Configure ASA IPsec VTI Connection to Azure

Contents

Introduction

This document describes how to configure an Adaptive Security Appliance (ASA) IPsec Virtual Tunnel Interface (VTI) connection to Azure.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- An ASA connected directly to the Internet with a public static IPv4 address that runs ASA 9.8.1 or later.
- An Azure account

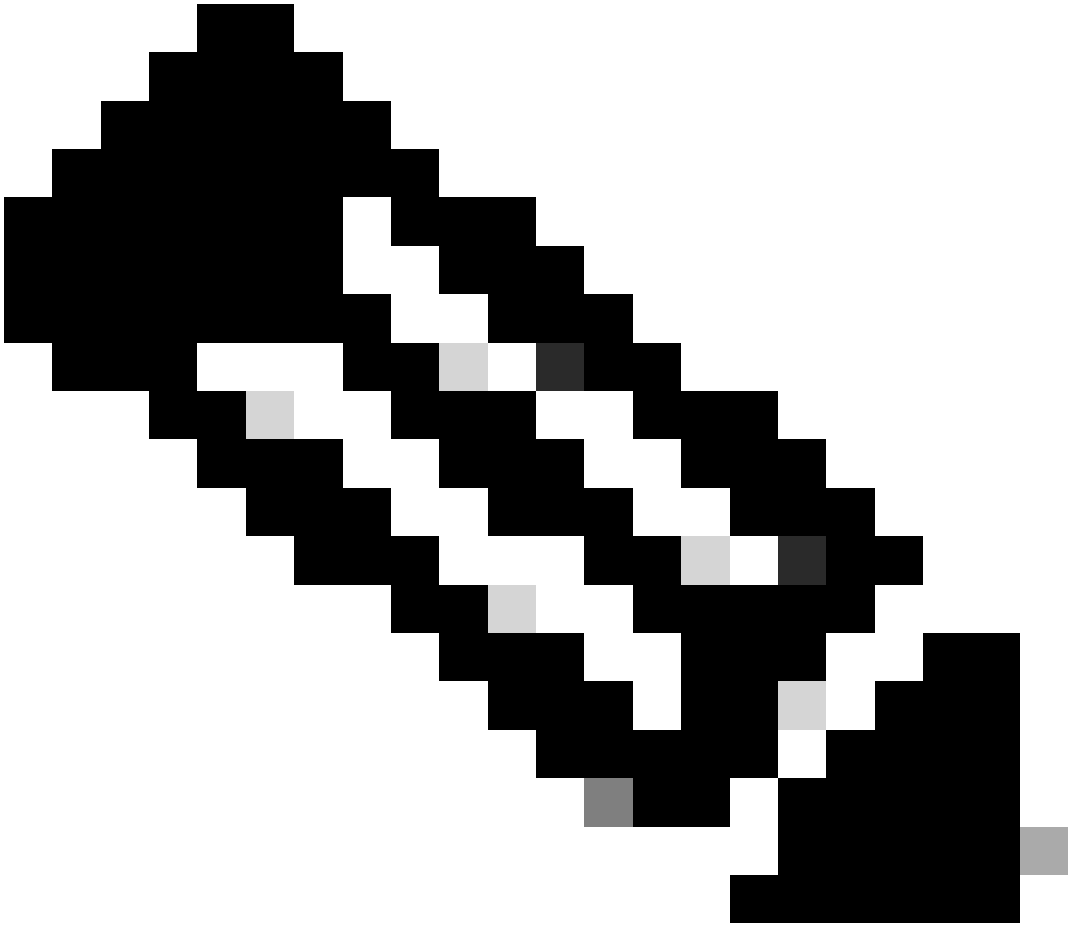
Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In ASA 9.8.1, the IPsec VTI feature was extended to utilize IKEv2, however, it is still limited to sVTI IPv4 over IPv4. This configuration guide was produced with the use of the ASA CLI interface and the Azure Portal. The configuration of the Azure portal can also be performed by PowerShell or API. For more information about the Azure configuration methods, refer to the Azure documentation.



