ASA 및 FTD에서 Microsoft Azure로의 정책 기반 및 경로 기반 VPN 구성

목차

소개

이 문서에서는 Cisco ASA 및 Cisco Secure Firewall과 Microsoft Azure 클라우드 서비스 간 VPN의 개념과 구성에 대해 설명합니다.

개념

VPN 암호화 도메인

IP 주소 범위 IPSec은 VPN 터널에 참여할 수 있습니다. 암호화 도메인은 로컬 트래픽 선택기와 원격 트래픽 선택기를 사용하여 IPSec이 캡처하고 암호화한 로컬 및 원격 서브넷 범위를 지정합니다. VPN 암호화 도메인을 정의하는 방법에는 두 가지가 있습니다. 경로 기반 또는 정책 기반 트래픽 선택기

경로 기반:
암호화 도메인은 IPSec 터널로 들어오는 모든 트래픽을 허용하도록 설정됩니다. IPSec 로컬 및 원격 트래픽 선택기는 0.0.0.0으로 설정됩니다. 이는 IPSec 터널로 라우팅되는 모든 트래픽이 소스/대상 서브넷에 관계없이 암호화됨을 의미합니다.

Cisco ASA(Adaptive Security Appliance)는 버전 9.8 이상에서 VTI(Virtual Tunnel Interface)를 사용하여 경로 기반 VPN을 지원합니다.

FMC(Firepower Management Center)에서 관리하는 Cisco Secure Firewall 또는 FTD(Firepower Threat Defense)는 버전 6.7 이상에서 VTI를 사용하여 경로 기반 VPN을 지원합니다.

정책 기반:

암호화 도메인은 소스와 대상 모두에 대해 특정 IP 범위만 암호화하도록 설정됩니다. 정책 기반 로컬 트래픽 선택기 및 원격 트래픽 선택기는 IPSec을 통해 암호화할 트래픽을 식별합니다.

ASA는 버전 8.2 이상에서 암호화 맵과 함께 정책 기반 VPN을 지원합니다.

Microsoft Azure는 경로 기반, 정책 기반 또는 시뮬레이션된 정책 기반 트래픽 선택기를 사용하는 경로 기반을 지원합니다. Azure는 현재 선택한 VPN 방법을 기반으로 구성할 수 있는 IKE(Internet Key Exchange) 버전을 제한하고 있습니다. 경로 기반에는 IKEv2가 필요하고 정책 기반에는 IKEv1이 필요합니다. 즉, IKEv2를 사용하는 경우 Azure에서 경로 기반을 선택하고 ASA에서 VTI를 사용해야 하지만, ASA에서 코드 버전 때문에 암호화 맵만 지원하는 경우 정책 기반 트래픽 선택기를 사용하여 경로 기반에 대해 Azure를 구성해야 합니다. 이 작업은 Microsoft에서 UsePolicyBasedTrafficSelectors를 호출하는 옵션을 구현하기 위해 PowerShell 스크립트 배포를 통해 Azure 포털에서 수행됩니다. https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps

ASA 및 FTD 컨피그레이션 관점에서 요약하려면

- 암호화 맵으로 구성된 ASA/FTD의 경우 Azure는 정책 기반 VPN 또는 UsePolicyBasedTrafficSelectors로 경로 기반에 대해 구성해야 합니다.
- VTI로 구성된 ASA의 경우 경로 기반 VPN에 대해 Azure를 구성해야 합니다.
- FTD의 경우 VTI를 구성하는 방법에 대한 자세한 내용은 여기에서 확인할 수 있습니다. https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/firepower_threat_defense_site_to_site_vpns.html#concept_ccj_p4r_cmb

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA에서 VTI를 사용하는 IKEv2 경로 기반 VPN의 경우: ASA 코드 버전 9.8(1) 이상 (경로 기반 VPN에 대해 Azure를 구성해야 합니다.)
- ASA 및 FTD에서 암호화 맵을 사용하는 IKEv1 정책 기반 VPN의 경우: ASA 코드 버전 8.2 이상 및 FTD 6.2.0 이상(정책 기반 VPN에 대해 Azure를 구성해야 함)
- 정책 기반 트래픽 선택기와 함께 ASA에서 암호화 맵을 사용하는 IKEv2 경로 기반 VPN의 경우: 암호화 맵으로 구성된 ASA 코드 버전 8.2 이상 (UsePolicyBasedTrafficSelectors를 사용하여 경로 기반 VPN에 대해 Azure를 구성해야 합니다.)
- FTD 관리 및 구성에 대한 FMC 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA
- Microsoft Azure

- Cisco FTD
- Cisco FMC

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

구성

구성 단계를 완료합니다. IKEv1, VTI를 통한 IKEv2 경로 기반 또는 정책 기반 트래픽 선택기 사용(ASA의 암호화 맵)을 통한 IKEv2 경로 기반 구성 중 하나를 선택합니다.

ASA의 IKEv1 컨피그레이션

ASA에서 Azure로의 사이트 간 IKEv1 VPN의 경우 다음 ASA 컨피그레이션을 따릅니다. Azure 포털에서 정책 기반 터널을 구성해야 합니다. 이 예에서는 ASA에서 암호화 맵이 사용됩니다.

ASA의 전체 IKEv1 컨피그레이션 정보는 이 Cisco 문서를 참조하십시오.

1단계. 외부 인터페이스에서 IKEv1을 활성화합니다.

```
Cisco-ASA(config)#crypto ikev1 enable outside
```

2단계. 해시, 인증, Diffie-Hellman 그룹, 수명 및 암호화에 사용할 알고리즘/방법을 정의하는 IKEv1 정책을 생성합니다.

> **참고:** 나열된 1단계 IKEv1 특성은 이 공개적으로 제공되는 Microsoft 문서에서 가장 효과적으로 제공됩니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto ikev1 policy 1
Cisco-ASA(config-ikev1-policy)#authentication pre-share
Cisco-ASA(config-ikev1-policy)#encryption aes
Cisco-ASA(config-ikev1-policy)#hash sha
Cisco-ASA(config-ikev1-policy)#group 2
Cisco-ASA(config-ikev1-policy)#lifetime 28800
```

3단계. IPsec 특성 아래에 터널 그룹을 만들고 피어 IP 주소 및 터널 사전 공유 키를 구성합니다.

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
```

4단계. 암호화 및 터널링할 트래픽을 정의하는 액세스 목록을 생성합니다. 이 예에서 관심 트래픽은 터널에서 10.2.2.0 서브넷에서 10.1.1.0으로 이동하는 트래픽입니다. 사이트 사이에 여러 서브넷이 포함된 경우 여러 항목을 포함할 수 있습니다.

버전 8.4 이상에서는 네트워크, 서브넷, 호스트 IP 주소 또는 여러 개체의 컨테이너 역할을 하는 개체 또는 개체 그룹을 만들 수 있습니다. 로컬 및 원격 서브넷이 있는 두 객체를 생성하여 암호화 ACL(Access Control List) 및 NAT(Network Address Translation) 문 모두에 사용합니다.

```
Cisco-ASA(config)#object network 10.2.2.0_24
Cisco-ASA(config-network-object)#subnet 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.1.1.0_24
Cisco-ASA(config-network-object)#subnet 10.1.1.0 255.255.255.0

Cisco-ASA(config)#access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

5단계. TS(Transform Set)를 구성합니다. 이 설정에는 키워드가 포함되어야 합니다.**IKEv1**. 원격 엔드에도 동일한 TS를 생성해야 합니다.

> **참고:** 나열된 2단계 IKEv1 특성은 공개적으로 제공되는 이 Microsoft 문서에서 가장 효과적으로 제공됩니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

6단계. 암호화 맵을 구성하고 다음 구성 요소가 있는 외부 인터페이스에 적용합니다.
·피어 IP 주소
·원하는 트래픽이 포함된 정의된 액세스 목록
·TS
·구성이 PFS(Perfect Forwarding Secrecy)를 설정하지 않았습니다. 공개적으로 사용할 수 있는 Azure 설명서에는 PFS가 Azure의 IKEv1에 대해 비활성화되어 있습니다. 데이터를 보호하기 위해 사용되는 새 Diffie-Hellman 키 쌍을 생성하는 선택적 PFS 설정은 다음 컨피그레이션을 사용하여 활성화할 수 있습니다. 이 두 키는 2단계를 시작하기 전에 PFS를 활성화해야 합니다. **crypto map outside_map 20 set pfs .**
· 2단계 IPSec 수명은 공개적으로 제공되는 Azure 문서를 기반으로 합니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
Cisco-ASA(config)#crypto map outside_map 20 set ikev1 transform-set myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 3600
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes
102400000
Cisco-ASA(config)#crypto map outside_map interface outside
```

7단계. VPN 트래픽이 다른 NAT 규칙을 따르지 않는지 확인합니다. NAT 예외 규칙을 만듭니다.

```
Cisco-ASA(config)#nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination
static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

> **참고**: 여러 서브넷을 사용하는 경우 모든 소스 및 대상 서브넷으로 개체 그룹을 생성하여 NAT 규칙에서 사용해야 합니다.

```
Cisco-ASA(config)#object-group network 10.x.x.x_SOURCE
Cisco-ASA(config-network-object-group)#network-object 10.4.4.0 255.255.255.0
```

```
Cisco-ASA(config-network-object-group)#network-object 10.2.2.0 255.255.255.0

Cisco-ASA(config)#object network 10.x.x.x_DESTINATION
Cisco-ASA(config-network-object-group)#network-object 10.3.3.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.1.1.0 255.255.255.0

Cisco-ASA(config)#nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE
destination static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

ASA Code 9.8(1) 이상에서 VTI를 사용하는 IKEv2 경로 기반

ASA 코드에서 사이트 대 사이트 IKEv2 경로 기반 VPN의 경우 이 컨피그레이션을 따릅니다. Azure가 경로 기반 VPN에 대해 구성되어 있는지 확인하고 Azure 포털에서 UsePolicyBasedTrafficSelectors를 구성하지 마십시오. VTI는 ASA에 구성됩니다.

전체 ASA VTI 컨피그레이션 정보는 이 Cisco 문서를 참조하십시오.

1단계. 외부 인터페이스에서 IKEv2를 활성화합니다.

```
Cisco-ASA(config)#crypto ikev2 enable outside
```

2단계. IKEv2 1단계 정책을 추가합니다.

