Azure에 대한 ASA IPsec VTI 연결 구성

목차

소개

이 문서에서는 Azure에 대한 ASA(Adaptive Security Appliance) IPsec VTI(Virtual Tunnel Interface) 연결을 구성하는 방법에 대해 설명합니다. ASA 9.8.1에서는 IKEv2를 활용하도록 IPsec VTI 기능이 확장되었지만 여전히 IPv4를 통한 sVTI IPv4로 제한됩니다. 이 컨피그레이션 가이드는 ASA CLI 인터페이스 및 Azure 포털을 사용하여 제작되었습니다. Azure 포털의 컨피그레이션은 PowerShell 또는 API에서 수행할 수도 있습니다. Azure 구성 방법에 대한 자세한 내용은 Azure 설명서를 참조하십시오.

참고: 현재 VTI는 단일 컨텍스트, 라우팅 모드에서만 지원됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA 9.8.1 이상을 실행하는 공용 고정 IPv4 주소를 사용하여 인터넷에 직접 연결된 ASA
- Azure 계정

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

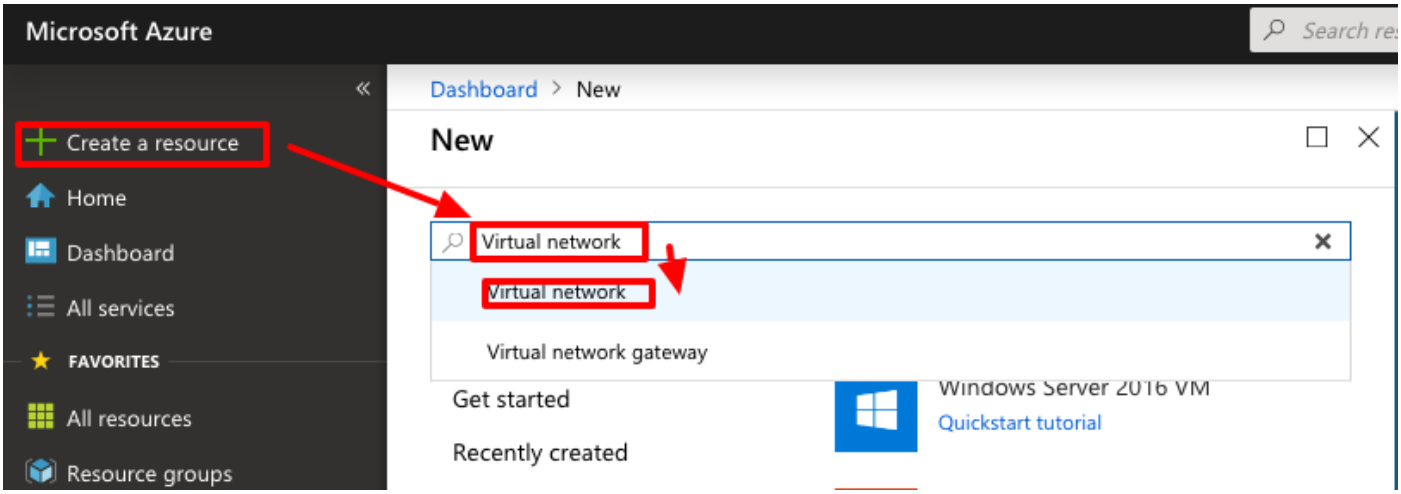
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

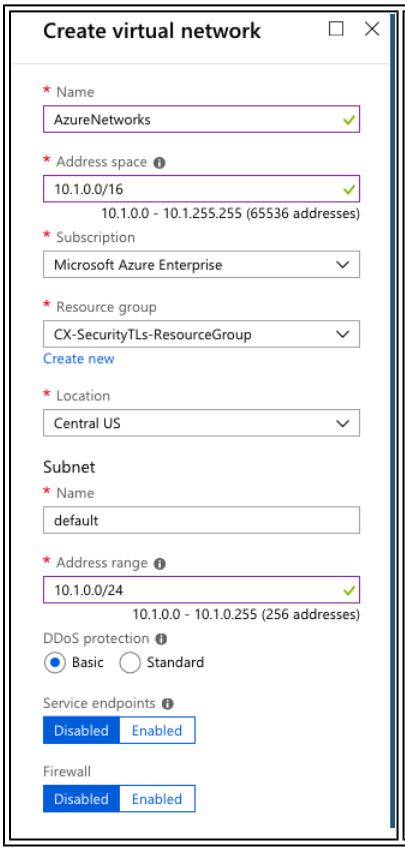
구성

이 가이드에서는 Azure 클라우드가 구성되지 않았다고 가정합니다. 리소스가 이미 설정되어 있으면 이 단계 중 일부를 건너뛸 수 있습니다.

1단계. Azure 내에서 네트워크를 구성합니다.

Azure 클라우드에 있는 네트워크 주소 공간입니다. 이 주소 공간은 이미지에 표시된 대로 하위 네트워크를 수용할 수 있을 만큼 충분히 커야 합니다.

