IPSec VPN을 통한 FTD BGP 구성

목차

소개

이 문서에서는 두 Cisco FTD(FirePower Threat Defense) 간에 IPsec 사이트 간 VPN 터널을 통해 BGP(Border Gateway Protocol) 인접 디바이스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD의 BGP 컨피그레이션
- FTD의 IPsec Site-to-Site VPN 터널 구성

사용되는 구성 요소

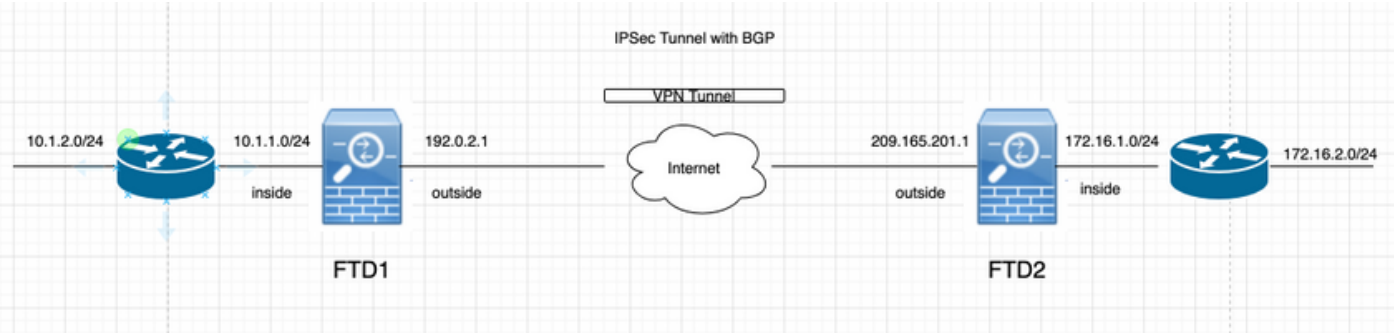
이 문서의 정보는 6.4.0.7 및 6.4.0.9을 실행하는 Cisco FTDv를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 IPSec 터널을 통해 BGP 인접 디바이스를 가져오기 위해 FTD에 필요한 컨피그레이션에 대해 설명합니다.

