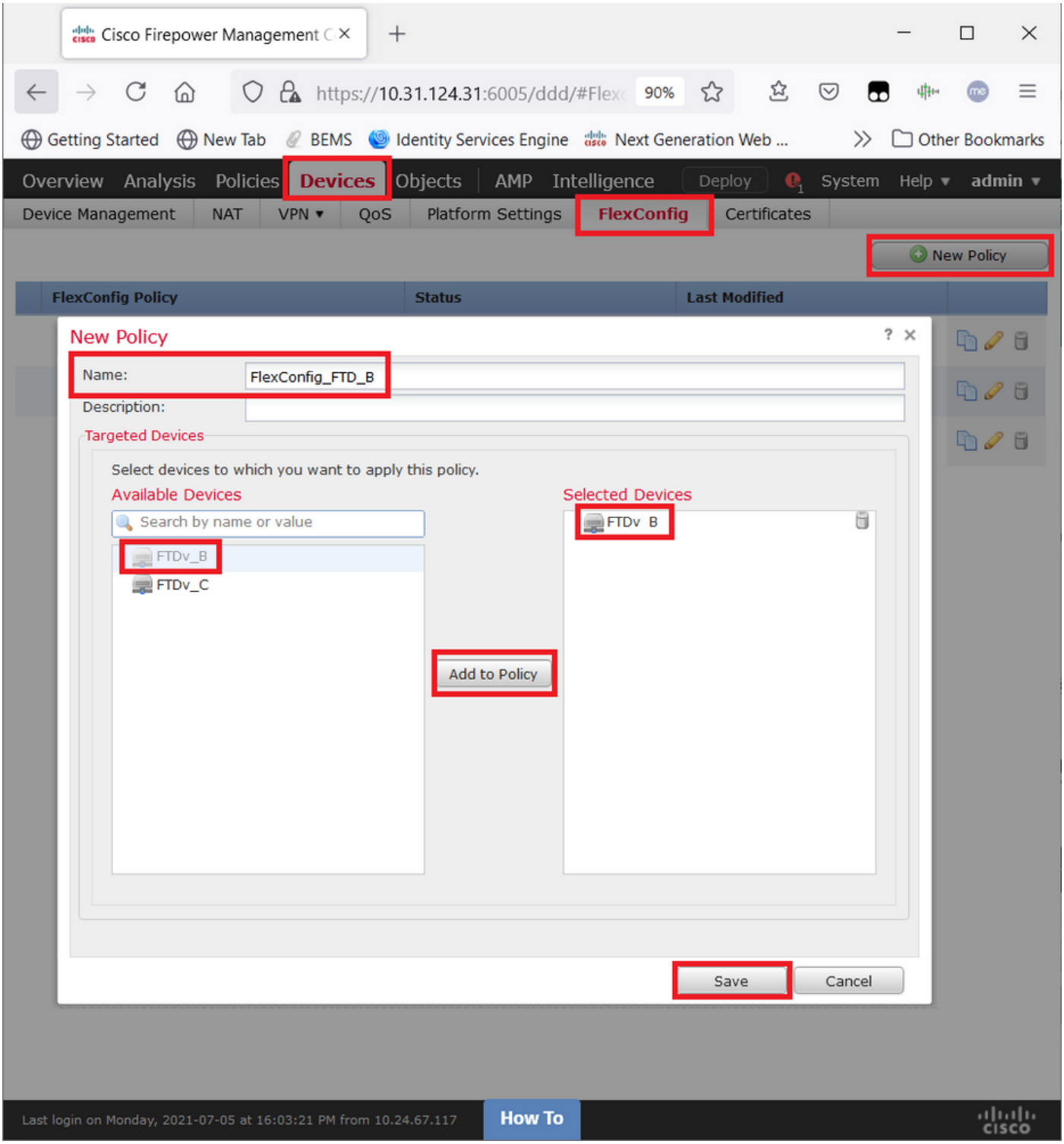
배경 정보

IKEv1(Internet Key Exchange version 1) 및 IKEv2(Internet Key Exchange version 2) Policy Based(Crypto map) Site-to-Site VPN은 모두 온디맨드 터널입니다. 기본적으로 FTD는 vpn-idle-timeout이라는 특정 기간 동안 터널을 통한 통신 활동이 없는 경우 VPN 연결을 **종료합니다**. 이 타이머는 기본적으로 30분으로 설정됩니다.