> **참고**: Microsoft는 Azure에서 사용하는 특정 IKEv2 1단계 암호화, 무결성 및 수명 특성과 충돌하는 정보를 게시했습니다. 나열된 특성은 공개적으로 제공되는 이 Microsoft 문서에서 가장 효과적으로 제공됩니다. Microsoft의 IKEv2 특성과 충돌하는 정보가 여기에 표시됩니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

3단계. IKEv2 2단계 IPsec 제안서를 추가합니다. 암호화 IPsec에서 보안 매개변수를 지정합니다 **ikev2 ipsec-proposal** 컨피그레이션 모드:

프로토콜 esp 암호화 {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
프로토콜 esp 무결성 {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

> **참고:** Microsoft는 Azure에서 사용되는 특정 2단계 IPSec 암호화 및 무결성 특성과 관련하여 상충되는 정보를 게시했습니다. 나열된 특성은 공개적으로 제공되는 이 Microsoft 문서에서 가장 효과적으로 제공됩니다. Microsoft의 2단계 IPSec 특성과 충돌하는 정보가 여기에 표시됩니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

4단계. 다음을 지정하는 IPSec 프로필을 추가합니다.

- 이전에 구성한 ikev2 2단계 IPSec 제안
- 2단계 IPSec 수명(선택 사항)(초 및/또는 킬로바이트)
- PFS 그룹(선택 사항)

참고: Microsoft는 Azure에서 사용되는 특정 2단계 IPSec 수명 및 PFS 특성과 관련하여 상충되는 정보를 게시했습니다. 나열된 특성은 공개적으로 제공되는 이 Microsoft 문서에서 가장 효과적으로 제공됩니다. Microsoft의 2단계 IPSec 특성과 충돌하는 정보가 여기에 표시됩니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto ipsec profile PROFILE1
Cisco-ASA(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-profile)#set security-association lifetime seconds 27000
Cisco-ASA(config-ipsec-profile)#set security-association lifetime kilobytes unlimited
Cisco-ASA(config-ipsec-profile)#set pfs none
```

5단계. IPsec 특성 아래에 터널 그룹을 만들고 피어 IP 주소 및 IKEv2 로컬 및 원격 터널 사전 공유 키를 구성합니다.

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key cisco
Cisco-ASA(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key cisco
```

6단계. 다음을 지정하는 VTI를 생성합니다.

- 새 터널 인터페이스 번호: 인터페이스 터널 [번호]
- 새 터널 인터페이스 이름: nameif [이름]
- 터널 인터페이스에 존재하지 않는 IP 주소: ip 주소 [ip-address] [mask]
- VPN이 로컬로 종료되는 터널 소스 인터페이스: 터널 소스 인터페이스 [int-name]
- Azure 게이트웨이 IP 주소: 터널 대상 [Azure 공용 IP]
- IPSec IPv4 모드: 터널 모드 ipsec ipv4
- 이 VTI에 사용할 IPSec 프로파일: 터널 보호 ipsec 프로필 [profile-name]

```
Cisco-ASA(config)#interface tunnel 100
Cisco-ASA(config-if)#nameif vti
Cisco-ASA(config-if)#ip address 169.254.0.1 255.255.255.252
Cisco-ASA(config-if)#tunnel source interface outside
Cisco-ASA(config-if)#tunnel destination [Azure Public IP]
Cisco-ASA(config-if)#tunnel mode ipsec ipv4
Cisco-ASA(config-if)#tunnel protection ipsec profile PROFILE1
```

7단계. 고정 경로를 생성하여 터널을 향하는 트래픽을 지정합니다. 고정 경로를 추가하려면 다음 명령을 입력합니다.

route if_name dest_ip mask gateway_ip [distance]

이 **dest_ip** 및 **mask** 은 Azure 클라우드의 대상 네트워크에 대한 IP 주소입니다(예: 10.0.0.0/24). gateway_ip는 터널 인터페이스 서브넷의 IP 주소(예: 169.254.0.2)여야 합니다. 이 gateway_ip의 목적은 터널 인터페이스로 트래픽을 보내는 것이지만 특정 게이트웨이 IP 자체는 중요하지 않습니다.