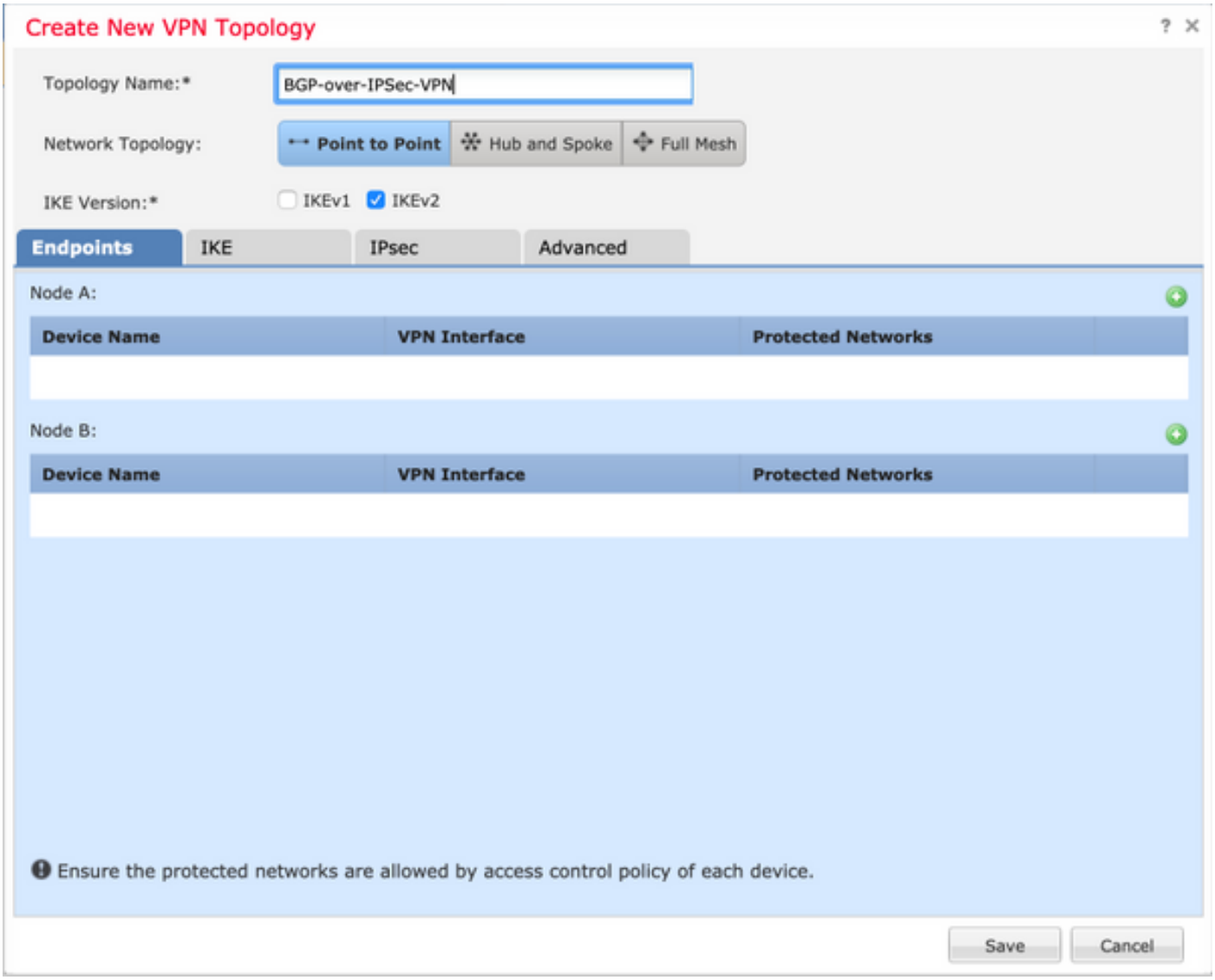
네트워크 다이어그램



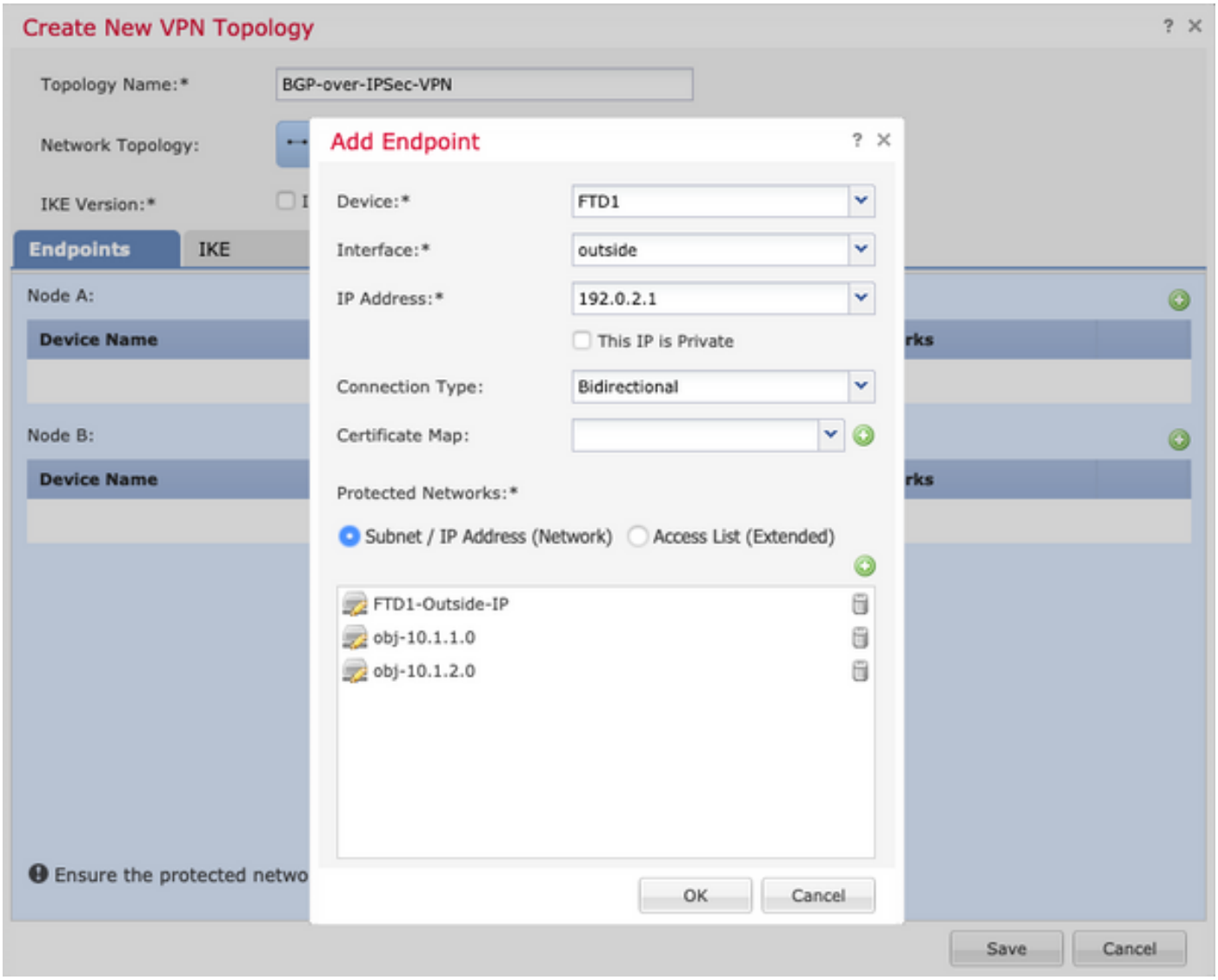
IPSec VPN 구성

1단계. 새 Point-to-Point VPN 토폴로지를 만듭니다.

Devices(**디바이스) > VPN > Site-to-Site(사이트 대 사이트)**로 이동하고 새 FirePower Threat Defense 디바이스 VPN을 추가합니다.