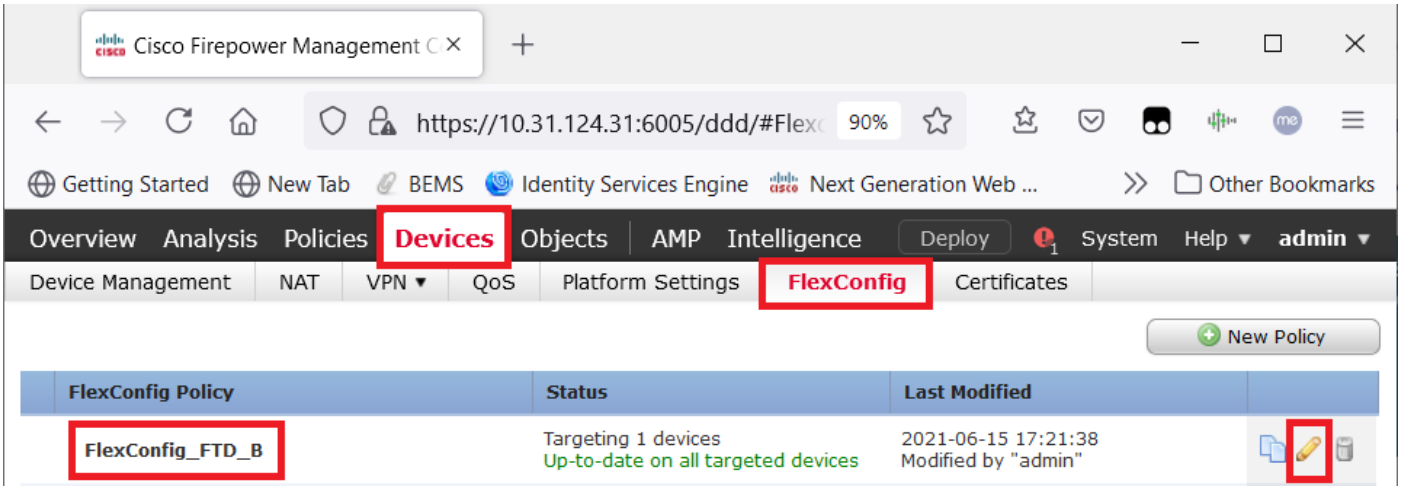
구성

FlexConfig 정책 및 FlexConfig 개체 구성

1단계. Devices(**디바이스) > FlexConfig**에서 새 FlexConfig 정책을 생성하고(존재하지 않는 경우) Site-to-Site VPN이 구성된 FTD에 연결합니다.