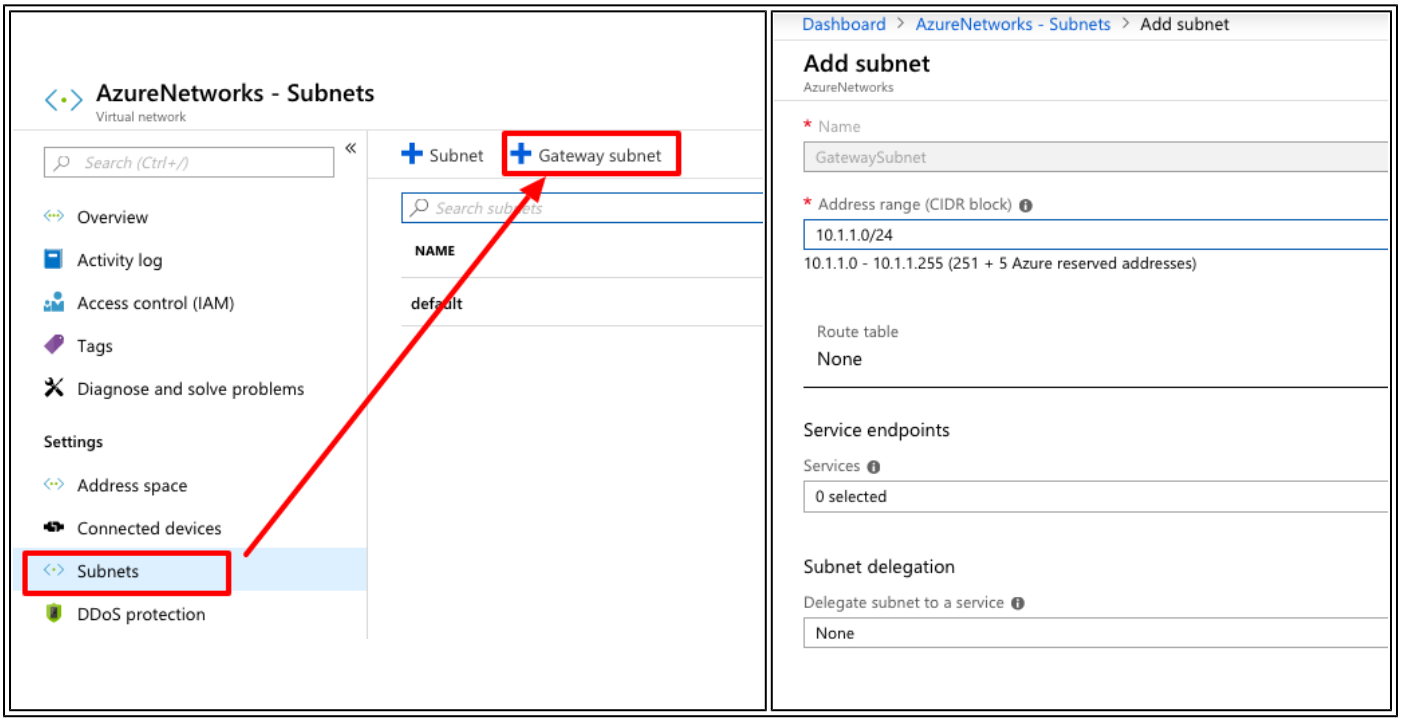




이름	클라우드에 호스팅된 IP 주소 공간의 이름
주소 공간	Azure에서 호스팅되는 전체 CIDR 범위입니다. 이 예에서는 10.1.0.0/16이 사용됩니다
서브넷 이름	일반적으로 VM이 연결되는 가상 네트워크 내에서 생성된 첫 번째 서브넷의 이름
서브넷 주소 범위	가상 네트워크 내에서 생성된 서브넷

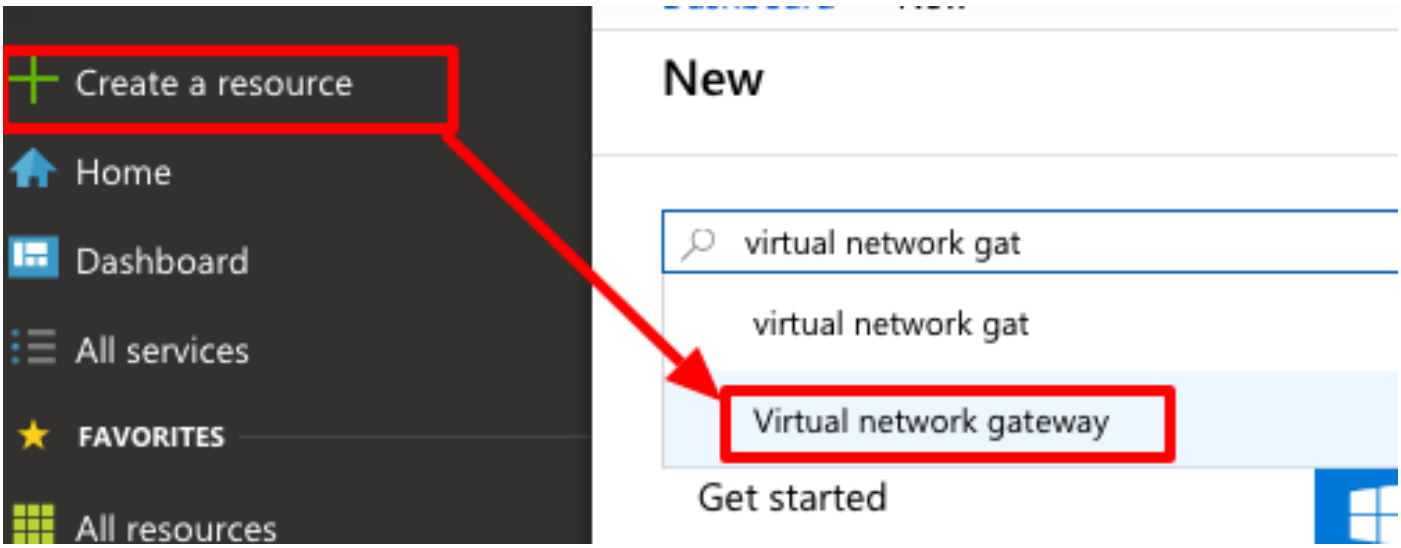
2단계. 가상 네트워크를 수정하여 게이트웨이 서브넷을 생성합니다.

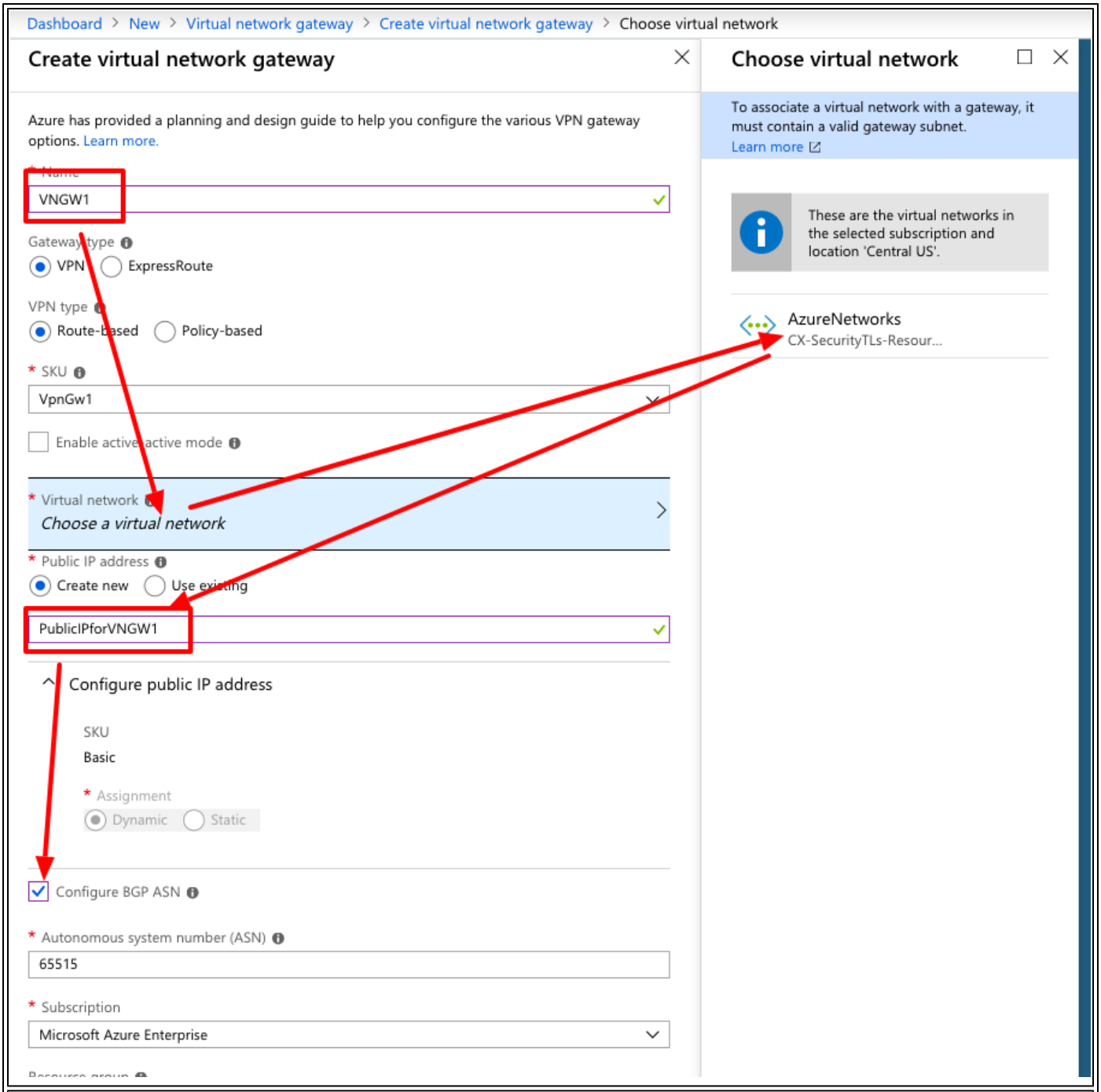
가상 네트워크로 이동하여 게이트웨이 서브넷을 추가합니다. 이 예에서는 10.1.1.0/24이 사용됩니다.