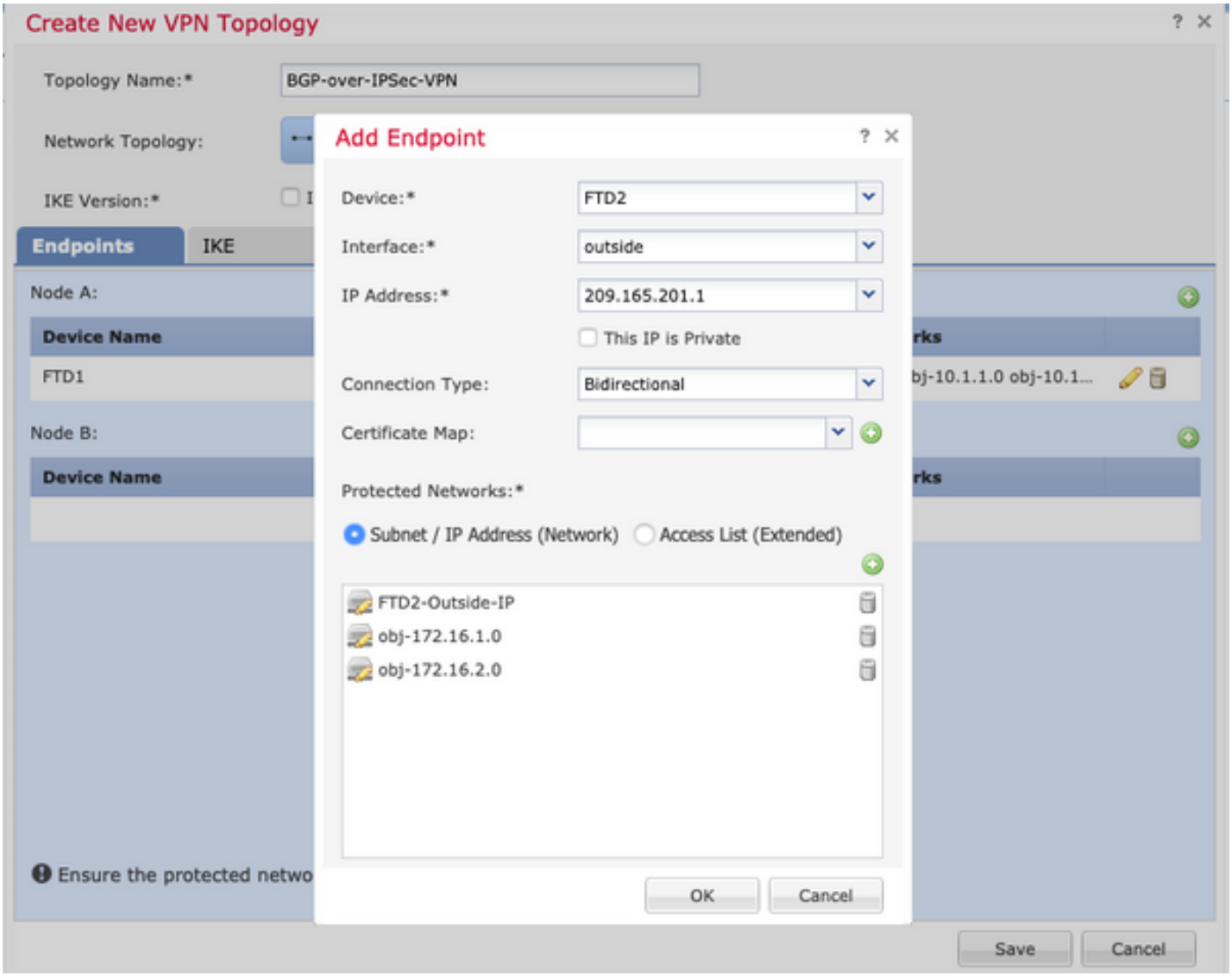


2단계. FTD1을 엔드포인트 중 하나로 구성합니다.



- 개체 네트워크 FTD1-Outside-IP는 FTD1의 외부 인터페이스 IP 주소를 포함합니다.
- obj-10.1.1.0 및 obj-10.1.2.0 개체에는 각각 서브넷 10.1.1.0/24 및 10.1.2.0/24이 포함됩니다 .VPN 트래픽은 이러한 서브넷에서 생성됩니다.BGP 컨피그레이션 섹션의 BGP는 이러한 서브넷을 네이버에 알리도록 구성됩니다.

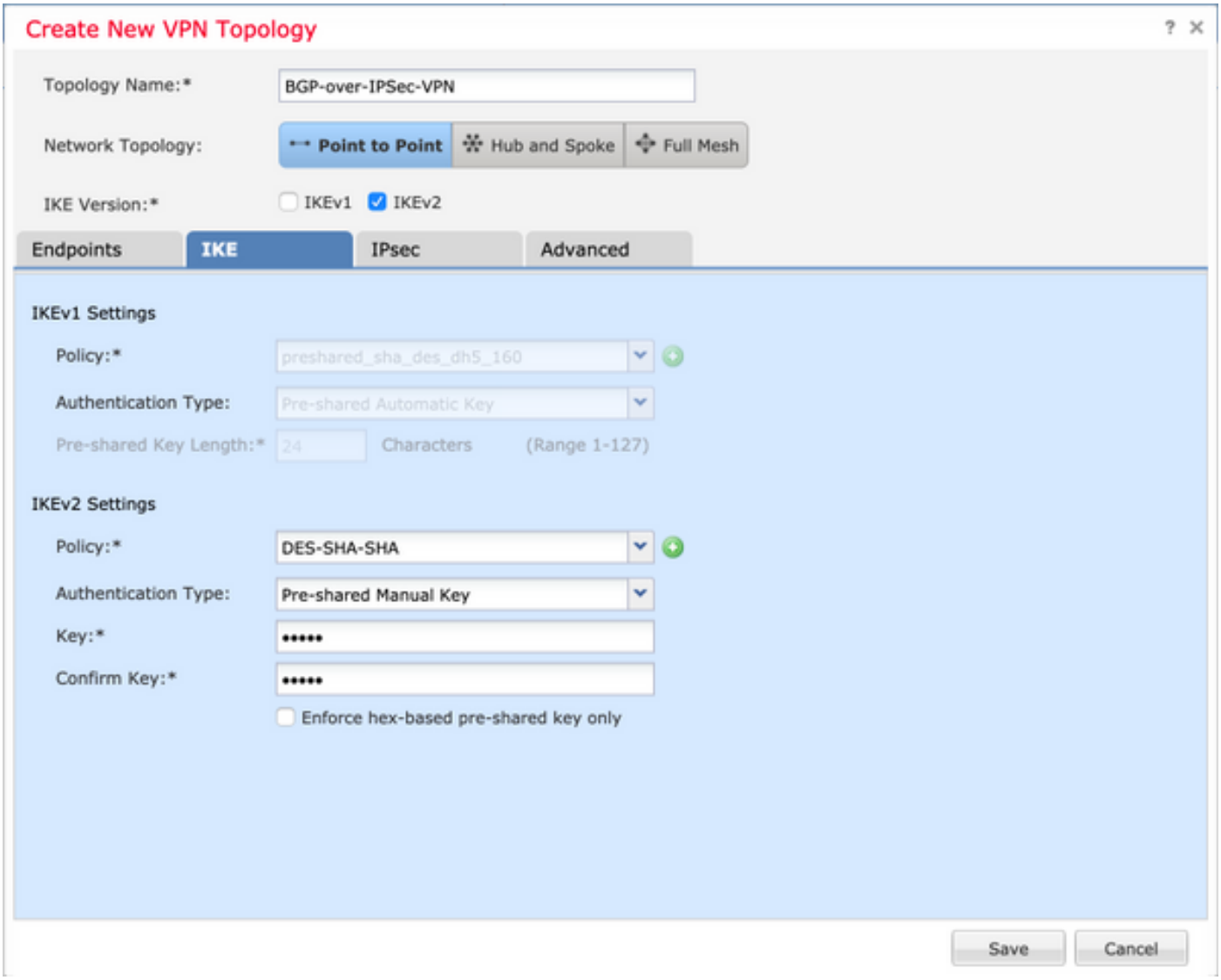
3단계. FTD2를 두 번째 엔드포인트로 구성합니다.