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

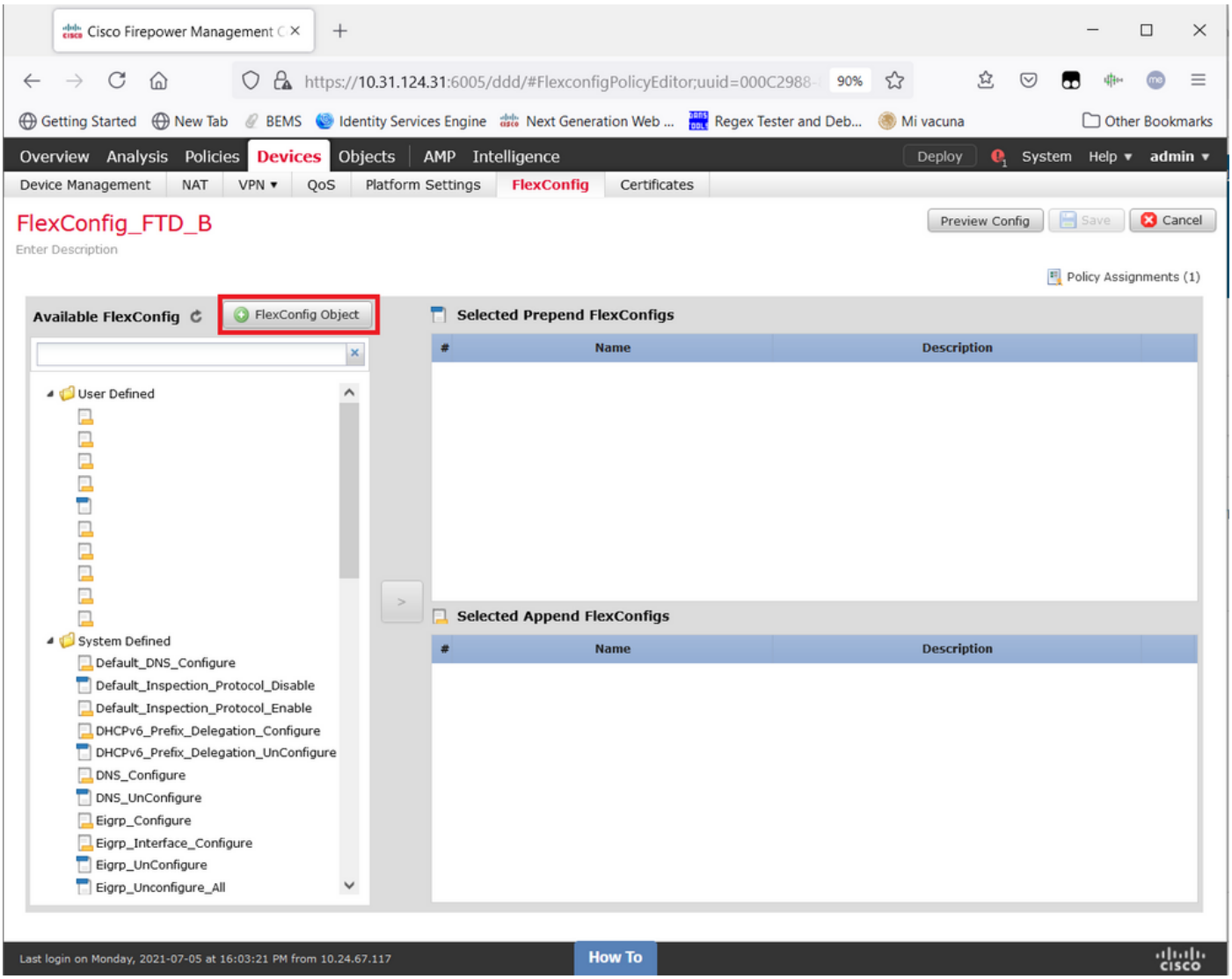