3단계. 가상 네트워크 게이트웨이를 만듭니다.

클라우드에서 호스팅되는 VPN 엔드포인트입니다. ASA가 IPsec 터널을 구축하는 데 사용하는 디바이스입니다. 이 단계에서는 가상 네트워크 게이트웨이에 할당된 공용 IP도 생성합니다.



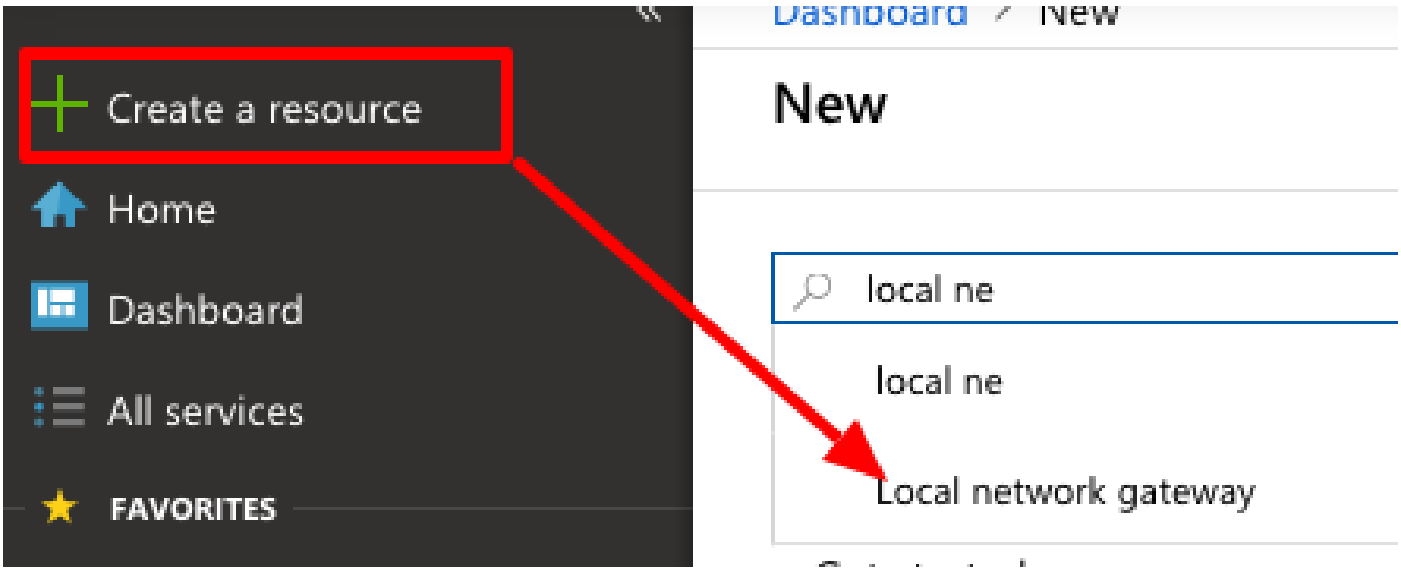


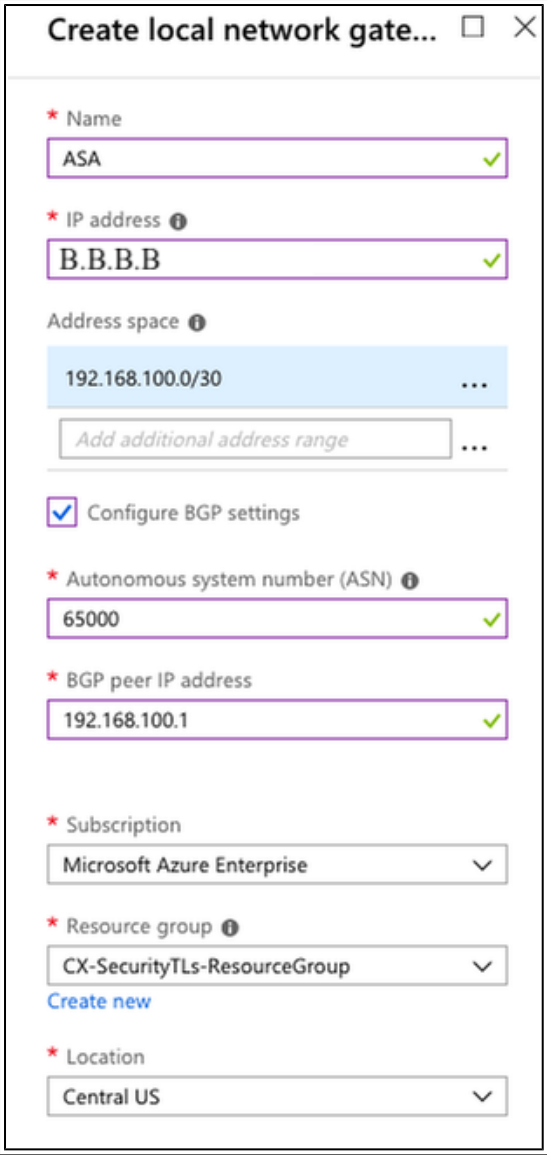
이름	가상 네트워크 게이트웨이의 이름
게이트웨이 유형	IPsec VPN이므로 VPN 선택
VPN 유형	VTI이므로 Route-based(경로 기반)를 선택합니다. 암호화 맵 VPN이 완료될 때 정책 기반 사용
SKU	필요한 트래픽의 양에 따라 VpnGw1 이상을 선택해야 합니다. Basic은 BGP를 지원하지 않습니다.
활성/활성 모드 사용	활성화하지 마십시오. 게시 시 ASA에는 루프백 또는 인터페이스 내부에서 BGP 세션을 소싱할 수 있는 기능이 없습니다. Azure에서는 BGP 피어링에 대해 1개의 IP 주소만 허용합니다.
공용 IP 주	새 IP 주소를 생성하고 리소스에 이름을 할당합니다