- 개체 네트워크 FTD2-Outside-IP는 FTD2의 외부 인터페이스 IP 주소를 포함합니다.
- obj-172.16.1.0 및 obj-172.16.2.0 객체에는 각각 서브넷 172.16.1.0/24 및 172.16.2.0/24이 포함됩니다.VPN 트래픽은 이러한 서브넷에서 생성됩니다.BGP 컨피그레이션 섹션의 BGP는 이러한 서브넷을 네이버에 알리도록 구성됩니다.

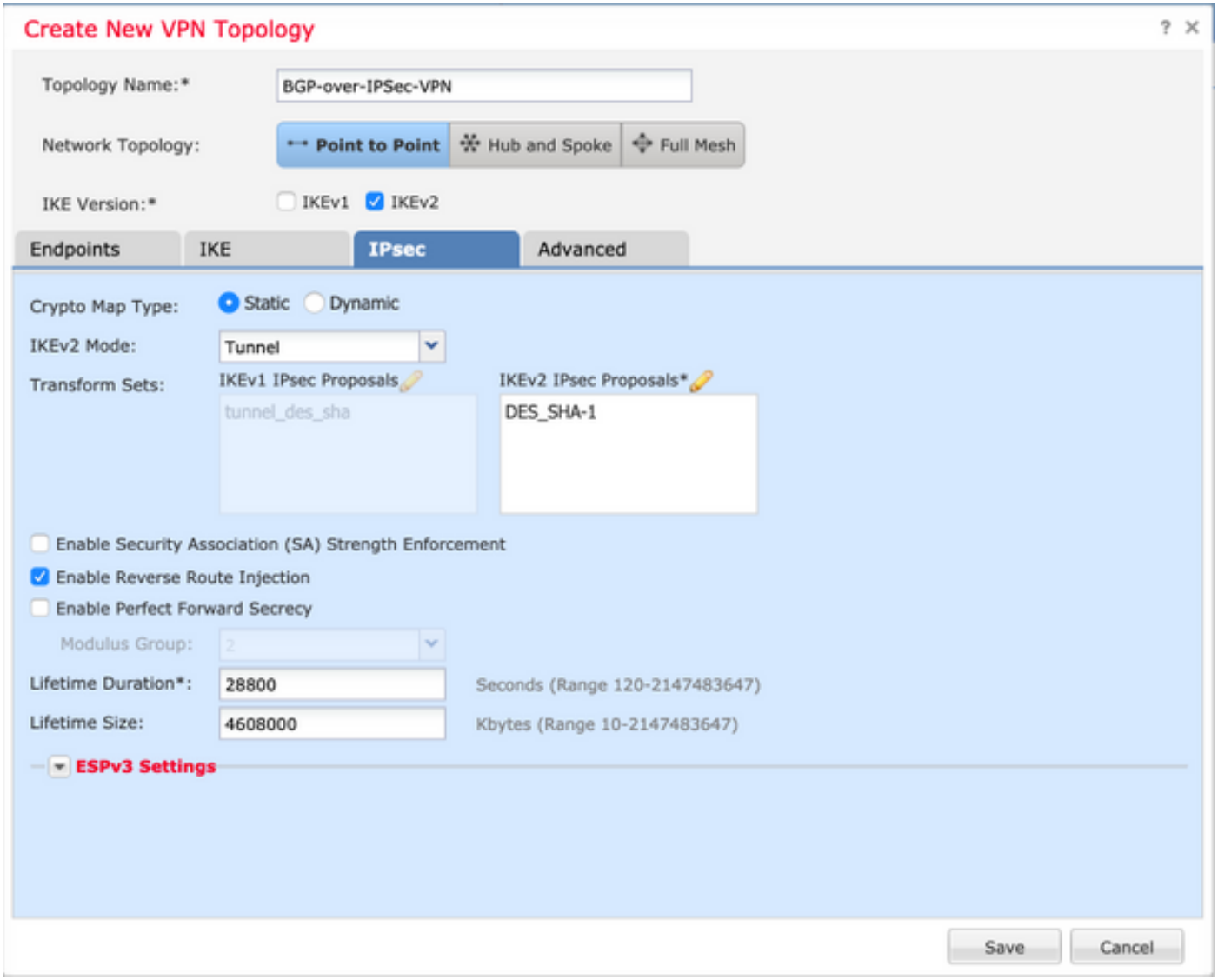
4단계. IKE 매개변수를 구성합니다.