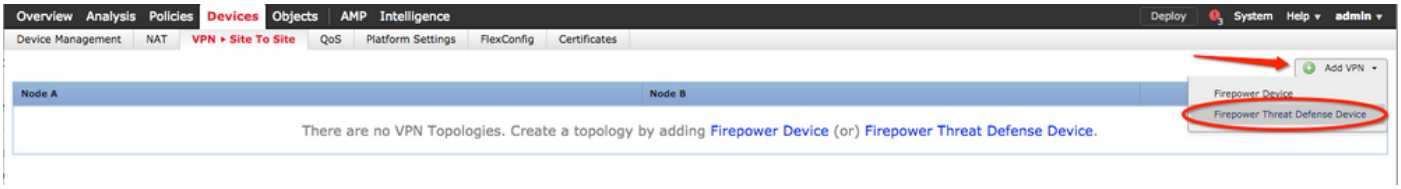
```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

FTD의 IKEv1 컨피그레이션

FTD에서 Azure로의 Site-to-Site IKEv1 VPN의 경우 FTD 디바이스를 FMC에 미리 등록해야 합니다 .

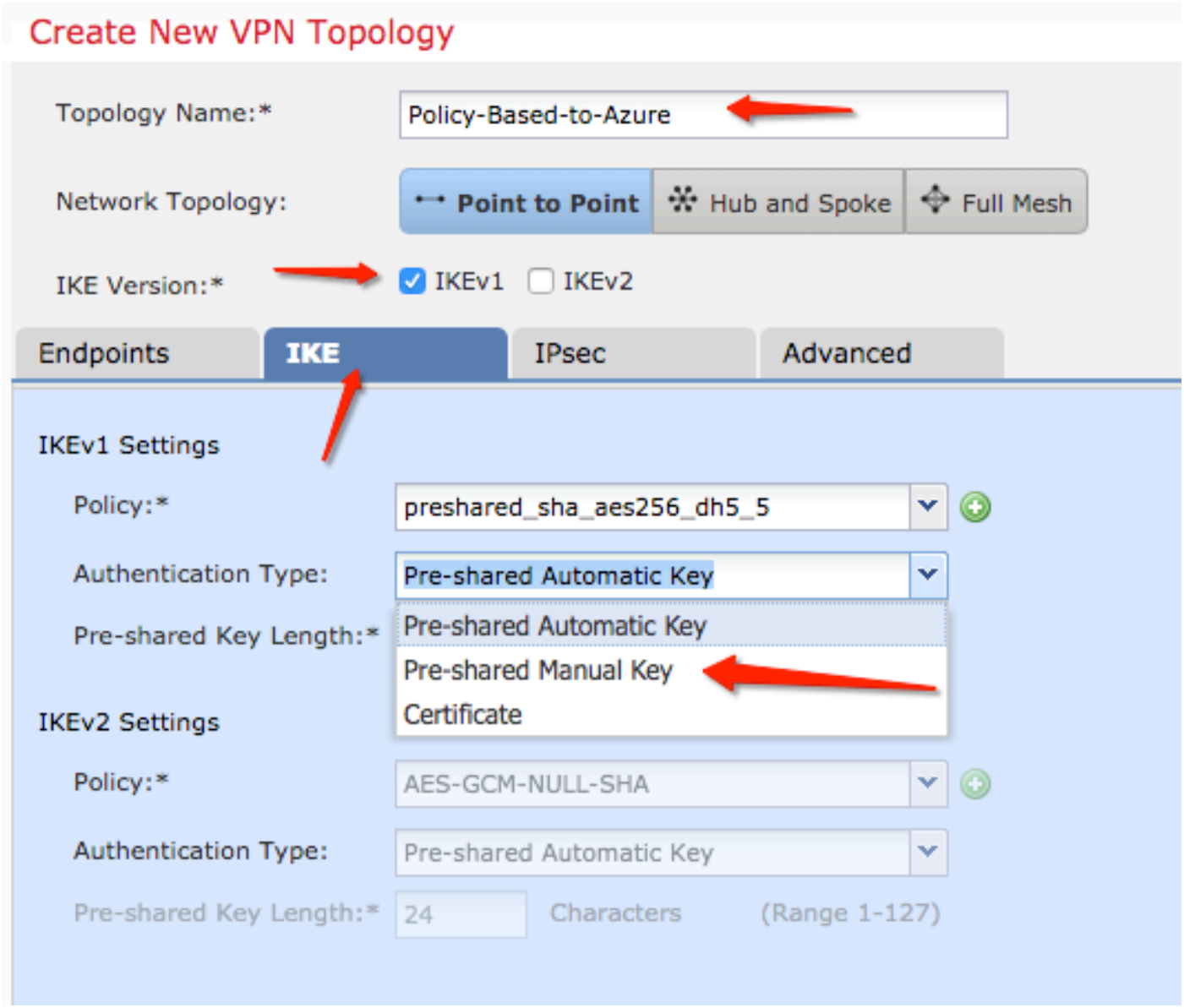
1단계. Site-to-Site 정책을 생성합니다. 탐색 **FMC dashboard > Devices > VPN > Site to Site**.

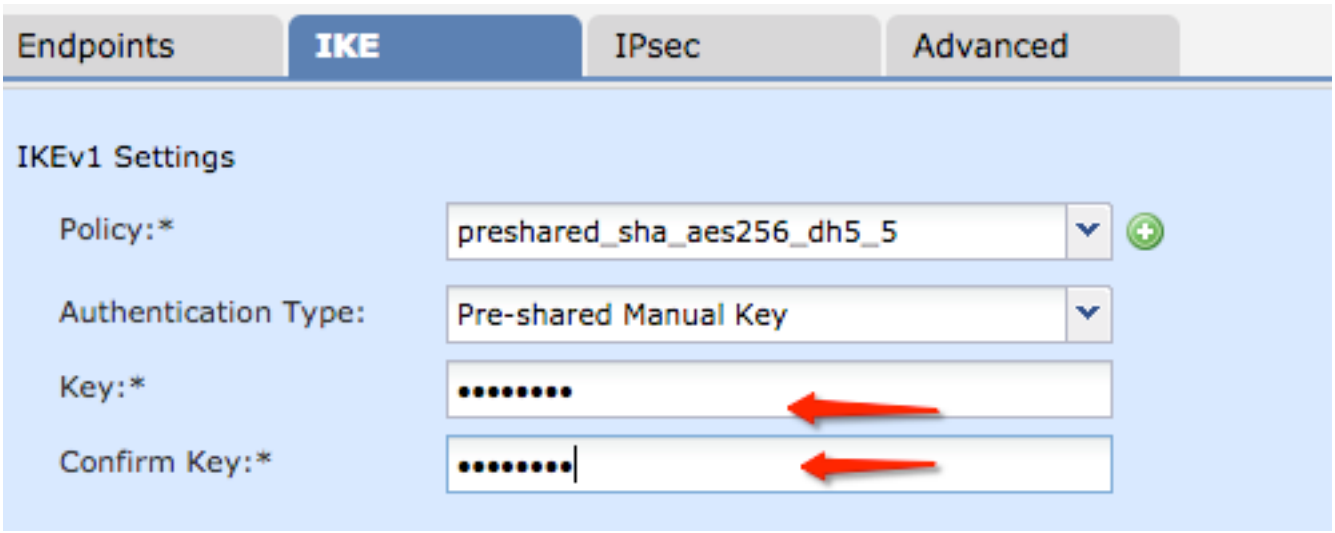
2단계. 새 정책을 생성합니다. 다음을 클릭합니다. **Add VPN** 드롭다운 메뉴 및 선택 **Firepower Threat Defense device** .



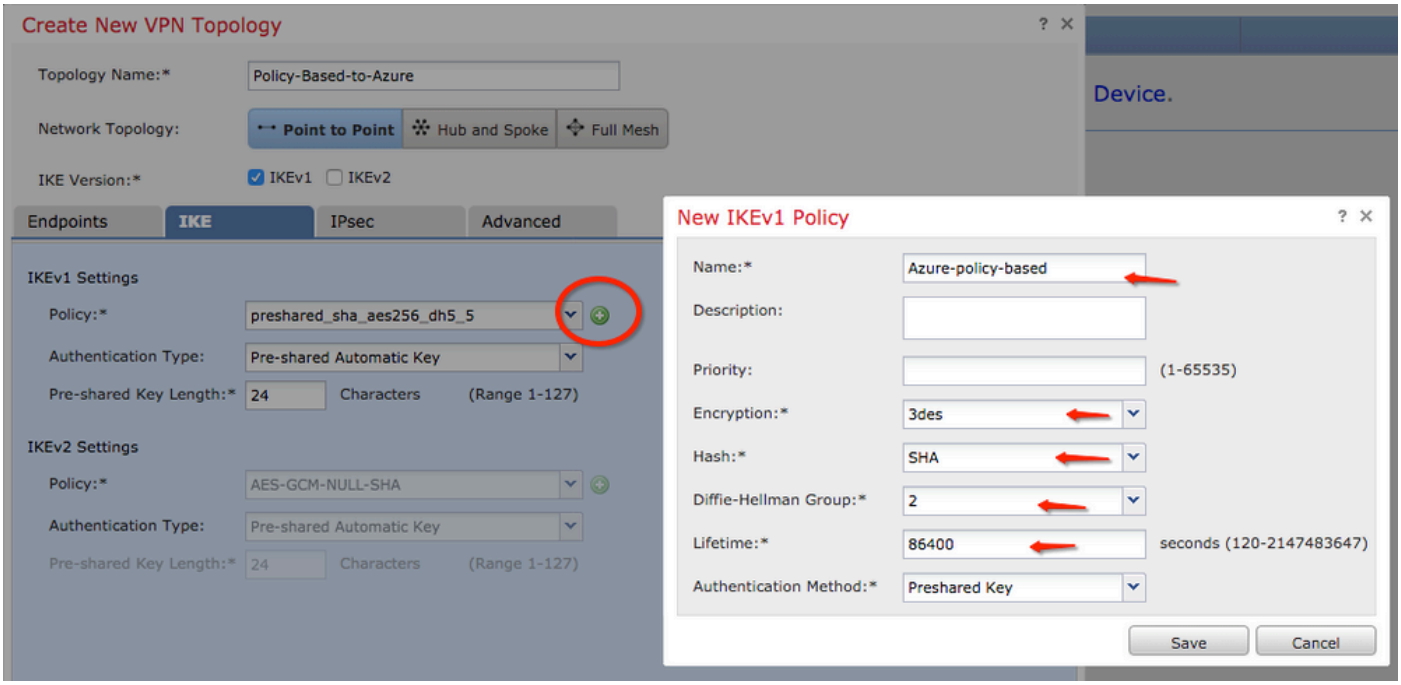
3단계. **Create new VPN Topology** 창에서 **Topology Name**, **IKEV1** 프로토콜 확인란을 클릭하고 **IKE** 탭. 이 예에서는 사전 공유 키가 인증 방법으로 사용됩니다.

다음을 클릭합니다. **Authentication Type** 드롭다운 메뉴, **Pre-shared manual key** . 수동 사전 공유 키를 **Key** 및**Confirm Key** 텍스트 필드.

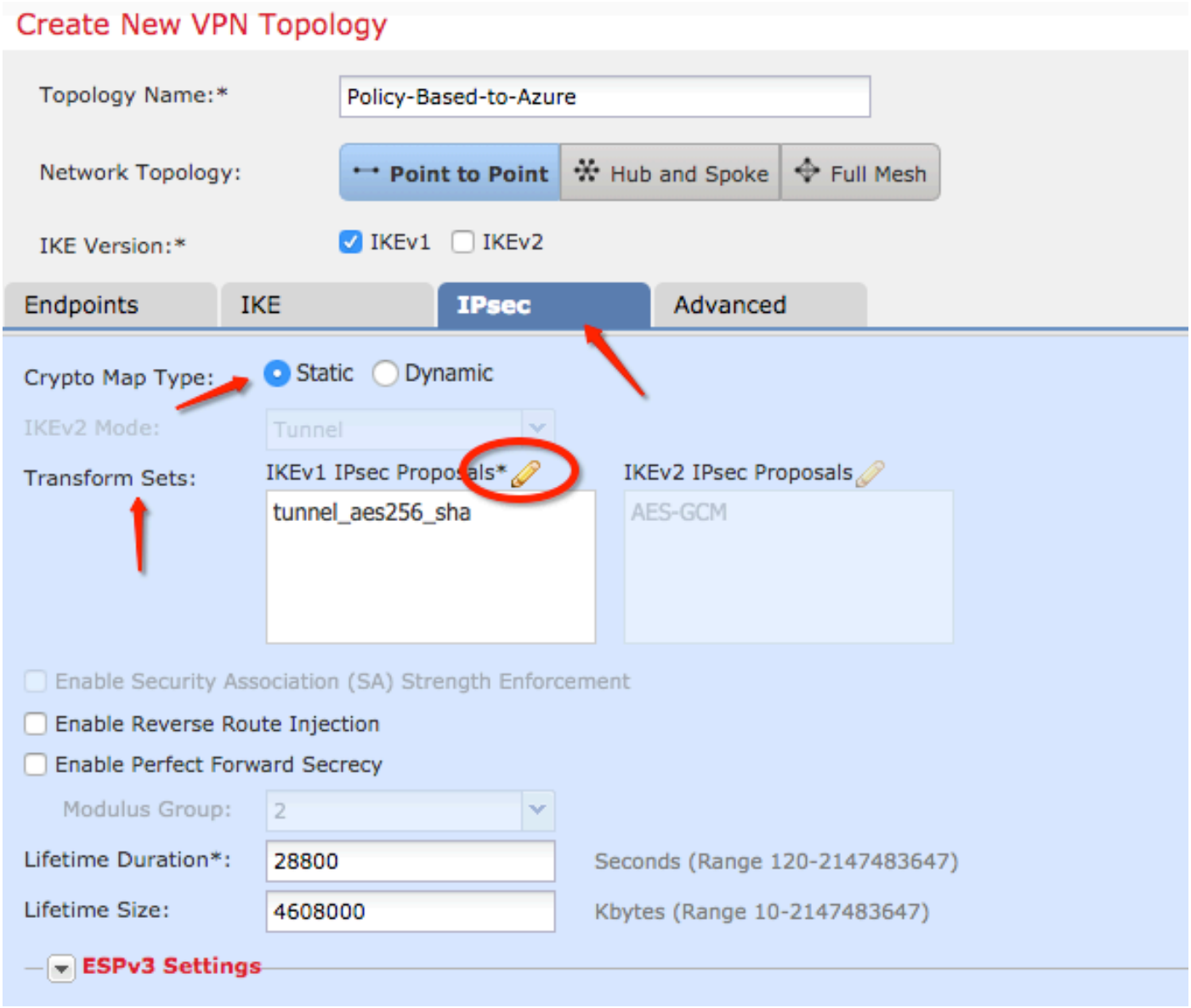




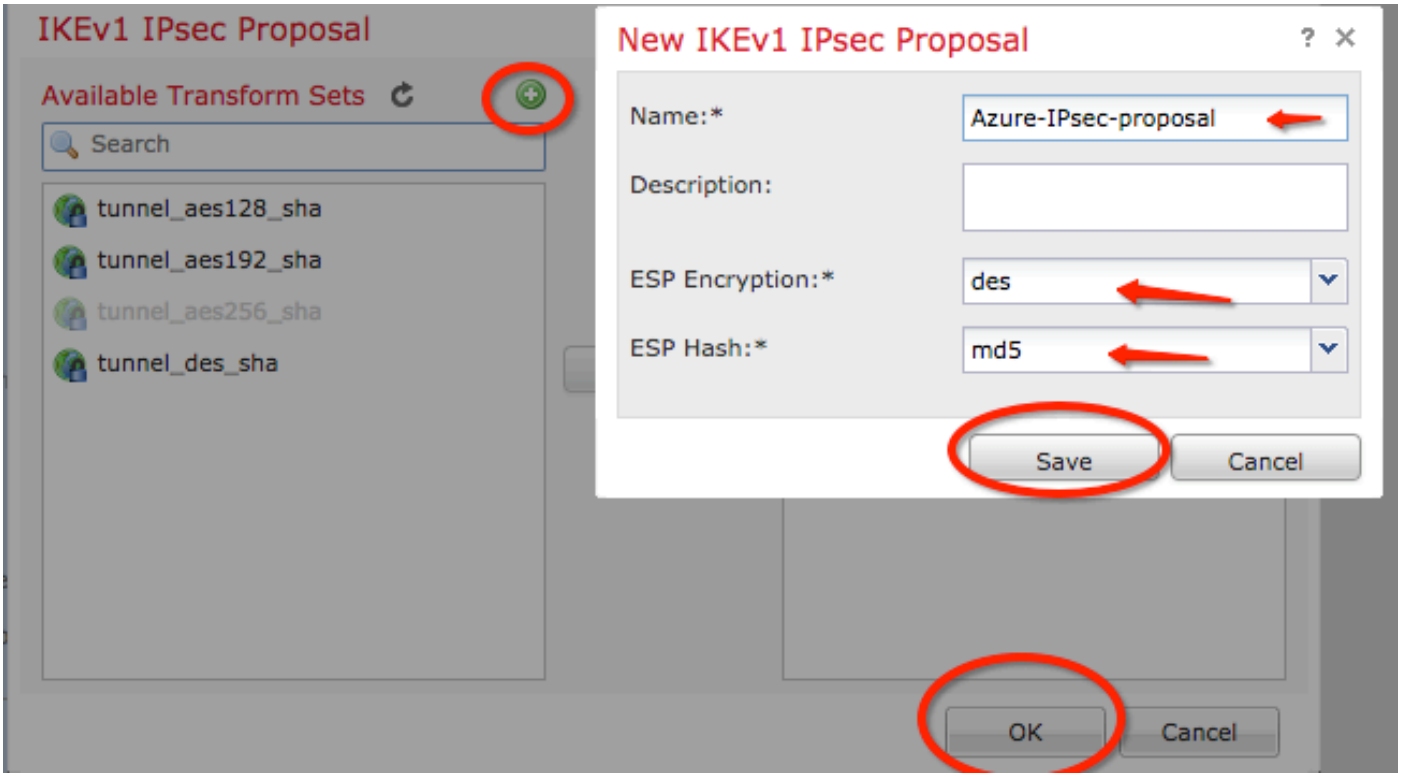
4단계. 새 매개변수를 생성하여 ISAKMP 정책 또는 1단계 매개변수를 구성합니다. 같은 창에서 **green plus button** 새 ISAKMP 정책을 추가합니다. 정책의 이름을 지정하고 원하는 Encryption(암호화), Hash(해시), Diffie-Hellman Group(Diffie-Hellman 그룹), Lifetime(수명) 및 Authentication Method(인증 방법)를 선택한 다음 **Save** .