소	
BGP ASN 구성	링크에서 BGP를 활성화하려면 이 확인란을 선택합니다
ASN	이 값을 기본 값으로 65515. ASN Azure는 다음과 같이 표시됩니다.

4단계. 로컬 네트워크 게이트웨이를 만듭니다.

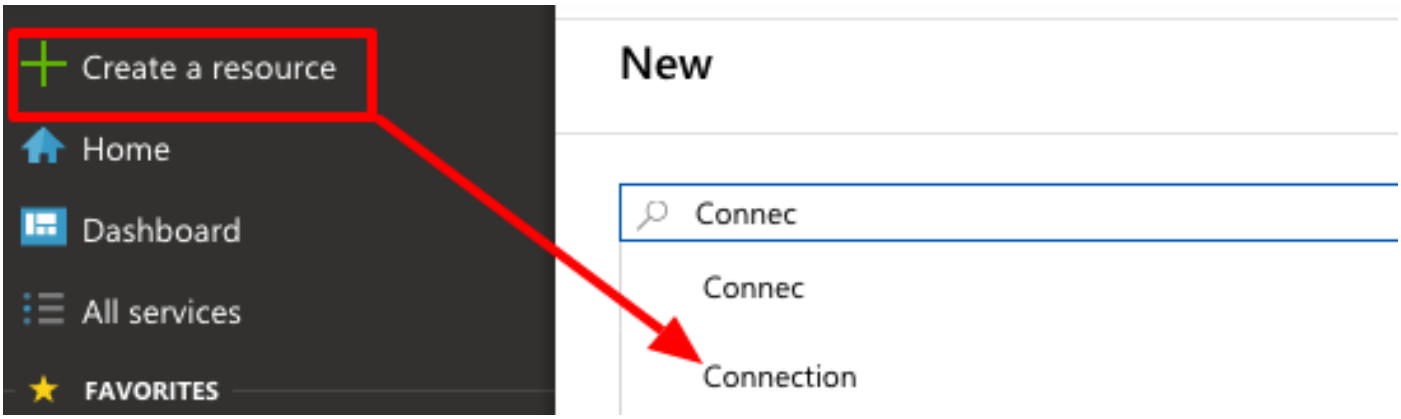
로컬 네트워크 게이트웨이는 ASA를 나타내는 리소스입니다.