1. IKEv2 정책을 구성합니다.
2. 인증 방법(PSK/인증서)을 구성합니다.

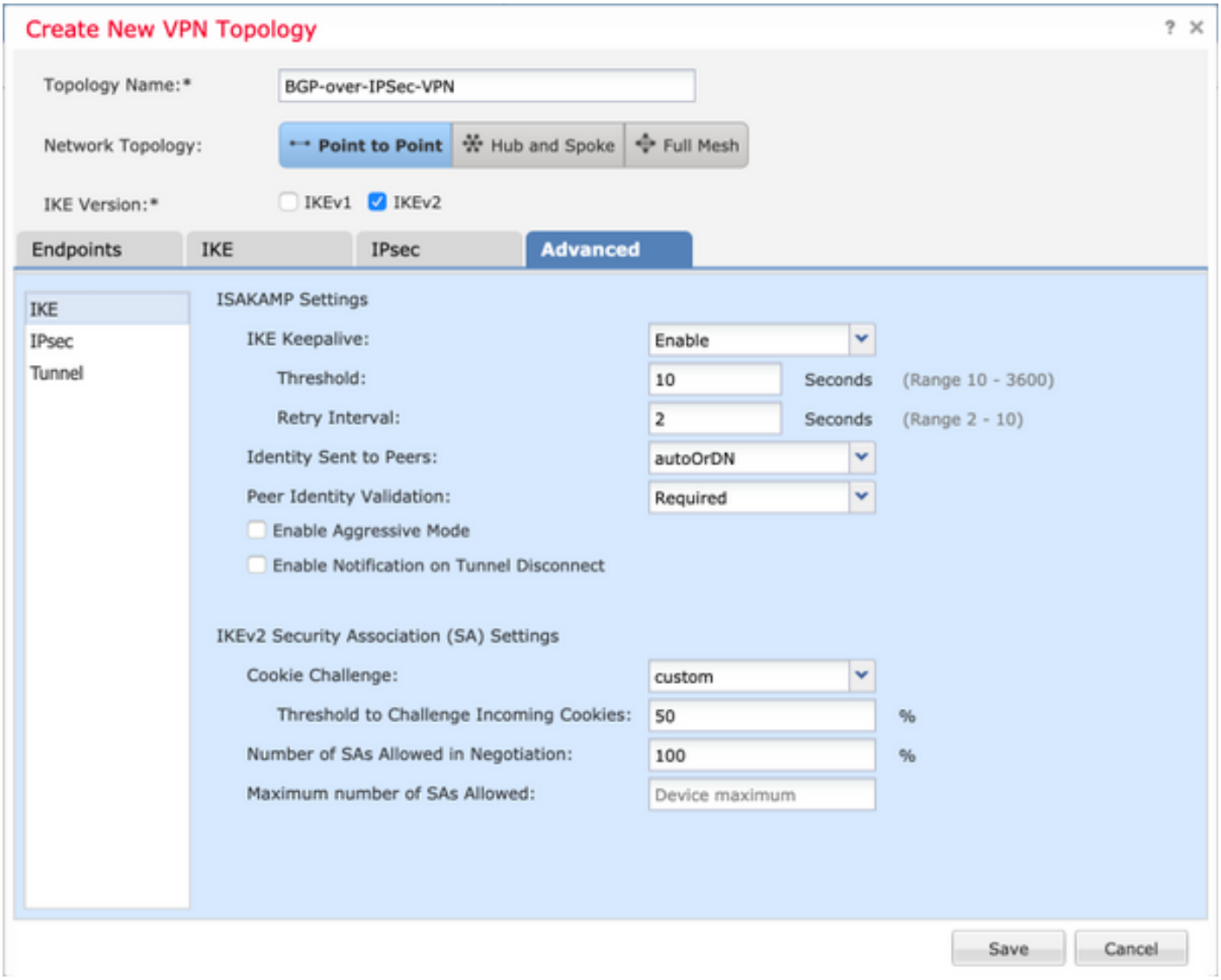


5단계. 필요한 IPSec 매개변수를 구성합니다.

1. 암호화 맵 유형 구성(정적 또는 동적)
2. IKEv2 모드 구성(터널 또는 전송)
3. IPSec 제안 구성
4. Perfect Forward Secrecy 활성화(선택 사항)
5. 역방향 경로 삽입 사용(선택 사항)



6단계. 필요에 따라 고급 설정을 구성합니다.