또는

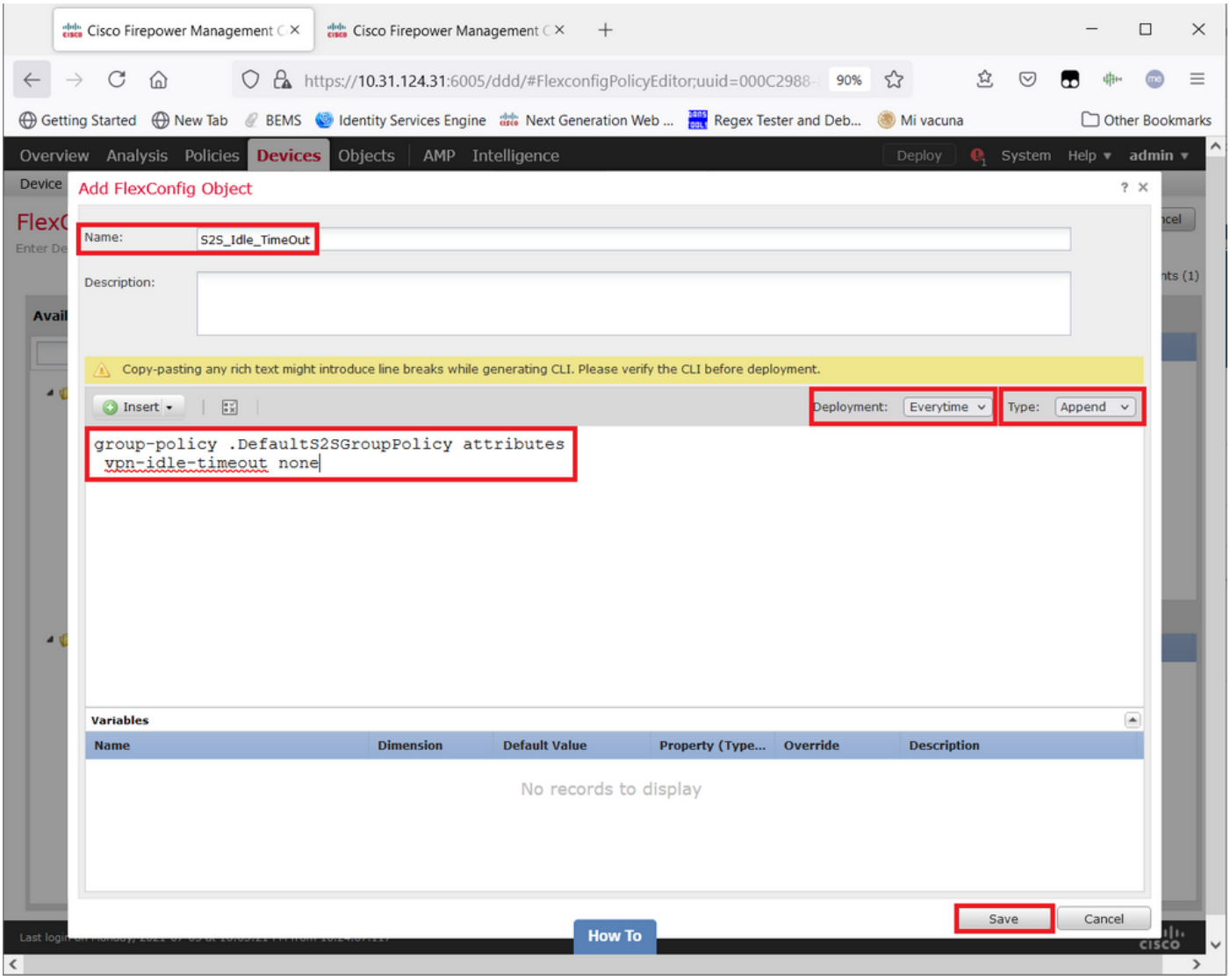


2단계. 해당 정책 내에서 다음과 같이 **FlexConfig 객체**를 생성합니다.