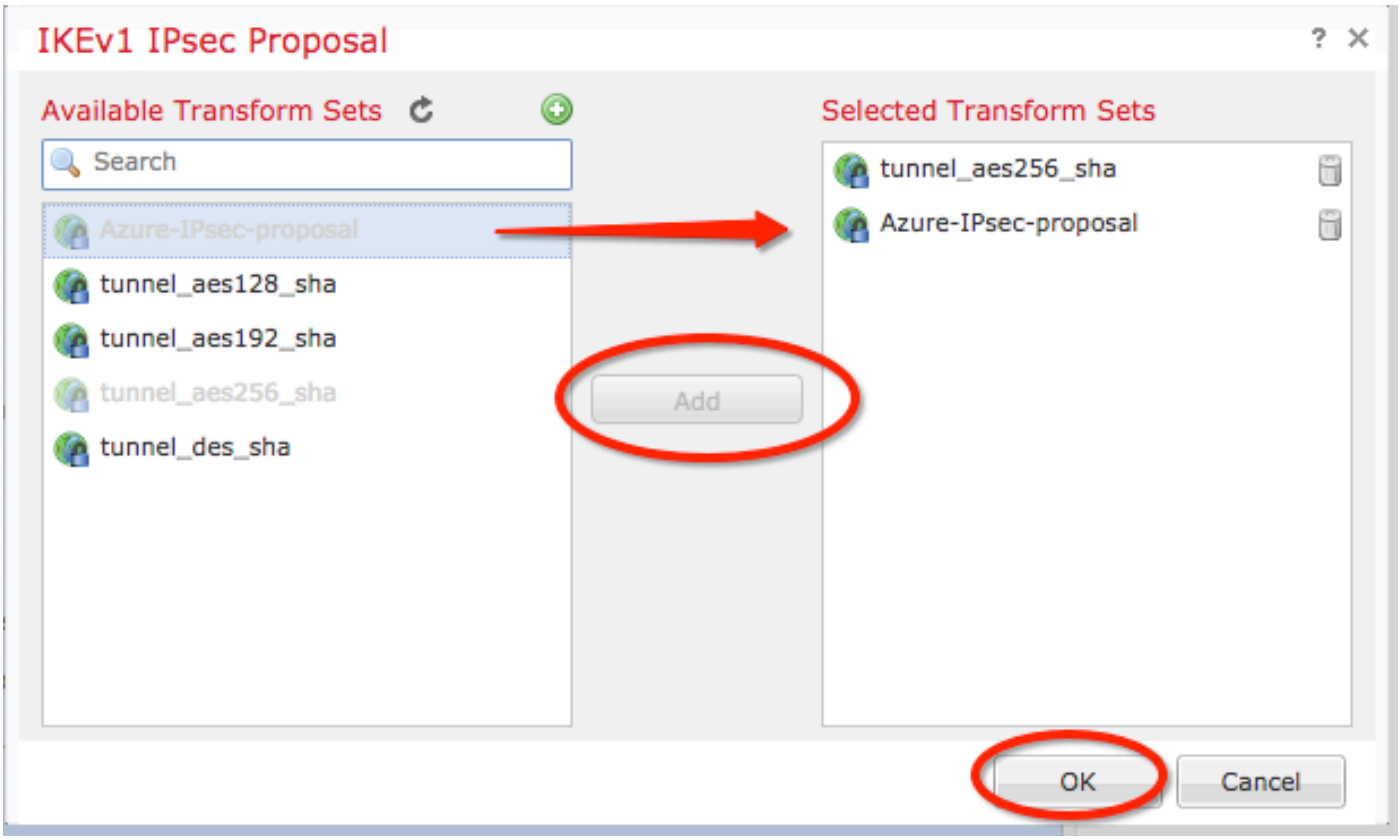
5단계. IPsec 정책 또는 2단계 매개변수를 구성합니다. 탐색 **IPsec** 탭, 선택 **Static** 에 **Crypto Map Type** 확인란을 선택합니다. 다음을 클릭합니다. **edit pencil** 아이콘 **IKEV1 IPsec Proposals** 에 **Transform Sets** 옵션을 선택합니다.



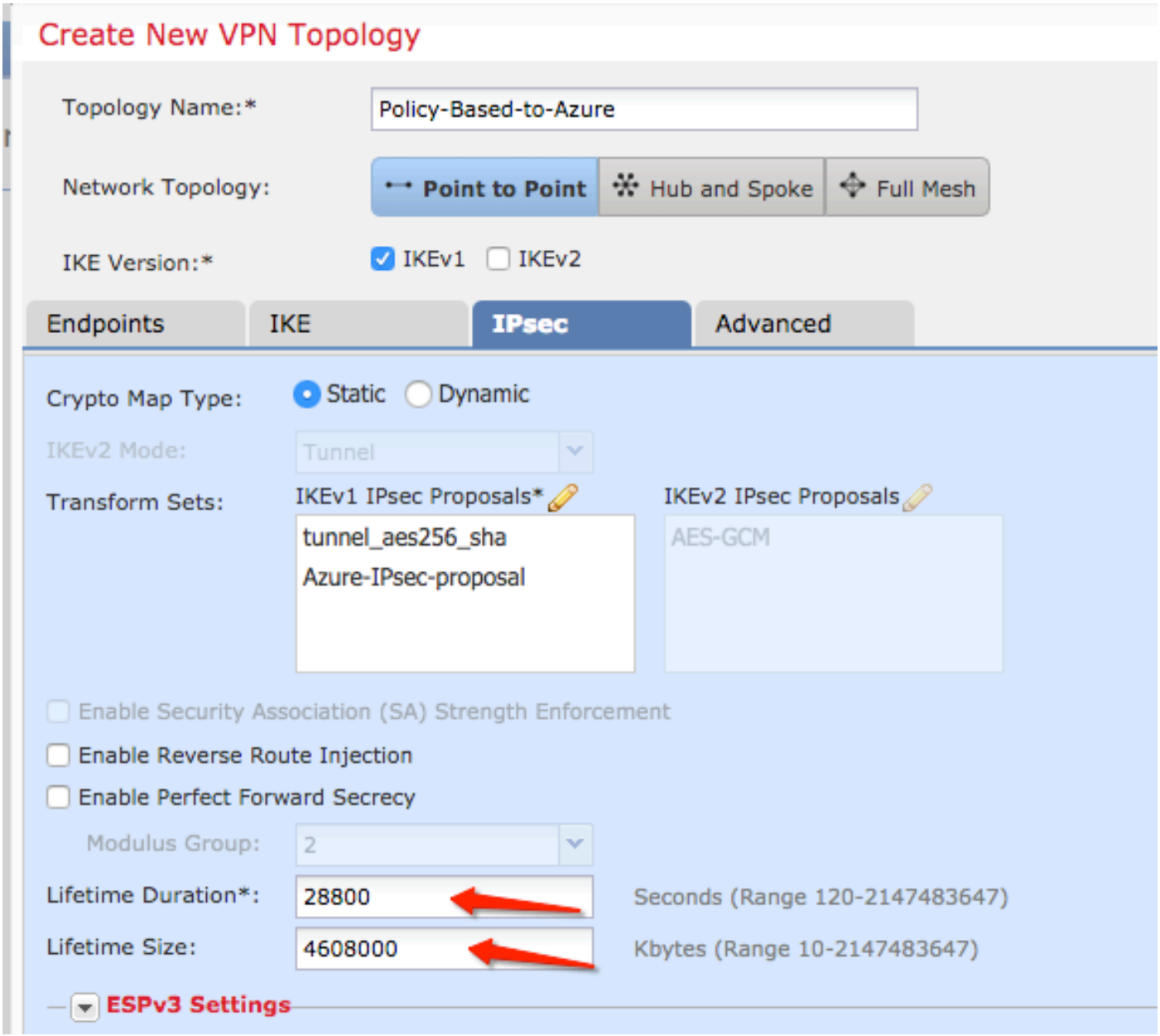
6단계. 새 IPsec 제안을 만듭니다. 에 **IKEv1 IPSec Proposal** 창에서 **green plus button** 새 파일을 추가합니다. ESP 암호화 및 ESP 해시 알고리즘에 대한 정책 이름 및 원하는 매개변수를 지정하고 **Save** .



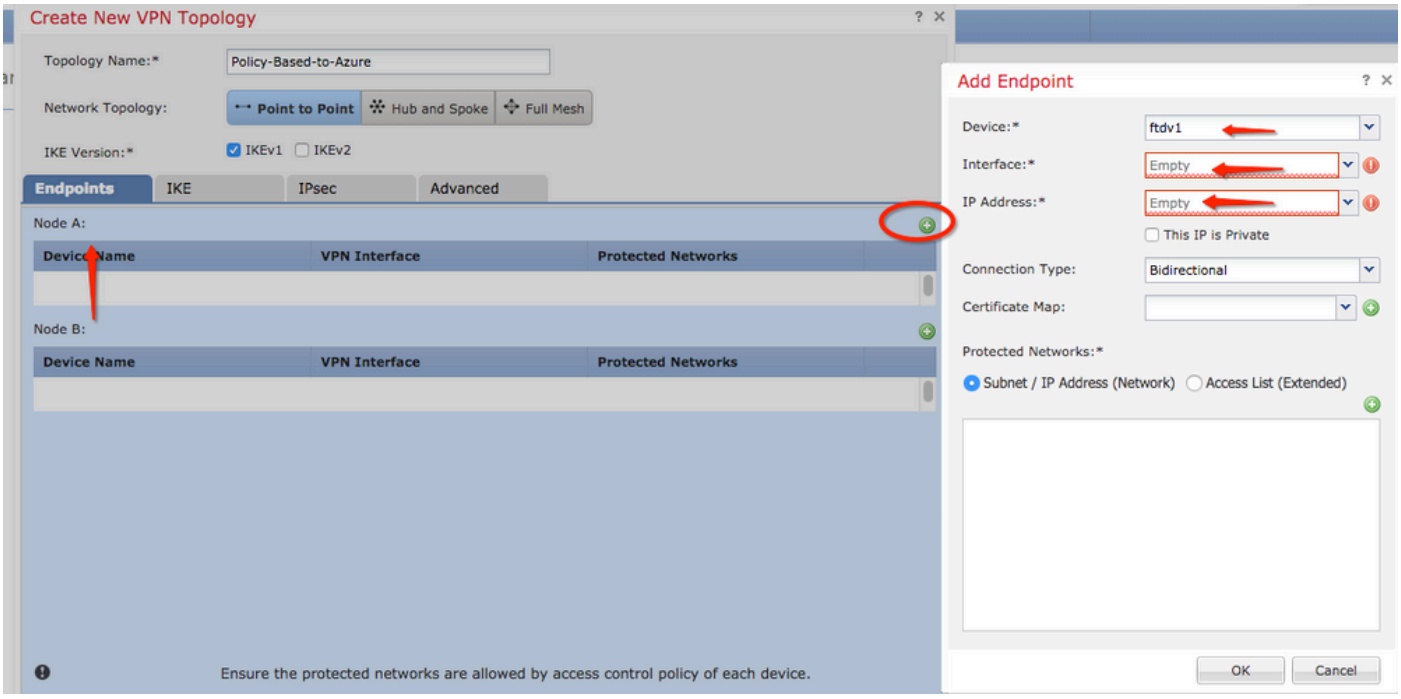
7단계. 에 **IKEV1 IPsec Proposal** 창에 새 IPsec 정책을 **Selected Transform Sets** 섹션 및 클릭 **OK** .



8단계. **IPSec** 탭에서 원하는 수명 기간 및 크기를 구성합니다.



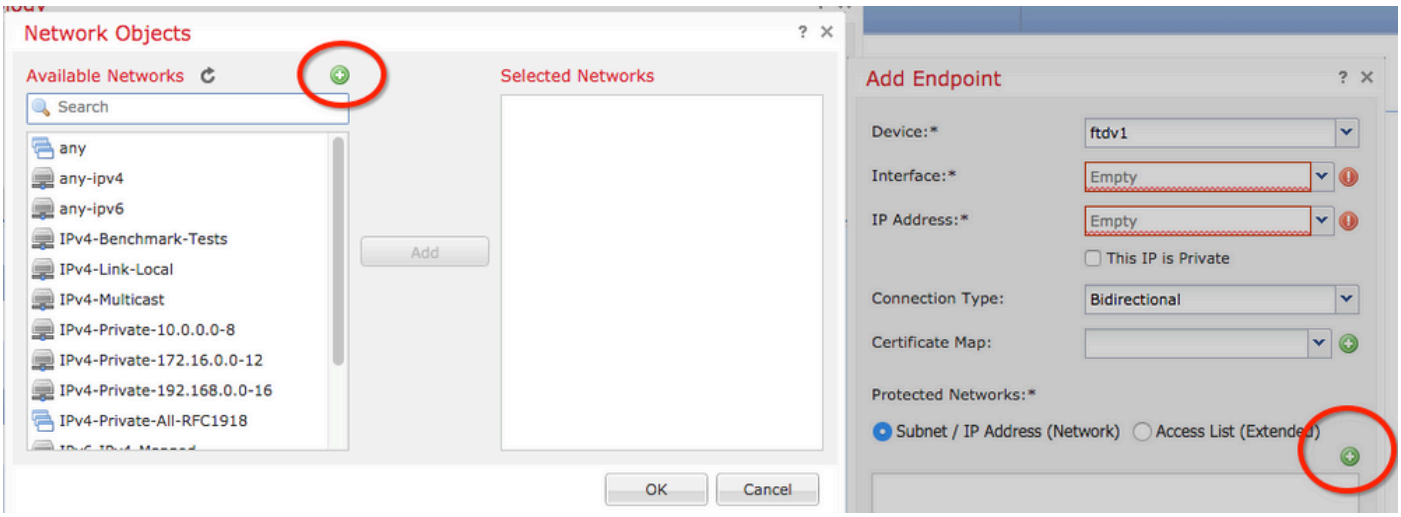
9단계. 암호화 도메인/트래픽 선택기/보호된 네트워크를 선택합니다. 탐색 **Endpoints** 탭. 에 **Node A** 섹션 **green plus button** 새 파일을 추가합니다. 이 예에서는 노드 A가 FTD에 대한 로컬 서브넷으로 사용됩니다.



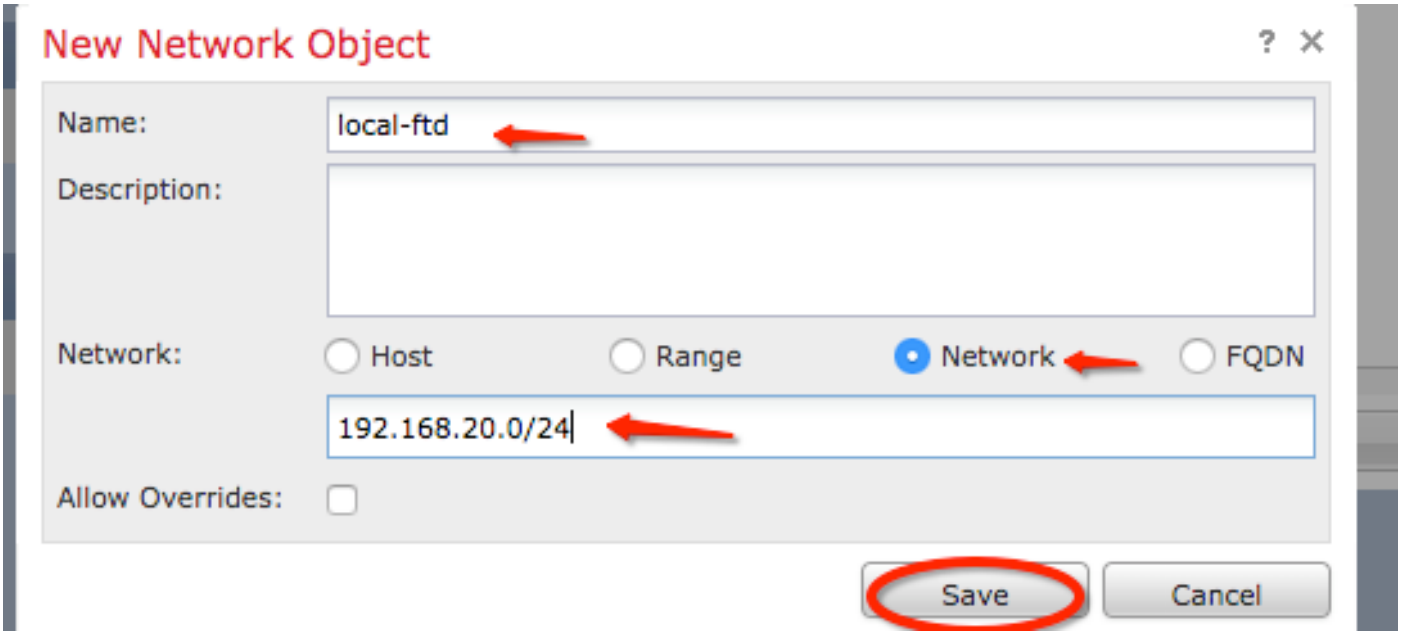
10단계. **Add Endpoint** 창에서 사용할 FTD를 **Device** 물리적 인터페이스 및 사용할 IP 주소와 함께 드롭다운 메뉴를 선택합니다.