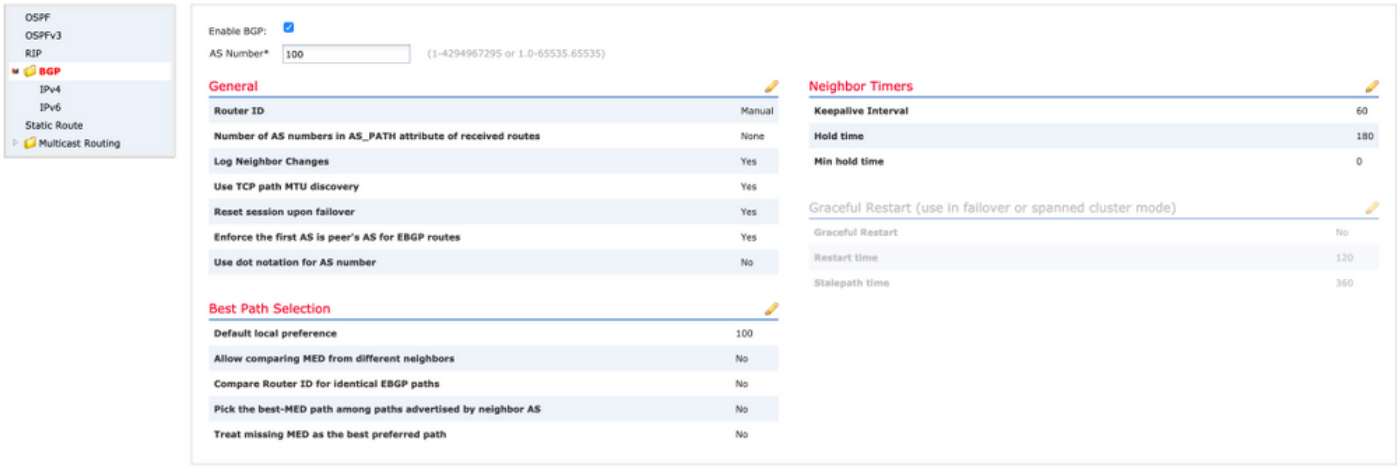


BGP 구성

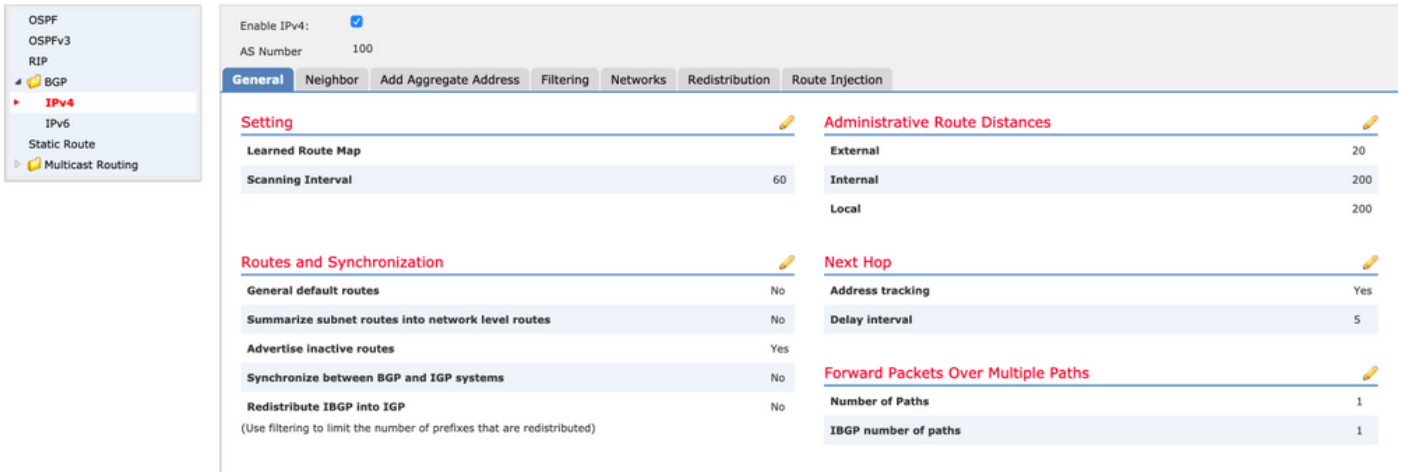
FTD1 및 FTD2를 구성하는 절차입니다.

Device **Management(디바이스 관리)**에서 디바이스를 선택한 다음 Routing(라우팅) **> BGP로 이동합니다**.

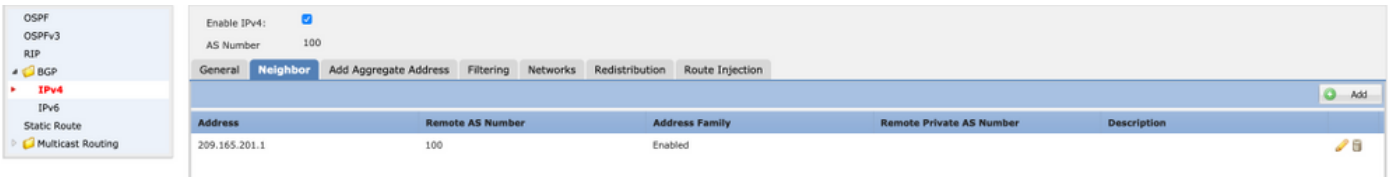
1. 이 이미지에 표시된 대로 BGP를 활성화하고 AS(Autonomous System) 번호를 구성합니다.



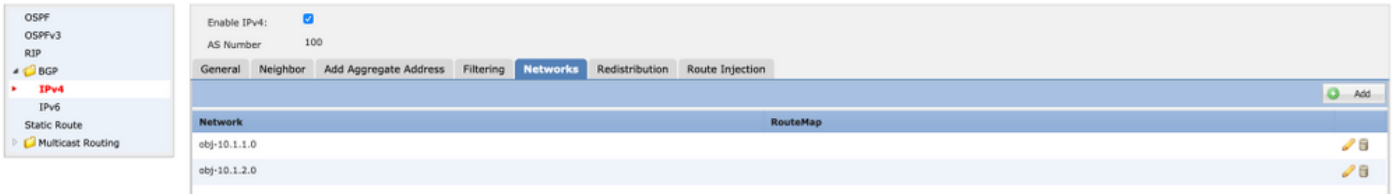
2. BGP **> IPv4**로 이동하여 이 이미지에 표시된 대로 FTD에서 BGP IPv4를 활성화합니다.



3. **네이버** 탭 아래에서 다른 FTD를 네이버로 추가하고 이 이미지에 표시된 대로 네이버를 활성화합니다.



4. **네트워크** 탭 아래에서 BGP를 통해 광고할 네트워크를 추가합니다.



5. 다른 모든 BGP 설정은 선택 사항이며 환경에 따라 구성할 수 있습니다.

두 디바이스의 최종 컨피그레이션

FTD1

```
!--- FTD Version ---! ftd1# show version ----------------------[ ftd1 ]----------------------
Model : Cisco Firepower Threat Defense for VMWare (75) Version 6.4.0.7 (Build 53) UUID :
cbd4966c-daf4-11ea-8637-c8977622bc2d Rules update version : 2018-10-10-001-vrt VDB version : 309
------------------------------------------------- Cisco Adaptive Security Appliance Software
Version 9.12(2)151 !--- Configure the Inside and outside interface ---! interface
GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag policy static sgt
disabled trusted security-level 0 ip address 192.0.2.1 255.255.255.0 ! interface
GigabitEthernet0/1 nameif inside cts manual propagate sgt preserve-untag policy static sgt
disabled trusted security-level 0 ip address 10.1.1.1 255.255.255.0 !--- Configure VPN ---! !---
Configure IPSec Policy ---! crypto ipsec ikev2 ipsec-proposal CSM_IP_1 protocol esp encryption
des protocol esp integrity sha-1 !--- Configure Crypto Map ---! crypto map CSM_outside_map 1
match address CSM_IPSEC_ACL_2 crypto map CSM_outside_map 1 set peer 209.165.201.1 crypto map
CSM_outside_map 1 set ikev2 ipsec-proposal CSM_IP_1 crypto map CSM_outside_map 1 set reverse-
route !--- Apply the Crypto Map to the outside interface ---! crypto map CSM_outside_map
interface outside !--- Configure IKEv2 policy ---! crypto ikev2 policy 80 encryption des
integrity sha group 5 prf sha lifetime seconds 86400 !--- Enable IKEv2 on the outside interface
---! crypto ikev2 enable outside !--- Configure BGP Router Process ---! router bgp 100 bgp log-
neighbor-changes bgp router-id 10.127.248.35 address-family ipv4 unicast neighbor 209.165.201.1
remote-as 100 neighbor 209.165.201.1 transport path-mtu-discovery disable neighbor 209.165.201.1
```

activate network 10.1.1.0 mask 255.255.255.0 network 10.1.2.0 mask 255.255.255.0 no auto-summary no synchronization exit-address-family ! !--- Configure the necessary routes ---! route outside 0.0.0.0 0.0.0.0 192.0.2.100 1 route inside 10.1.2.0 255.255.255.0 10.1.1.100 1