이름: S2S_Idle_TimeOut
구축: 매번
유형: 추가

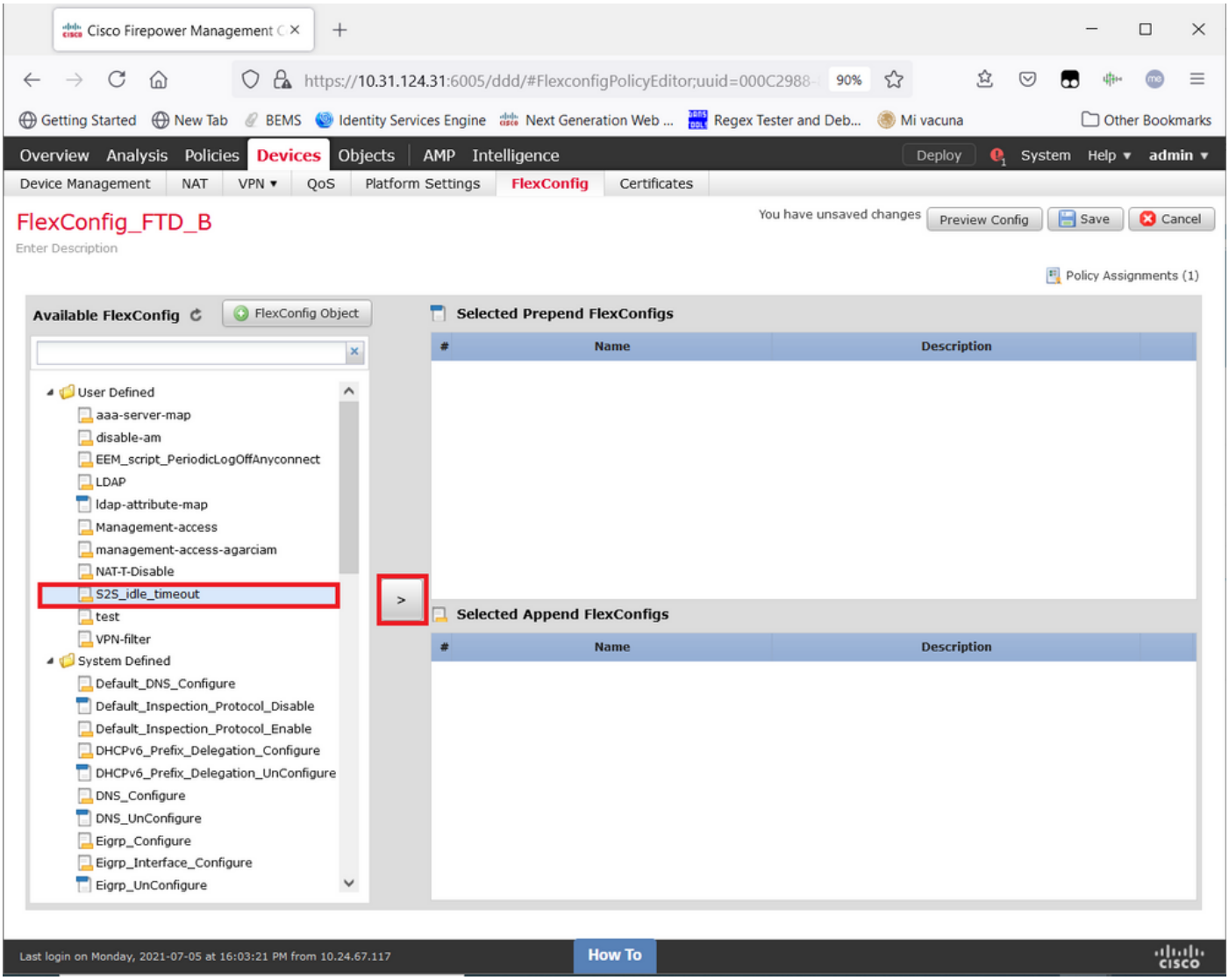
group-policy .DefaultS2SGroupPolicy 특성
vpn-idle-timeout 없음