11단계. 로컬 트래픽 선택기를 지정하려면 **Protected Networks** 옵션을 클릭하고 **green plus button** 새 객체를 만듭니다.

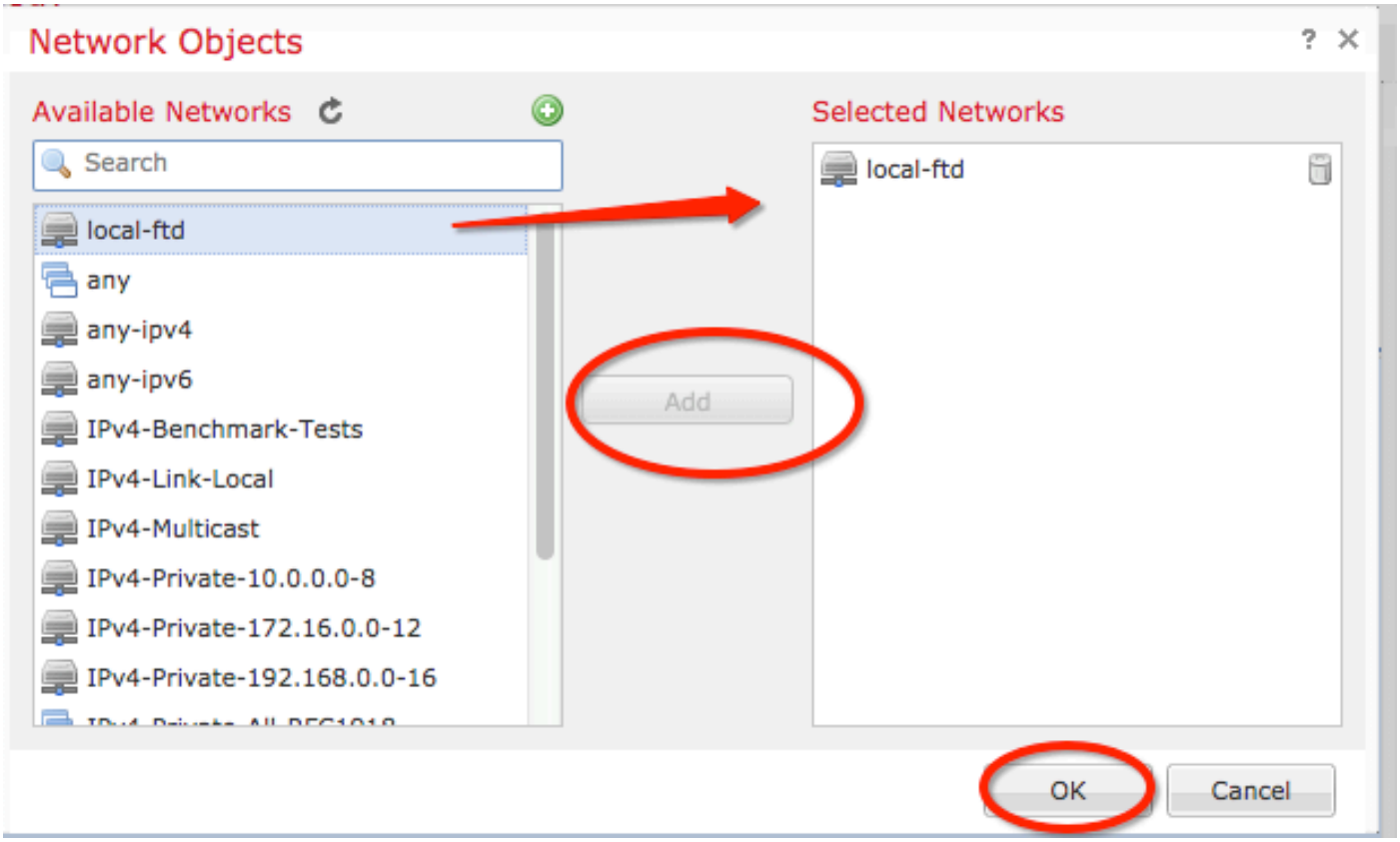
12단계. **Network Objects** 창에서 **green plus button** 옆에 **Available Networks** 텍스트를 입력하여 새 로컬 트래픽 선택기 객체를 만듭니다.



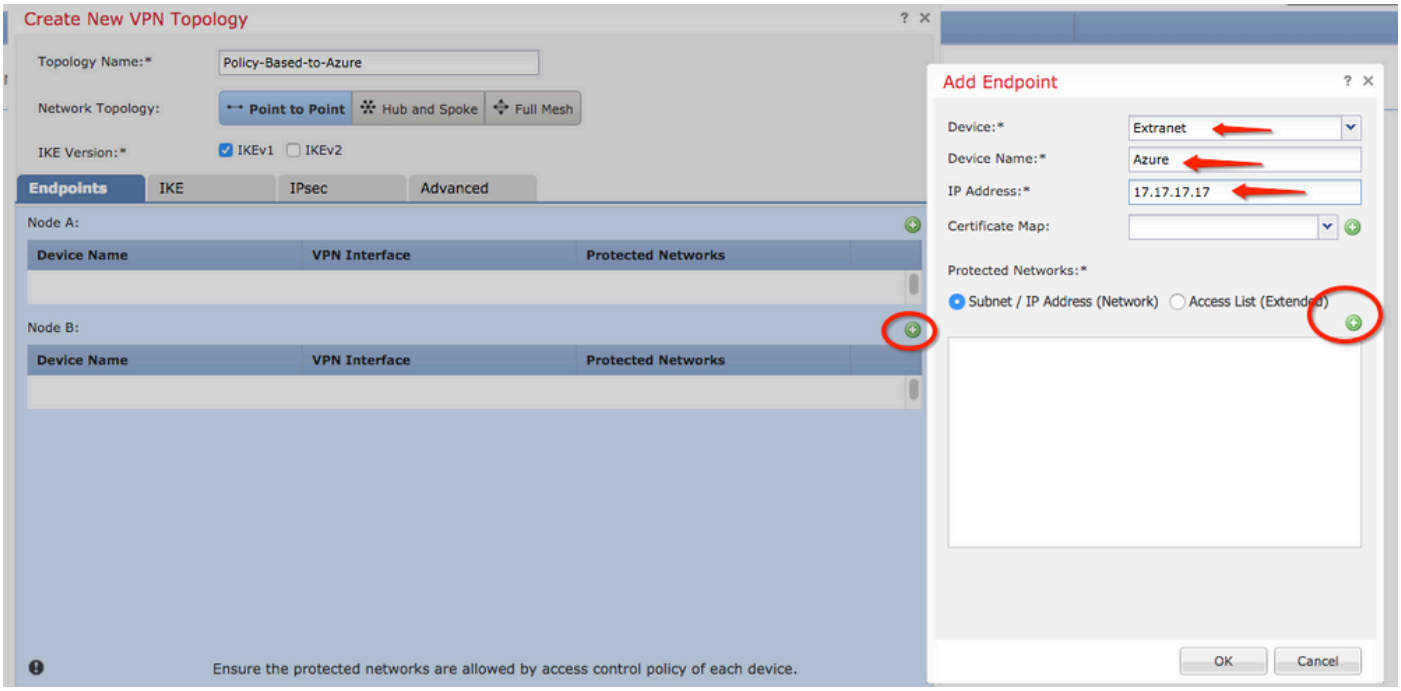
13단계. **New Network Object** 창에서 개체의 이름을 지정하고 host/network/range/FQDN을 선택합니다. 그런 다음 **Save** .



14단계. 개체를 **Selected Networks** 섹션 **Network Objects** 창에서 **OK** . 클릭 **OK** 에 **Add Endpoint** 창입니다.

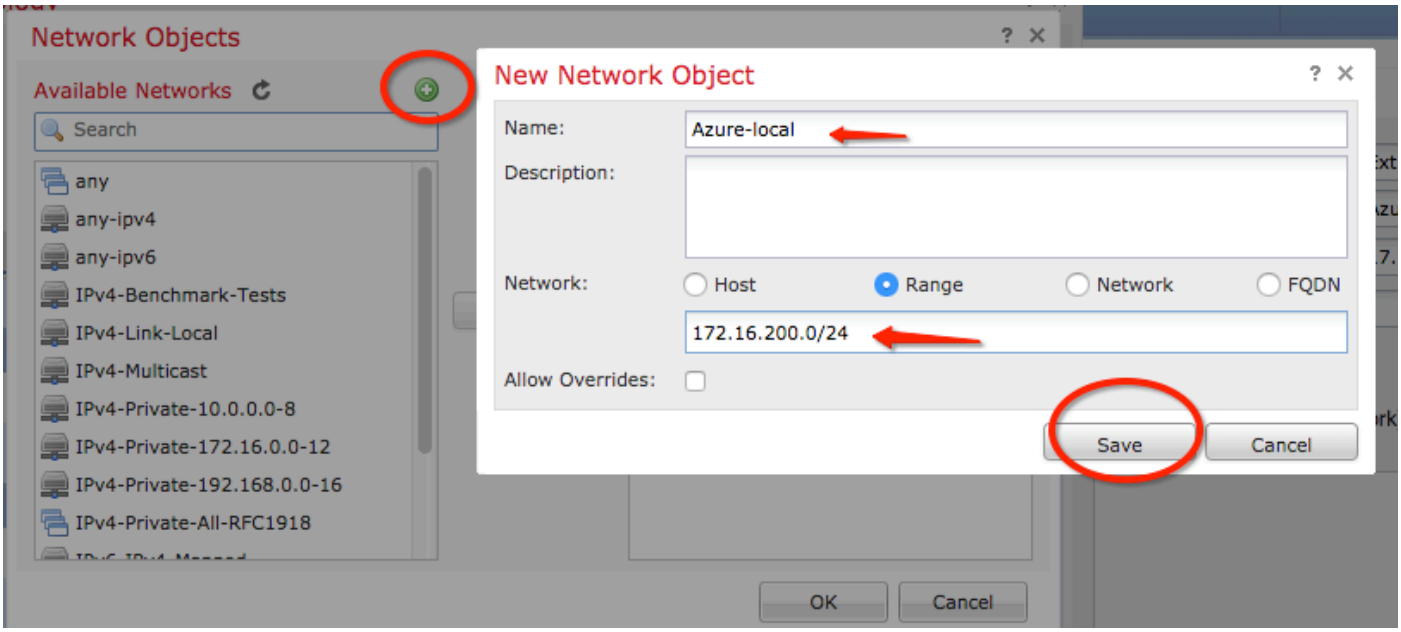


15단계. 이 예에서 Azure 끝점인 노드 B 끝점을 정의합니다. 에 **Create New VPN Topology** 창에서 **Node B** 섹션을 클릭하고 **green plus button** 원격 엔드포인트 트래픽 선택기를 추가합니다. 지정 **Extranet** 노드 A와 동일한 FMC에서 관리하지 않는 모든 VPN 피어 엔드포인트에 대해 디바이스 이름(로컬로 중요한 경우에만) 및 해당 IP 주소를 입력합니다.

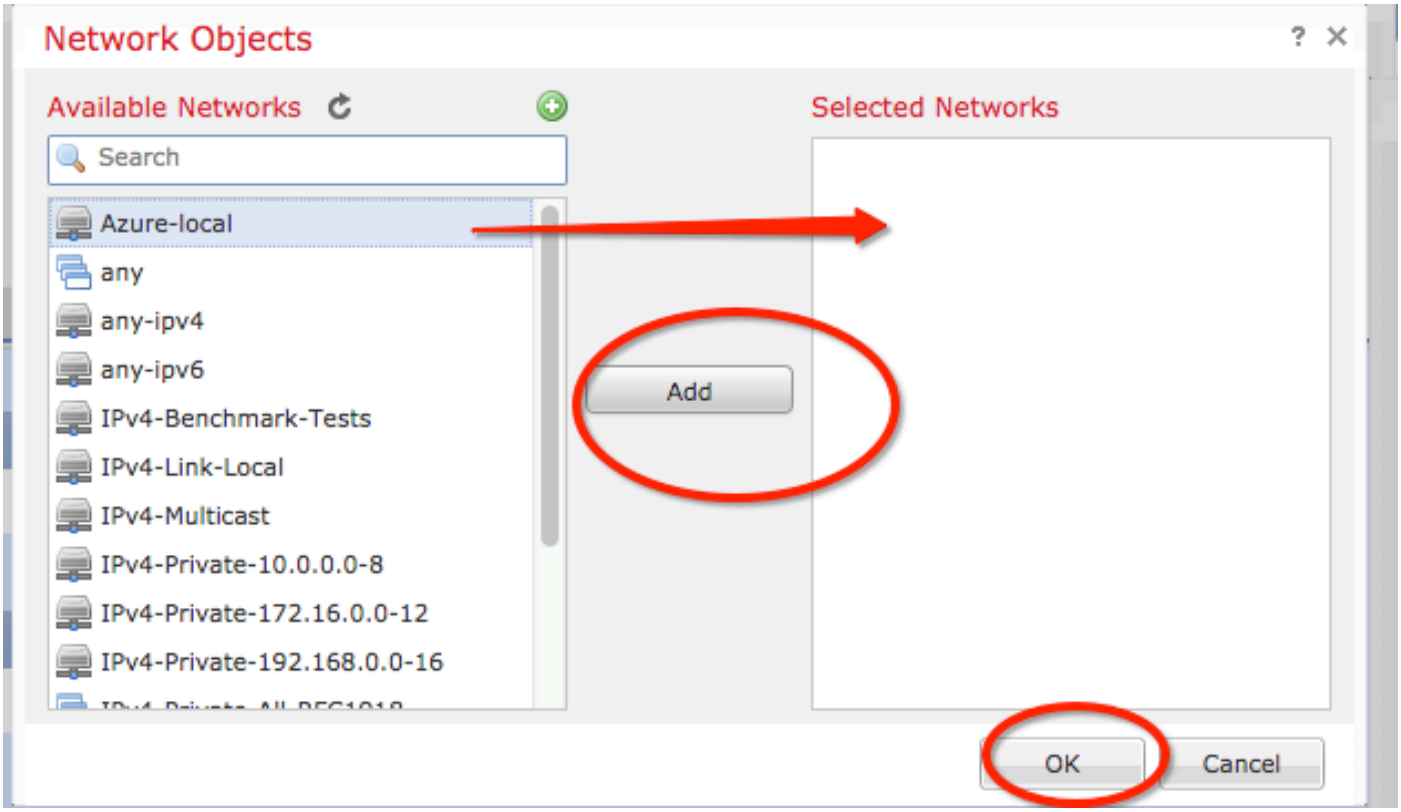


16단계. 원격 트래픽 선택기 객체를 생성합니다. 탐색 **Protected Networks** 섹션을 클릭하고 **green plus button** 새 객체를 추가합니다.

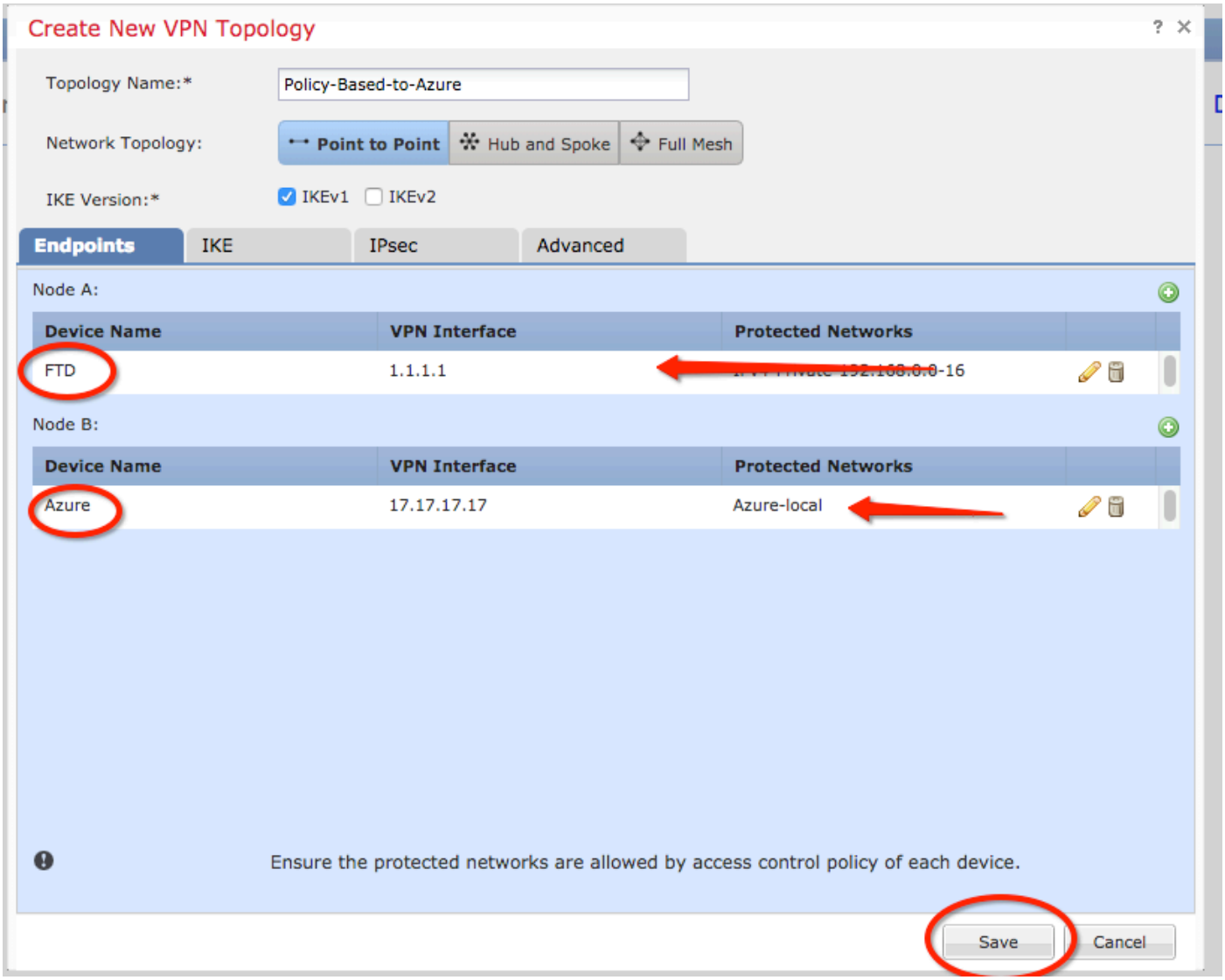