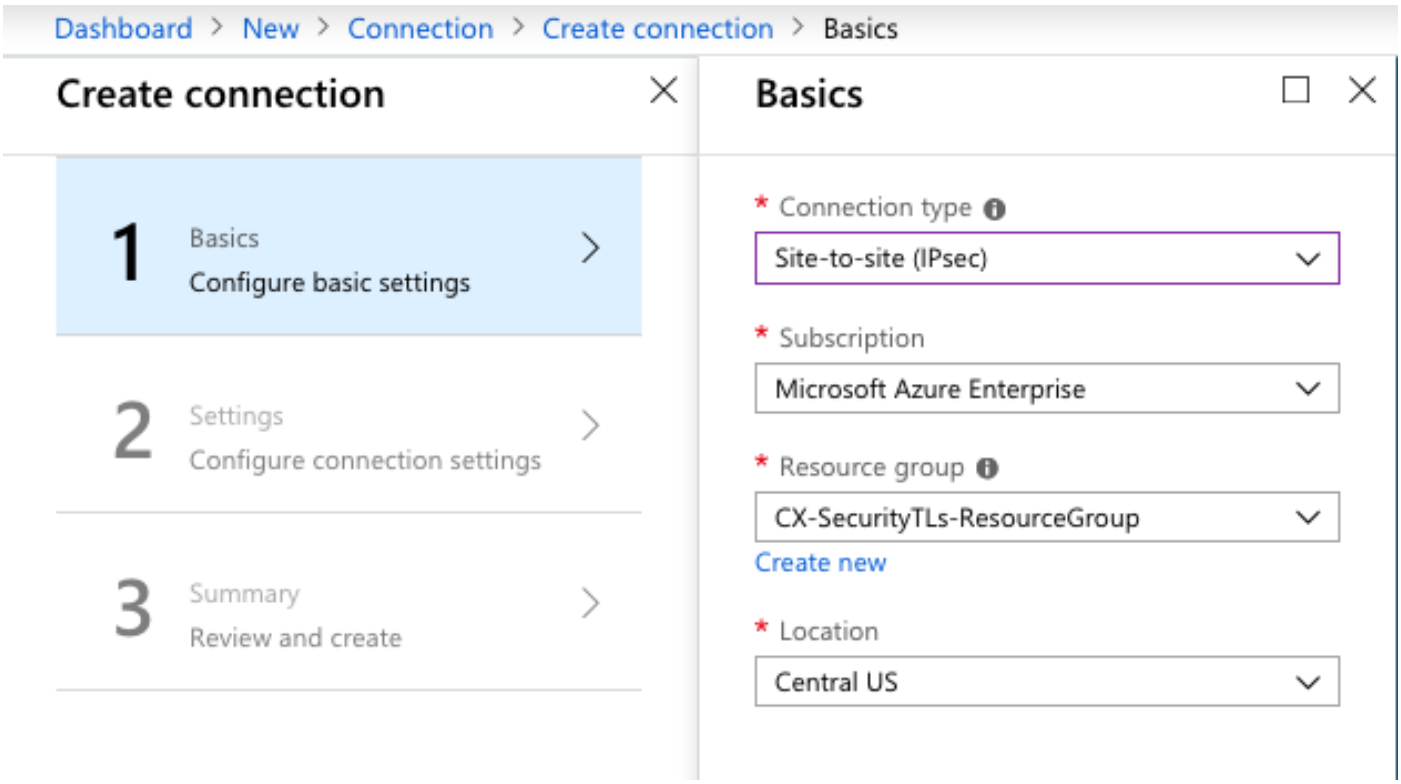


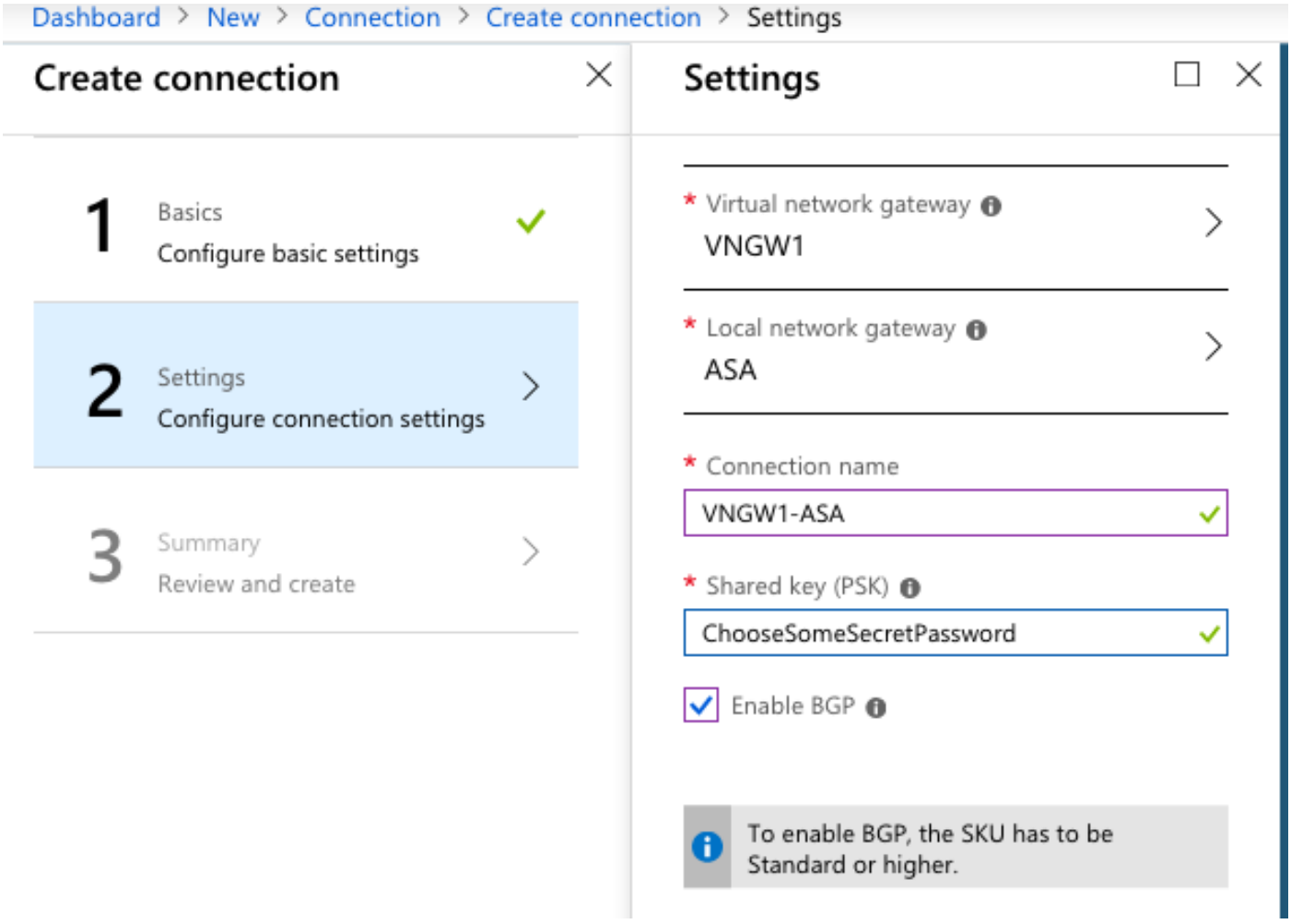


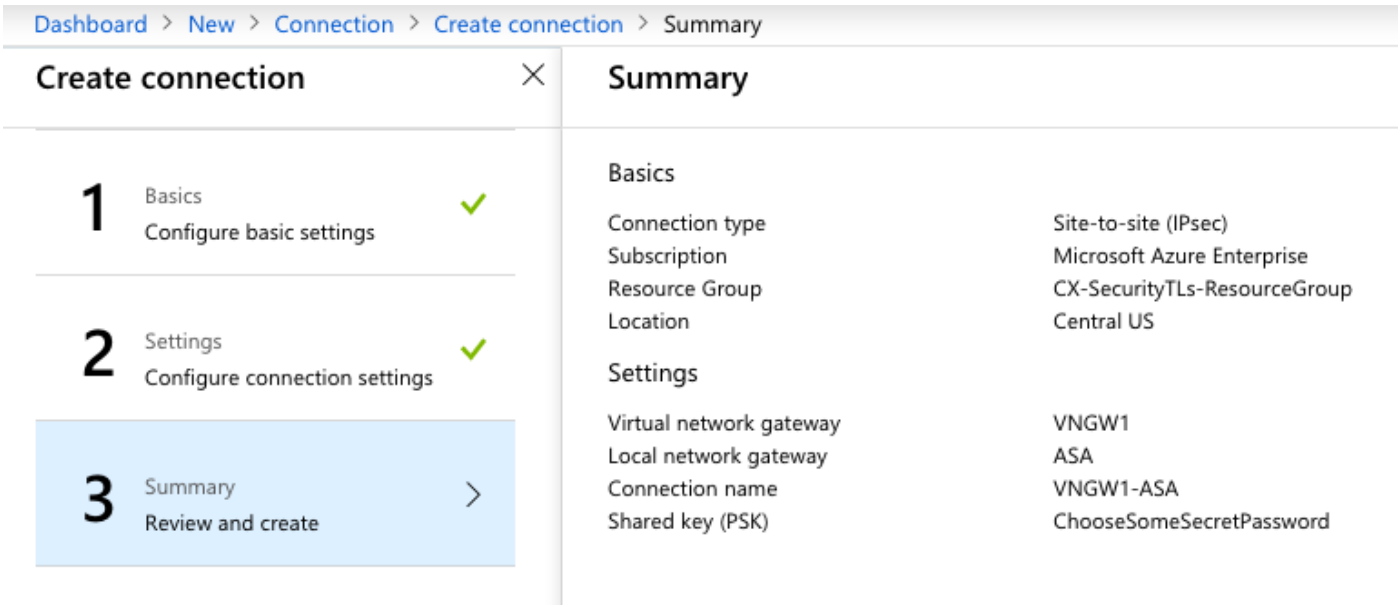
이름	ASA의 이름
IP 주소	ASA 외부 인터페이스의 공용 IP 주소
주소 공간	서브넷은 나중에 VTI에서 구성됩니다
BGP 설정 구성	BGP를 활성화하려면 이 확인란을 선택합니다
ASN	이 ASN은 ASA에서 구성됩니다
BGP 피어 IP 주소	IP 주소는 ASA VTI 인터페이스에 구성됩니다

5단계. 이미지에 표시된 대로 가상 네트워크 게이트웨이와 로컬 네트워크 게이트웨이 간에 새 연결을 생성합니다.