FTD2

!--- FTD Version ---! ftd2# show version ----------------------[ftd2]---------------------- Model : Cisco Firepower Threat Defense for VMWare (75) Version 6.4.0.9 (Build 62) UUID : 4ebe8e3a-dd8d-11ea-a599-a348a450d5ff Rules update version : 2018-10-10-001-vrt VDB version : 309 -- Cisco Adaptive Security Appliance Software Version 9.12(2)33 !--- Configure the Inside and outside interface ---! interface GigabitEthernet0/0 nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 209.165.201.1 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 172.16.1.1 255.255.255.0 !--- Configure VPN ---! !-- Configure IPSec Policy ---! crypto ipsec ikev2 ipsec-proposal CSM_IP_1 protocol esp encryption des protocol esp integrity sha-1 !--- Configure Crypto Map ---! crypto map CSM_outside_map 2 match address CSM_IPSEC_ACL_2 crypto map CSM_outside_map 2 set peer 192.0.2.1 crypto map CSM_outside_map 2 set ikev2 ipsec-proposal CSM_IP_1 crypto map CSM_outside_map 2 set reverse-route !--- Apply the Crypto Map to the outside interface ---! crypto map CSM_outside_map interface outside !--- Configure IKEv2 policy ---! crypto ikev2 policy 80 encryption des integrity sha group 5 prf sha lifetime seconds 86400 !--- Enable IKEv2 on the outside interface ---! crypto ikev2 enable outside !--- Configure BGP Router Process ---! router bgp 100 bgp log-neighbor-changes bgp router-id 10.127.248.36 address-family ipv4 unicast neighbor 192.0.2.1 remote-as 100 neighbor 192.0.2.1 transport path-mtu-discovery disable neighbor 192.0.2.1 activate network 172.16.1.0 mask 255.255.255.0 network 172.16.2.0 mask 255.255.255.0 no auto-summary no synchronization exit-address-family !--- Configure the necessary routes ---! route outside 0.0.0.0 0.0.0.0 209.165.201.100 1 route inside 172.16.2.0 255.255.255.0 172.16.1.100 1

다음을 확인합니다.

FTD1

!--- Check the IKEv2 sa with remote peer ---! ftd1# show crypto ikev2 sa IKEv2 SAs: Session-id:34, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote Status Role 315310279 192.0.2.1/500 209.165.201.1/500 READY INITIATOR Encr: DES, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/32514 sec Child sa: local selector 192.0.2.1/0 - 192.0.2.1/65535 remote selector 209.165.201.1/0 - 209.165.201.1/65535 ESP spi in/out: 0xd8ba0545/0x4b6beb6c !--- Check the IPSec sa with remote peer and check the number of encrypts and decrypts---! ftd1# show crypto ipsec sa interface: outside Crypto map tag: CSM_outside_map, seq num: 1, local addr: 192.0.2.1 access-list CSM_IPSEC_ACL_2 extended permit ip host 192.0.2.1 host 209.165.201.1 local ident (addr/mask/prot/port): (192.0.2.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (209.165.201.1/255.255.255.255/0/0) current_peer: 209.165.201.1 #pkts encaps: 1110, #pkts encrypt: 1110, #pkts digest: 1110 #pkts decaps: 1111, #pkts decrypt: 1111, #pkts verify: 1111 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 1110, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 192.0.2.1/500, remote crypto endpt.: 209.165.201.1/500 path mtu 1500, ipsec overhead 58(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: 4B6BEB6C current inbound spi : D8BA0545 inbound esp sas: spi: 0xD8BA0545 (3636069701) SA State: active transform: esp-des esp-sha-hmac no compression in use settings ={L2L, Tunnel, IKEv2, } slot: 0, conn_id: 1515, crypto-map: CSM_outside_map sa timing: remaining key lifetime (kB/sec): (4101105/21619) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF outbound esp sas: spi: 0x4B6BEB6C (1265363820) SA State: active transform: esp-des esp-sha-hmac no compression in use settings ={L2L, Tunnel, IKEv2, } slot: 0, conn_id: 1515, crypto-map: CSM_outside_map sa timing: remaining key lifetime (kB/sec): (4239345/21619) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x00000001 !--- Check the BGP router summary ---! ftd1# show bgp summary BGP router identifier

10.127.248.35, local AS number 100 BGP table version is 43, main routing table version 43 4 network entries using 800 bytes of memory 4 path entries using 320 bytes of memory 2/2 BGP path/bestpath attribute entries using 416 bytes of memory 0 BGP route-map cache entries using 0 bytes of memory 0 BGP filter-list cache entries using 0 bytes of memory BGP using 1536 total bytes of memory BGP activity 20/16 prefixes, 26/22 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 209.165.201.1 4 100 494 488 43 0 0 09:01:15 2 !--- Check the BGP neighborship ---! ftd1# show bgp neighbors BGP neighbor is 209.165.201.1, context single_vf, remote AS 100, internal link BGP version 4, remote router ID 10.127.248.36 BGP state = Established, up for 09:01:18 Last read 00:00:52, last write 00:00:12, hold time is 180, keepalive interval is 60 seconds Neighbor sessions: 1 active, is not multisession capable (disabled) Neighbor capabilities: Route refresh: advertised and received(new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Multisession Capability: Message statistics: InQ depth is 0 OutQ depth is 0 Sent Rcvd Opens: 1 1 Notifications: 0 0 Updates: 3 3 Keepalives: 484 490 Route Refresh: 0 0 Total: 488 494 Default minimum time between advertisement runs is 0 seconds For address family: IPv4 Unicast Session: 209.165.201.1 BGP table version 43, neighbor version 43/0 Output queue size : 0 Index 19 19 update-group member Sent Rcvd Prefix activity: ---- ---- Prefixes Current: 2 2 (Consumes 160 bytes) Prefixes Total: 2 2 Implicit Withdraw: 0 0 Explicit Withdraw: 0 0 Used as bestpath: n/a 2 Used as multipath: n/a 0 Outbound Inbound Local Policy Denied Prefixes: -------- ------- Bestpath from this peer: 2 n/a Invalid Path: 1 n/a Total: 3 0 Number of NLRIs in the update sent: max 1, min 0 Address tracking is enabled, the RIB does have a route to 209.165.201.1 Connections established 2; dropped 1 Last reset 09:01:34, due to Peer closed the session of session 1 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled !--- Check the routes learned from BGP ---! ftd1# sh route bgp Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route Gateway of last resort is 192.0.2.100 to network 0.0.0.0 B 172.16.1.0 255.255.255.0 [200/0] via 209.165.201.1, 00:00:57 B 172.16.2.0 255.255.255.0 [200/0] via 172.16.1.100, 09:01:23