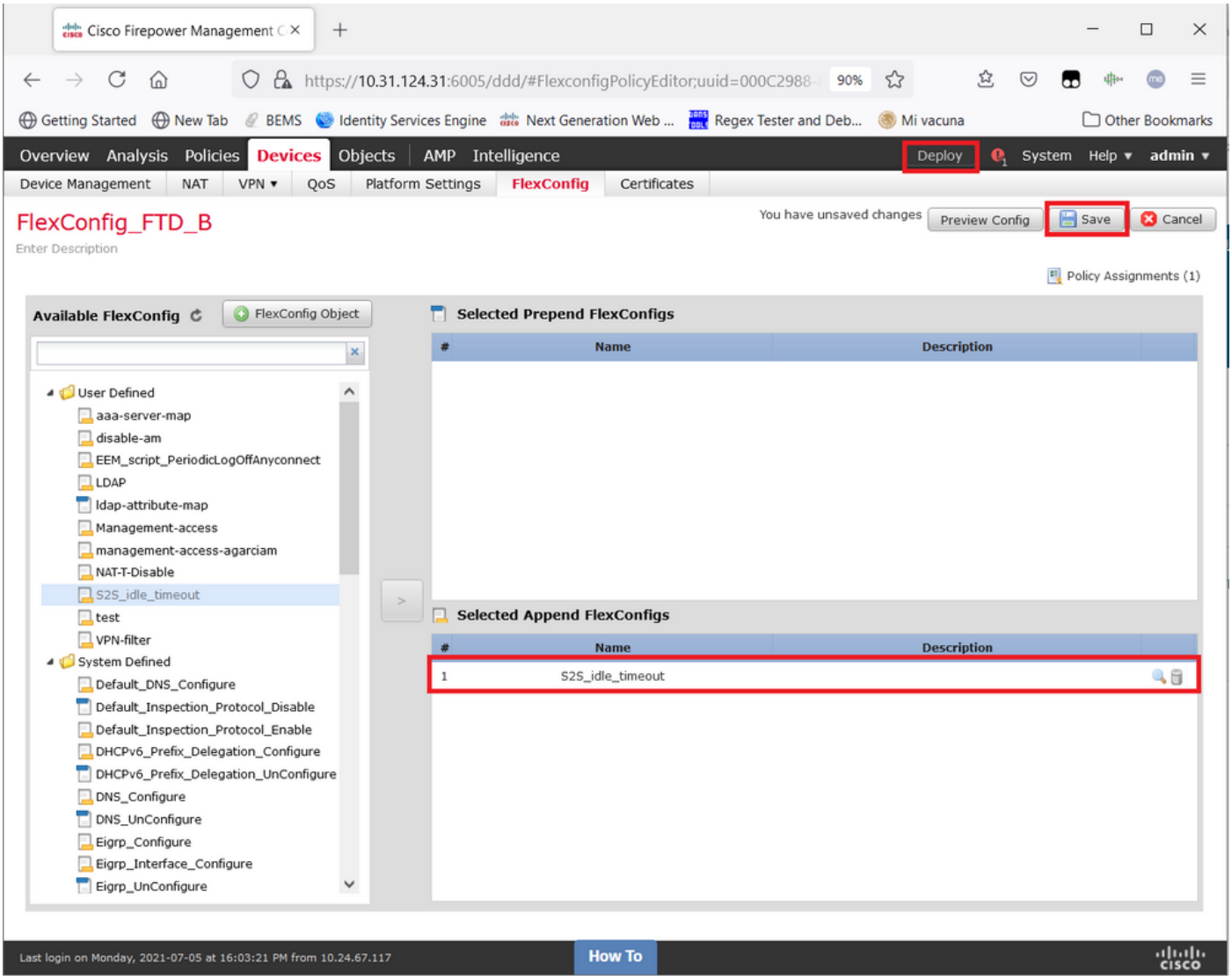




저장할 수 있습니다

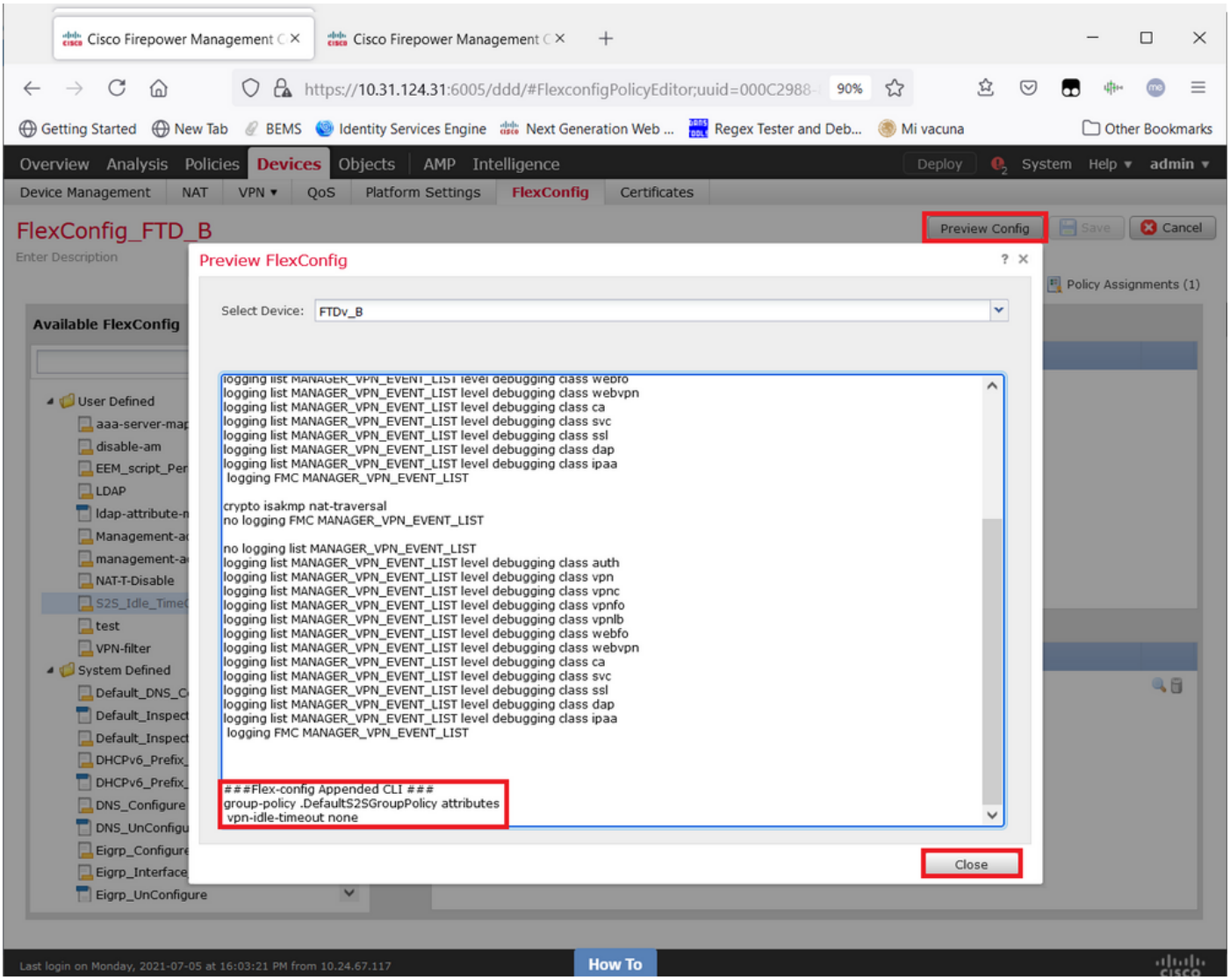
3단계. 왼쪽 창에서 검색하여 단추 **>**를 사용하여 오른쪽 창으로 끌어 놓습니다.


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



변경 사항을 저장하고 **구축**.

3.1단계(선택 사항) 컨피그레이션 변경 사항을 저장한 후 컨피그레이션 종료 시 FlexConfig 명령을 푸시할 준비가 되도록 Preview **Config**를 중간 단계로 선택할 수 있습니다.



다음을 확인합니다.

구축이 완료되면 LINA(**> 시스템 지원 diagnostic-cli**)에서 이 명령을 실행하여 새 컨피그레이션이 있는지 확인할 수 있습니다.

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

> **주의:** 이 변경은 FTD의 모든 S2S VPN에 영향을 미칩니다. 터널당 설정이 아니라 전역 설정입니다.

컨피그레이션이 있더라도 활성 터널을 바운스해야 합니다(**clear crypto ipsec sa peer<*Remote_Peer_IP_Address*>**). 그러면 터널이 다시 설정되면 변경 사항이 적용됩니다. 다음 명령을 사용하여 변경 사항이 적용되는지 확인할 수 있습니다.

```
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
```

유휴 시간 제한 카운터는 30분이 아닌 0분으로 설정해야 하며, VPN은 실행 중인 활동/트래픽에 관계없이 활성 상태를 유지해야 합니다.

> **참고:** 작성 시 Flexconfig를 사용하지 않고 FMC에서 직접 이 설정을 수정하는 기능을 통합하는 개선 버그가 있습니다. Cisco 버그 ID CSCvr82274 - ENH 참조: vpn-idle-timeout 구성 가능

문제 해결

현재 사용 가능한 문제 해결에 대한 구체적인 정보가 없습니다.

관련 정보

- Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 장: Firepower Threat Defense용 FlexConfig 정책
- Firepower Management Center 컨피그레이션 가이드, 버전 7.0 - 장: Firepower Threat Defense용 사이트 간 VPN
- 기술 지원 및 문서 – Cisco Systems