Dashboard > New > Connection > Create connection > Basics
Create connection
1 Basics
Configure basic settings
2 Settings
Configure connection settings
3 Summary
Review and create
Basics
* Connection type
Site-to-site (IPsec)
* Subscription
Microsoft Azure Enterprise
* Resource group
CX-SecurityTLs-ResourceGroup
Create new
* Location
Central US


Dashboard > New > Connection > Create connection > Settings
Create connection
1 Basics
Configure basic settings
2 Settings
Configure connection settings
3 Summary
Review and create
Settings
* Virtual network gateway
VNGW1
* Local network gateway
ASA
* Connection name
VNGW1-ASA
* Shared key (PSK)
ChooseSomeSecretPassword
Enable BGP
To enable BGP, the SKU has to be Standard or higher.



6단계. ASA를 구성합니다.

먼저 외부 인터페이스에서 IKEv2를 활성화하고 IKEv2 정책을 구성합니다.

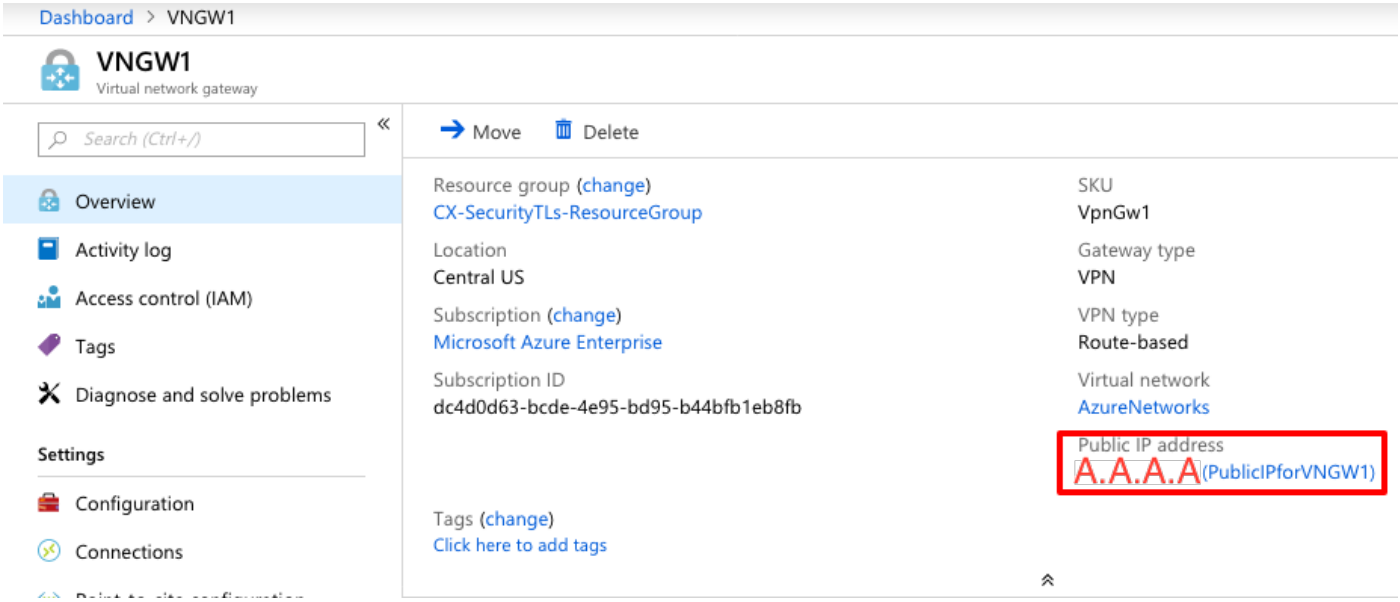
```
crypto ikev2 policy 10
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 14 5 2
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 14 5 2
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 enable outside
```

6단계. IPsec 변형 집합 및 IPsec 프로필을 구성합니다.

```
crypto ipsec ikev2 ipsec-proposal AZURE-PROPOSAL
 protocol esp encryption aes-256
 protocol esp integrity sha-256
crypto ipsec profile AZURE-PROPOSAL
 set ikev2 ipsec-proposal AZURE-PROPOSAL
```

8단계. 터널 그룹을 구성합니다.

그림과 같이 3단계에서 생성한 가상 네트워크 게이트웨이의 공용 IPv4 주소를 검색합니다.