FTD2

!--- Check the IKEv2 sa with remote peer ---! ftd2# show crypto ikev2 sa IKEv2 SAs: Session-id:34, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote Status Role 862624945 209.165.201.1/500 192.0.2.1/500 READY RESPONDER Encr: DES, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK Life/Active Time: 86400/32429 sec Child sa: local selector 209.165.201.1/0 - 209.165.201.1/65535 remote selector 192.0.2.1/0 - 192.0.2.1/65535 ESP spi in/out: 0x4b6beb6c/0xd8ba0545 !--- Check the IPSec sa with remote peer and check the number of encrypts and decrypts---! ftd2# show crypto ipsec sa interface: outside Crypto map tag: CSM_outside_map, seq num: 2, local addr: 209.165.201.1 access-list CSM_IPSEC_ACL_2 extended permit ip host 209.165.201.1 host 192.0.2.1 local ident (addr/mask/prot/port): (209.165.201.1/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (192.0.2.1/255.255.255.255/0/0) current_peer: 192.0.2.1 #pkts encaps: 1107, #pkts encrypt: 1107, #pkts digest: 1107 #pkts decaps: 1106, #pkts decrypt: 1106, #pkts verify: 1106 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 1107, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 209.165.201.1/500, remote crypto endpt.: 192.0.2.1/500 path mtu 1500, ipsec overhead 58(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: D8BA0545 current inbound spi : 4B6BEB6C inbound esp sas: spi: 0x4B6BEB6C (1265363820) SA State: active transform: esp-des esp-sha-hmac no compression in use settings ={L2L, Tunnel, IKEv2, } slot: 0, conn_id: 1516, crypto-map: CSM_outside_map sa timing: remaining key lifetime (kB/sec): (4008945/21713) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0xFFFFFFFF 0xFFFFFFFF outbound esp sas: spi: 0xD8BA0545 (3636069701) SA State: active transform: esp-des esp-sha-hmac no compression in use settings ={L2L, Tunnel, IKEv2, } slot: 0, conn_id: 1516, crypto-map: CSM_outside_map sa timing: remaining key lifetime (kB/sec): (4239345/21713) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0x00000000 0x00000001 !--- Check the BGP router summary ---! ftd2# show bgp summary BGP router identifier 10.127.248.36, local AS number 100 BGP table version is 44, main

routing table version 44 3 network entries using 600 bytes of memory 3 path entries using 240 bytes of memory 2/2 BGP path/bestpath attribute entries using 416 bytes of memory 0 BGP route-map cache entries using 0 bytes of memory 0 BGP filter-list cache entries using 0 bytes of memory BGP using 1256 total bytes of memory BGP activity 20/17 prefixes, 26/23 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 192.0.2.1 4 100 486 492 44 0 0 08:59:40 2 !--- Check the BGP neighborship ---! ftd2# show bgp neighbors BGP neighbor is 192.0.2.1, context single_vf, remote AS 100, internal link BGP version 4, remote router ID 10.127.248.35 BGP state = Established, up for 08:59:42 Last read 00:00:53, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds Neighbor sessions: 1 active, is not multisession capable (disabled) Neighbor capabilities: Route refresh: advertised and received(new) Four-octets ASN Capability: advertised and received Address family IPv4 Unicast: advertised and received Multisession Capability: Message statistics: InQ depth is 0 OutQ depth is 0 Sent Rcvd Opens: 1 1 Notifications: 0 0 Updates: 2 3 Keepalives: 489 482 Route Refresh: 0 0 Total: 492 486 Default minimum time between advertisement runs is 0 seconds For address family: IPv4 Unicast Session: 192.0.2.1 BGP table version 44, neighbor version 44/0 Output queue size : 0 Index 19 19 update-group member Sent Rcvd Prefix activity: ---- ---- Prefixes Current: 1 2 (Consumes 160 bytes) Prefixes Total: 1 2 Implicit Withdraw: 0 0 Explicit Withdraw: 0 0 Used as bestpath: n/a 2 Used as multipath: n/a 0 Outbound Inbound Local Policy Denied Prefixes: -------- ------- Bestpath from this peer: 2 n/a Invalid Path: 2 n/a Total: 4 0 Number of NLRIs in the update sent: max 1, min 0 Address tracking is enabled, the RIB does have a route to 192.0.2.1 Connections established 2; dropped 1 Last reset 08:59:57, due to Peer closed the session of session 1 Transport(tcp) path-mtu-discovery is disabled Graceful-Restart is disabled !--- Check the routes learned from BGP ---! ftd2# show route bgp Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route Gateway of last resort is 209.165.201.100 to network 0.0.0.0 B 10.1.1.0 255.255.255.0 [200/0] via 192.0.2.1, 08:59:46 B 10.1.2.0 255.255.255.0 [200/0] via 10.1.1.100, 08:59:46

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.