17단계. **Network Objects** 창에서 **green plus button** 옆에 **Available Networks** 새 개체를 만들 텍스트입니다. 에 **New Network Object** 창에서 개체의 이름을 지정하고 host/range/network/FQDN을 적절히 선택한 다음 **Save** .



18단계. **Network Objects** 창에 새 원격 개체를 추가합니다. **Selected Networks** 섹션 및 클릭 **OK** . 클릭 **Ok** 에 **Add Endpoint** 창입니다.



19단계. **Create New VPN Topology** 이제 올바른 트래픽 선택기/보호 네트워크가 있는 두 노드를 볼 수 있습니다. 클릭 **Save** .



20단계. FMC 대시보드에서 **Deploy** 오른쪽 상단 창에서 FTD 디바이스를 선택하고 **Deploy** .

21단계. CLI에서 VPN 컨피그레이션은 ASA 디바이스의 컨피그레이션과 동일하게 보입니다.

정책 기반 트래픽 선택기를 사용하는 IKEv2 경로 기반

암호화 맵이 있는 ASA의 사이트 간 IKEv2 VPN에 대해서는 이 컨피그레이션을 따릅니다. Azure가 경로 기반 VPN에 대해 구성되어 있는지 확인하고 PowerShell을 사용하여 Azure 포털에서 UsePolicyBasedTrafficSelectors를 구성해야 합니다.

Microsoft에서 제공하는 이 문서에서는 경로 기반 Azure VPN 모드와 함께 UsePolicyBasedTrafficSelector를 구성하는 방법을 설명합니다. 이 단계를 완료하지 않으면 Azure에서 수신한 트래픽 선택기가 일치하지 않아 암호화 맵이 있는 ASA에서 연결을 설정하지 못합니다.

암호화 맵 컨피그레이션 정보가 포함된 전체 ASA IKEv2에 대해서는 이 Cisco 문서를 참조하십시오 .

1단계. 외부 인터페이스에서 IKEv2를 활성화합니다.