그런 다음 ASA에서 3단계에서 정의한 사전 공유 키를 사용하여 그룹 정책 및 터널 그룹을 구성합니다.

```
group-policy AZURE internal
group-policy AZURE attributes
 vpn-tunnel-protocol ikev2
tunnel-group A.A.A.A type ipsec-l2l
tunnel-group A.A.A.A general-attributes
 default-group-policy AZURE
tunnel-group A.A.A.A ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

9단계. 터널 인터페이스를 구성합니다.

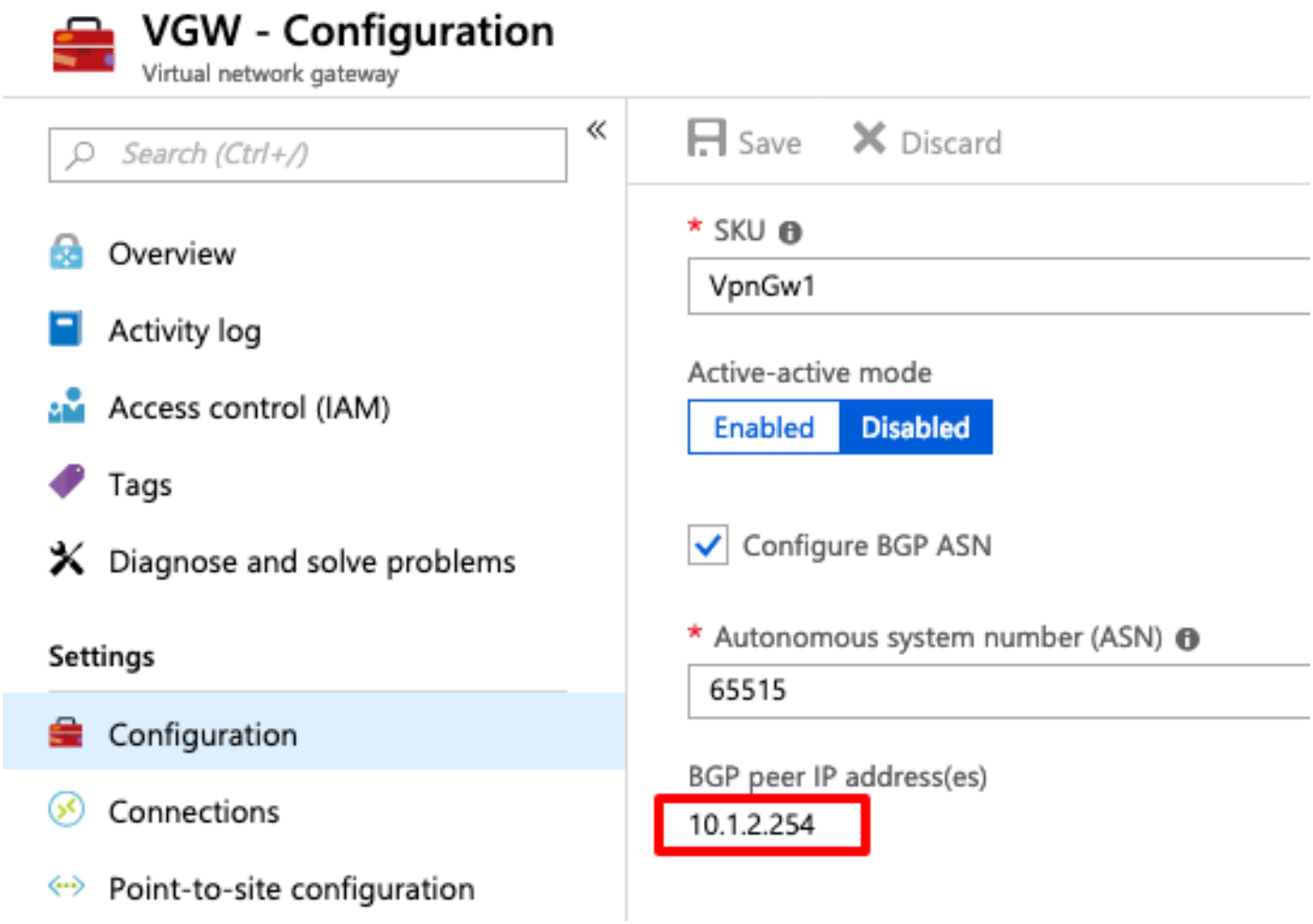
4단계(로컬 네트워크 게이트웨이 구성)에서 BGP 연결을 위한 네트워크 주소와 IP 주소를 구성했습니다. VTI에서 구성할 IP 주소 및 네트워크입니다.

```
interface Tunnel1
 nameif AZURE
 ip address 192.168.100.1 255.255.255.252
 tunnel source interface outside
 tunnel destination A.A.A.A
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AZURE-PROPOSAL
 no shutdown
```

10단계.

옵션 1. 동적 라우팅을 구성합니다. BGP를 사용하여 Azure와 경로를 교환합니다.

3단계에서 만든 가상 네트워크 게이트웨이의 구성을 보려면 Azure에서 BGP 라우터의 IP 주소를 찾습니다. 이 예에서는 10.1.2.254입니다.



ASA에서 VTI 터널을 벗어난 10.1.2.254를 가리키는 고정 경로를 구성합니다. 이 예에서 192.168.100.2는 VTI와 동일한 서브넷 내에 있습니다. 해당 IP 주소를 가진 디바이스가 없더라도 ASA는 VTI 인터페이스를 가리키는 경로를 설치합니다.

```
route AZURE 10.1.2.254 255.255.255.255 192.168.100.2 1
```

그런 다음 ASA에서 BGP를 구성합니다. 네트워크 192.168.2.0/24은 ASA의 내부 인터페이스이며 클라우드로 전파되는 경로입니다. 또한 Azure에 구성된 네트워크는 ASA에 광고됩니다.

```
router bgp 65000
 bgp log-neighbor-changes
 bgp graceful-restart
 address-family ipv4 unicast
  neighbor 10.1.2.254 remote-as 65515
  neighbor 10.1.2.254 ebgp-multihop 255
  neighbor 10.1.2.254 activate
  network 192.168.2.0
  network 192.168.100.0 mask 255.255.255.252
  no auto-summary
```

```
  no synchronization
 exit-address-family
```

옵션 2. 고정 라우팅 구성 - ASA 및 Azure 모두에서 경로를 정적으로 구성합니다. VTI 터널을 통해 Azure 네트워크로 트래픽을 전송하도록 ASA를 구성합니다.

```
route AZURE 10.1.0.0 255.255.0.0 192.168.100.2 1
```

4단계에서 생성한 로컬 네트워크 게이트웨이를 터널 인터페이스의 ASA 및 서브넷 뒤에 있는 네트워크로 수정하고 "추가 네트워크 공간 추가" 섹션에 접두사를 추가합니다.

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. show crypto ikev2 sa를 사용하여 IKEv2 세션이 설정되었는지 확인합니다.

<#root>

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:

Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
2006974029 B.B.B.B.    /500                                     A.A.A.A/500
```

READY

```
          INITIATOR
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/4640 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x74e90416/0xba17723a
```

2단계. IPsec SA도 show crypto ipsec sa 명령을 사용하여 협상되었는지 확인합니다.

<#root>

```
ciscoasa# show crypto ipsec sa
interface: AZURE
    Crypto map tag: __vti-crypto-map-3-0-1, seq num: 65280, local addr: B.B.B.B

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: A.A.A.A
```

```
#pkts encaps: 240,

 #pkts encrypt: 240, #pkts digest: 240


#pkts decaps: 377

, #pkts decrypt: 377, #pkts verify: 377
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 240, #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.: B.B.B.B/500, remote crypto endpt.: A.A.A.A/500
      path mtu 1500, ipsec overhead 78(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: BA17723A
      current inbound spi : 74E90416

    inbound esp sas:


spi: 0x74E90416 (1961427990)
         SA State: active

         transform: esp-aes-256 esp-sha-256-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 1722, crypto-map: __vti-crypto-map-3-0-1
         sa timing: remaining key lifetime (kB/sec): (3962863/24100)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:


spi: 0xBA17723A (3122098746)
         SA State: active

         transform: esp-aes-256 esp-sha-256-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 1722, crypto-map: __vti-crypto-map-3-0-1
         sa timing: remaining key lifetime (kB/sec): (4008947/24100)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001

ciscoasa#
```

3단계. 고정 라우팅을 사용하는 경우 BGP 또는 엔드포인트 리소스에 대한 레이어 3 라우팅과 레이어 4 연결을 검증하기 위해 ping 및 ping tcp를 사용하여 터널을 통해 BGP 원격 라우터에 대한 연결을 확인합니다.