```
Cisco-ASA(config)#crypto ikev2 enable outside
```

2단계. IKEv2 1단계 정책을 추가합니다.

> **참고**: Microsoft는 Azure에서 사용하는 특정 IKEv2 1단계 암호화, 무결성 및 수명 특성과 충돌하는 정보를 게시했습니다. 나열된 특성은 공개적으로 제공되는 이 Microsoft 문서에서 가장 효과적으로 제공됩니다. 충돌하는 Microsoft의 IKEv2 특성 정보가 여기에 표시됩니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

3단계. IPsec 특성 아래에 터널 그룹을 만들고 피어 IP 주소 및 IKEv2 로컬 및 원격 터널 사전 공유 키를 구성합니다.

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key cisco
Cisco-ASA(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key cisco
```

4단계. 암호화 및 터널링할 트래픽을 정의하는 액세스 목록을 생성합니다. 이 예에서 관심 트래픽은 터널에서 10.2.2.0 서브넷에서 10.1.1.0으로 이동하는 트래픽입니다. 사이트 사이에 여러 서브넷이 포함된 경우 여러 항목을 포함할 수 있습니다.

버전 8.4 이상에서는 네트워크, 서브넷, 호스트 IP 주소 또는 여러 개체의 컨테이너 역할을 하는 개체 또는 개체 그룹을 만들 수 있습니다. 로컬 및 원격 서브넷이 있는 두 객체를 생성하여 암호화 ACL 및 NAT 문 모두에 사용합니다.

```
Cisco-ASA(config)#object network 10.2.2.0_24
Cisco-ASA(config-network-object)#subnet 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.1.1.0_24
Cisco-ASA(config-network-object)#subnet 10.1.1.0 255.255.255.0

Cisco-ASA(config)#access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

5단계. IKEv2 2단계 IPsec 제안서를 추가합니다. 암호화 IPsec ikev2 ipsec-proposal 컨피그레이션 모드에서 보안 매개변수를 지정합니다.

프로토콜 esp 암호화 {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null}
프로토콜 esp 무결성 {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

> **참고**: Microsoft는 Azure에서 사용하는 특정 2단계 IPSec 암호화 및 무결성 특성과 충돌하는 정보를 게시했습니다. 나열된 특성은 공개적으로 제공되는 이 Microsoft 문서에서 가장 효과적으로 제공됩니다. 2단계 Microsoft에서 충돌되는 IPSec 특성 정보가 여기에 표시됩니다. 자

세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

6단계. 암호화 맵을 구성하고 다음 구성 요소가 포함된 외부 인터페이스에 적용합니다.
·피어 IP 주소
·원하는 트래픽이 포함된 정의된 액세스 목록
·IKEv2 2단계 IPSec 제안
· 2단계 IPSec 수명(초)
·PFS(Perfect Forward Secrecy) 설정(선택 사항) - 데이터 보호를 위해 사용되는 새로운 Diffie-Hellman 키 쌍을 생성합니다(2단계가 시작되기 전에 양쪽이 PFS를 활성화해야 함).

Microsoft는 Azure에서 사용하는 특정 2단계 IPSec 수명 및 PFS 특성과 관련하여 충돌하는 정보를 게시했습니다.

나열된 특성은 다음과 같은 최상의 노력을 제공합니다. 이 공개 Microsoft 문서.

2단계 Microsoft에서 충돌되는 IPSec 특성 정보가 여기에 표시됩니다. 자세한 내용은 Microsoft Azure 지원에 문의하세요.

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
Cisco-ASA(config)#crypto map outside_map 20 set ikev2 ipsec-proposal myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 27000
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes
unlimited
Cisco-ASA(config)#crypto map outside_map 20 set pfs none
Cisco-ASA(config)#crypto map outside_map interface outside
```

8단계. VPN 트래픽이 다른 NAT 규칙의 적용을 받지 않는지 확인합니다. NAT 예외 규칙을 만듭니다.

```
Cisco-ASA(config)#nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination
static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

참고: 여러 서브넷을 사용하는 경우 모든 소스 및 대상 서브넷으로 개체 그룹을 생성하여 NAT 규칙에서 사용해야 합니다.

```
Cisco-ASA(config)#object-group  network 10.x.x.x_SOURCE
Cisco-ASA(config-network-object-group)#network-object  10.4.4.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object  10.2.2.0 255.255.255.0

Cisco-ASA(config)#object network 10.x.x.x_DESTINATION
Cisco-ASA(config-network-object-group)#network-object  10.3.3.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object  10.1.1.0 255.255.255.0

Cisco-ASA(config)#nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE
destination static 10.x.x.x_DESTINATION  10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

다음을 확인합니다.

ASA 및 Azure 게이트웨이 모두에서 컨피그레이션을 완료한 후 Azure는 VPN 터널을 시작합니다. 다음 명령을 사용하여 터널이 올바르게 빌드되는지 확인할 수 있습니다.

1단계

1단계 SA(Security Association)가 구축되었는지 확인합니다.

IKEv2

다음으로, UDP 포트 500의 로컬 외부 인터페이스 IP 192.168.1.2에서 원격 대상 IP 192.168.2.2로 구축된 IKEv2 SA가 표시됩니다. 또한 암호화된 트래픽이 통과하도록 작성된 유효한 하위 SA도 있습니다.

```
Cisco-ASA# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44615, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
Status         Role
  3208253 192.168.1.2/500                                192.168.2.2/500
READY    INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/142 sec
*-->Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x9b60edc5/0x8e7a2e12
```

여기에서는 ASA를 개시자로 피어 IP 192.168.2.2에 대해 남은 수명이 86388초인 IKEv1 SA가 표시됩니다.

```
Cisco-ASA# sh crypto ikev1 sa detail

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.2.2
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
    Encrypt : aes             Hash    : SHA
    Auth    : preshared       Lifetime: 86400
    Lifetime Remaining: 86388
```

2단계

IPSec 보안 연결이 **show crypto ipsec sa peer [peer-ip]** .

```
Cisco-ASA# show crypto ipsec sa peer 192.168.2.2
peer address: 192.168.2.2
```

```
Crypto map tag: outside, seq num: 10, local addr: 192.168.1.2

access-list VPN extended permit ip 192.168.0.0 255.255.255.0 192.168.3.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 192.168.2.2


#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #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.: 192.168.1.2/500, remote crypto endpt.: 192.168.2.2/500
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 8E7A2E12
current inbound spi : 9B60EDC5

inbound esp sas:
spi: 0x9B60EDC5 (2606820805)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (4193279/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F

outbound esp sas:
spi: 0x8E7A2E12 (2390371858)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (3962879/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

IPSec SA를 통해 4개의 패킷이 전송되고 4개는 오류 없이 수신됩니다. SPI 0x9B60EDC5가 포함된 하나의 인바운드 SA와 SPI 0x8E7A2E12가 포함된 하나의 아웃바운드 SA가 예상대로 설치됩니다.

또한 의 검사를 통해 데이터가 터널을 통과하는지 확인할 수 있습니다 **vpn-sessiondb l2l** 항목:

```
Cisco-ASA#show vpn-sessiondb l2l

Session Type: LAN-to-LAN

Connection : 192.168.2.2
Index : 44615 IP Addr : 192.168.2.2
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
```

```
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 400 Bytes Rx : 400
Login Time : 18:32:54 UTC Tue Mar 13 2018
Duration : 0h:05m:22s
```
바이트 Tx: 및 바이트 Rx: ipsec SA를 통해 전송 및 수신된 데이터 카운터를 표시합니다.

문제 해결

1단계. VPN에 대한 트래픽이 Azure 개인 네트워크로 향하는 내부 인터페이스에서 ASA에 수신되는지 확인합니다. 테스트하기 위해 내부 클라이언트에서 연속 ping을 구성하고 ASA에서 패킷 캡처를 구성하여 수신 여부를 확인할 수 있습니다.

capture [cap-name] interface [if-name] match [protocol] [src-ip] [src-mask] [dest-ip] [dest-mask]

show capture [cap-name]

```
Cisco-ASA#capture inside interface inside match ip host [local-host] host [remote-host]
Cisco-ASA#show capture inside

2 packets captured

   1: 18:50:42.835863       192.168.0.2 > 192.168.3.2: icmp: echo request
   2: 18:50:42.839128       192.168.3.2 > 192.168.0.2: icmp: echo reply
2 packets shown
```
Azure의 회신 트래픽이 표시되면 VPN이 올바르게 구축되어 트래픽을 전송/수신합니다.

소스 트래픽이 없는 경우 발신자가 ASA로 올바르게 라우팅되고 있는지 확인합니다.

소스 트래픽이 표시되지만 Azure의 회신 트래픽이 없는 경우 계속 진행하여 이유를 확인합니다.

2단계. ASA 내부 인터페이스에서 수신한 트래픽이 ASA에서 올바르게 처리되고 VPN으로 라우팅되는지 확인합니다.

ICMP 에코 요청을 시뮬레이션하려면
packet-tracer input [inside-interface-name] icmp [inside-host-ip] 8 0 [azure-host-ip] detail

전체 패킷 추적기 사용 지침은 여기에서 확인할 수 있습니다.
https://community.cisco.com:443/t5/security-knowledge-base/troubleshooting-access-problems-using-packet-tracer/ta-p/3114976

```
Cisco-ASA# packet-tracer input inside icmp 192.168.0.2 8 0 192.168.3.2 detail

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19afb0a0, priority=13, domain=capture, deny=false
        hits=3, user_data=0x7f6c19afb9b0, cs_id=0x0, l3_type=0x0
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000
        input_ifc=inside, output_ifc=any
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c195971f0, priority=1, domain=permit, deny=false
        hits=32, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000
        input_ifc=inside, output_ifc=any

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.1 using egress ifc  outside

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19250290, priority=0, domain=nat-per-session, deny=true
        hits=41, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c1987c120, priority=0, domain=inspect-ip-options, deny=true
        hits=26, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=inside, output_ifc=any

Phase: 6
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c19a60280, priority=70, domain=qos-per-class, deny=false
        hits=30, user_data=0x7f6c19a5c030, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=any

Phase: 7
```

```
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f6c1983ab50, priority=66, domain=inspect-icmp-error, deny=false
        hits=27, user_data=0x7f6c1987afc0, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
        src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
        input_ifc=inside, output_ifc=any

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f6c19afe1a0, priority=70, domain=encrypt, deny=false
        hits=2, user_data=0x13134, cs_id=0x7f6c19349670, reverse, flags=0x0, protocol=0
        src ip/id=192.168.0.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=192.168.3.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=any, output_ifc=outside

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 43, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_encrypt
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

NAT는 트래픽을 제외합니다(변환이 적용되지 않음). VPN 트래픽에서 NAT 변환이 발생하지 않는지 확인합니다.

또한 **output-interface** is correct - 암호화 맵이 적용된 물리적 인터페이스 또는 가상 터널 인터페이스여야 합니다.

액세스 목록 드롭이 표시되지 않는지 확인합니다.

VPN 단계가 **ENCRYPT: ALLOW** , 터널은 이미 구축되어 있으며 IPSec SA가 encaps와 함께 설치된 것을 볼 수 있습니다.

2.1단계. **ENCRYPT: ALLOW** 패킷 추적기에서 볼 수 있습니다.

IPsec SA가 설치되어 있는지 확인하고 **show crypto ipsec sa** .

외부 인터페이스에서 캡처를 수행하여 암호화된 패킷이 ASA에서 전송되고 암호화된 응답이 Azure에서 수신되는지 확인할 수 있습니다.

2.2단계. **ENCRYPT:DROP** 패킷 추적기에서 볼 수 있습니다.

VPN 터널이 아직 설정되지 않았지만 협상 중입니다. 이는 터널을 처음 시작할 때 예상되는 조건입니다. 디버그를 실행하여 터널 협상 프로세스를 보고 어디서 오류가 발생하는지 확인합니다.

먼저 올바른 버전의 IKE가 트리거되었으며 ike-common 프로세스에 관련 오류가 표시되지 않는지 확인합니다.

```
Cisco-ASA#debug crypto ike-common 255

Cisco-ASA# Mar 13 18:58:14 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE message to
IKEv1.  Map Tag = outside.  Map Sequence Number = 10.
```

VPN 트래픽이 시작될 때 ike-common 디버그 출력이 표시되지 않으면, 이는 트래픽이 암호화 프로세스에 도달하기 전에 삭제되거나 crypto ikev1/ikev2가 상자에서 활성화되지 않았음을 의미합니다. 암호화 컨피그레이션 및 패킷 삭제를 다시 확인합니다.

ike-common 디버깅에 암호화 프로세스가 트리거된 것으로 표시되면 IKE 구성 버전을 디버깅하여 터널 협상 메시지를 보고 Azure를 사용한 터널 구성에서 오류가 발생한 위치를 식별합니다.

IKEv1

전체 ikev1 디버그 절차 및 분석은 여기서 확인할 수 있습니다.

```
Cisco-ASA#debug crypto ikev1 127
Cisco-ASA#debug crypto ipsec 127
```

IKEv2

전체 ikev2 디버그 절차 및 분석은 여기서 확인할 수 있습니다.

```
Cisco-ASA#debug crypto ikev2 platform 127
Cisco-ASA#debug crypto ikev2 protocol 127
Cisco-ASA#debug crypto ipsec 127
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.