<#root>

ciscoasa#

ping 10.1.2.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.254, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/50 ms
ciscoasa#

ping tcp 10.1.2.254 179

Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.1.2.254 port 179
from 192.168.100.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 41/42/42 ms
ciscoasa#

4단계. BGP를 사용하는 경우 BGP 연결, Azure로 수신 및 광고된 경로 및 ASA의 라우팅 테이블을 확인합니다.

<#root>

ciscoasa#

show bgp summary

BGP router identifier 192.168.100.1, local AS number 65000
BGP table version is 6, main routing table version 6
4 network entries using 800 bytes of memory
5 path entries using 400 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
1 BGP AS-PATH entries using 24 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 1640 total bytes of memory
BGP activity 14/10 prefixes, 17/12 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.2.254	4	65515	73	60	6	0	0		

01:02:26 3

ciscoasa#

show bgp neighbors 10.1.2.254 routes

BGP table version is 6, local router ID is 192.168.100.1

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path

*> 10.1.0.0/16      10.1.2.254                       0  65515 i   <<< This is the virtual network defi

*  192.168.100.0/30 10.1.2.254                       0  65515 i
r> 192.168.100.1/32 10.1.2.254                       0  65515 i

Total number of prefixes 3
ciscoasa#
```

show bgp neighbors 10.1.2.254 advertised-routes

```
BGP table version is 6, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path

*> 192.168.2.0      0.0.0.0              0         32768  i        <<< These are the routes being advert
*> 192.168.100.0/30 0.0.0.0              0         32768  i        <<<


Total number of prefixes 2
ciscoasa#
ciscoasa#
```

show route

```
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 10.1.251.33 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via B.B.B.C, outside

B        10.1.0.0 255.255.0.0 [20/0] via 10.1.1.254, 01:03:33


S        10.1.2.254 255.255.255.255 [1/0] via 192.168.100.2, AZURE
C        B.B.B.A 255.255.255.224 is directly connected, outside
L        B.B.B.B 255.255.255.255 is directly connected, outside
C        192.168.2.0 255.255.255.0 is directly connected, inside
L        192.168.2.2 255.255.255.255 is directly connected, inside
C        192.168.100.0 255.255.255.252 is directly connected, AZURE
L        192.168.100.1 255.255.255.255 is directly connected, AZURE
```

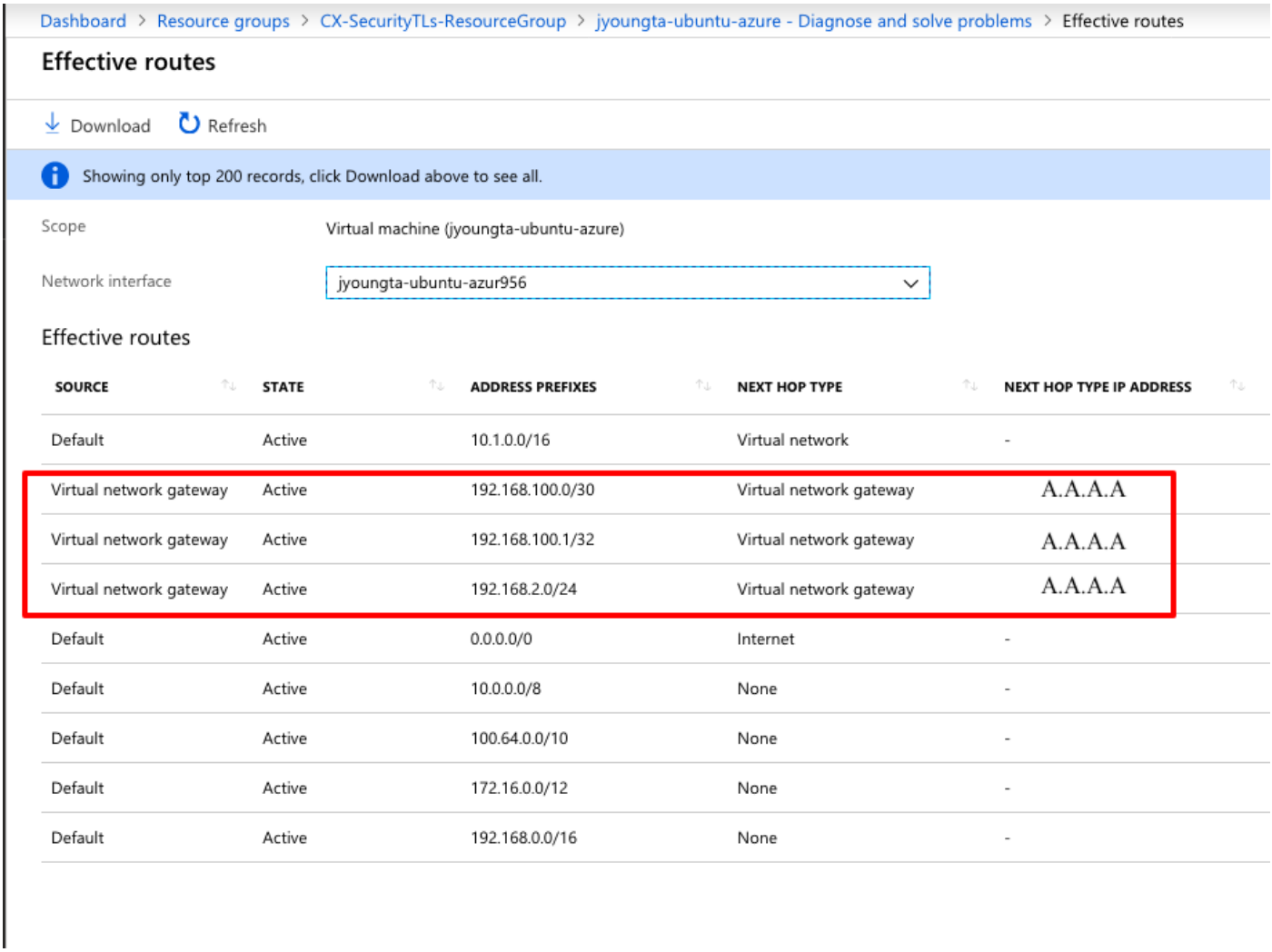
5단계. 터널을 통해 디바이스를 ping합니다. 이 예에서는 Azure에서 실행되는 Ubuntu VM입니다.

<#root>

```
ciscoasa# p
ing 10.1.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/42/50 ms
```

이제 원격 VM의 유효 경로를 확인합니다. 이미지에 표시된 대로 ASA가 클라우드에 보급된 경로를 표시해야 합니다.



문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

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.