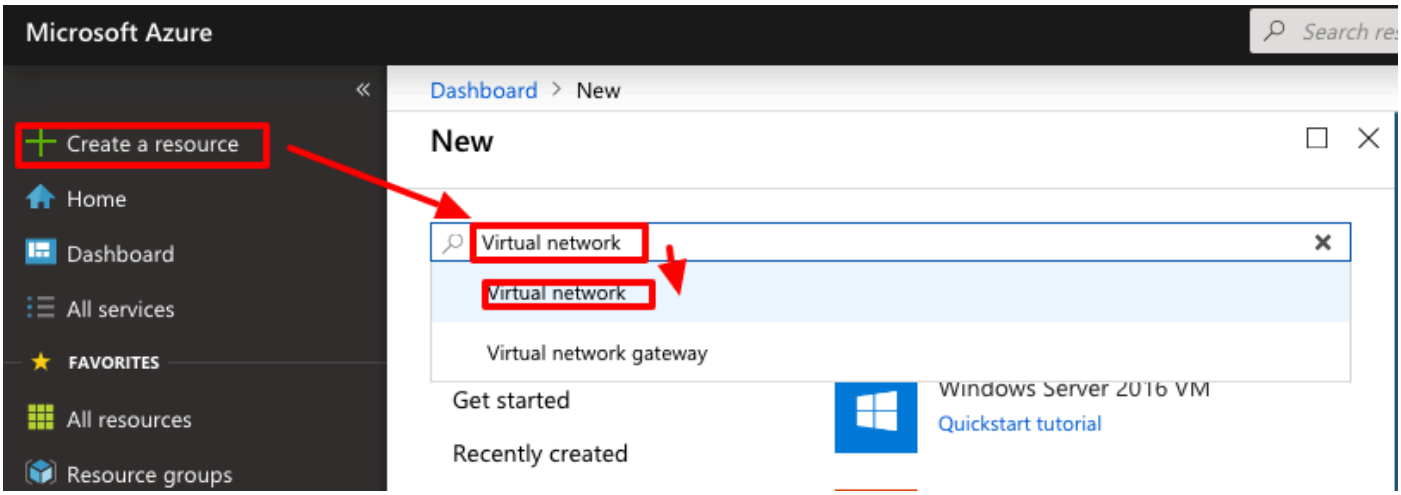
Note: Currently, VTI is only supported in single-context, routed mode.

Configure

This guide assumes that the Azure cloud has not been configured. Some of these steps can be skipped if the resources are already established.

Step 1. Configure a network within Azure.

This is the network address space that lives in the Azure Cloud. This address space must be large enough in order to accommodate sub-networks within them as shown in the image.


Microsoft Azure
Search re
Dashboard > New
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
New
Virtual network
Virtual network
Virtual network gateway
Get started
Recently created
Windows Server 2016 VM
Quickstart tutorial

Microsoft Azure

All services > Create a resource >

Marketplace

Get Started

Service Providers

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Networking (335)

Security (302)

Compute (193)

IT & Management Tools (169)

Storage (125)

New! Get AI-generated suggestions

Ask AI to suggest products, articles, and solutions for wl

virtual network

Azure benefit eligible only

Azure services only

Showing 1 to 20 of 8[illegible] results for 'virtual network'. Clear search

Virtual network

Microsoft

Azure Service

Create a logically isolated section in Microsoft Azure and securely connect it outward.

Create

Virtual network gateway

Microsoft

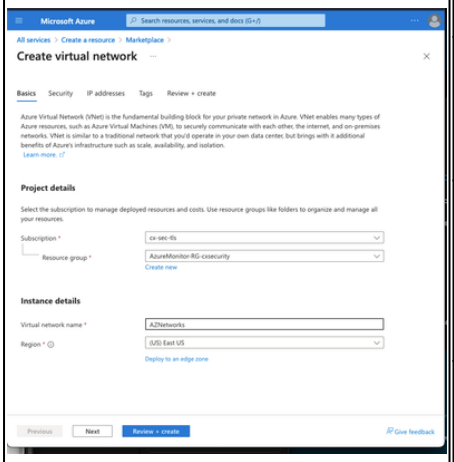
Azure Service

The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN connections.

Create

Virtual network

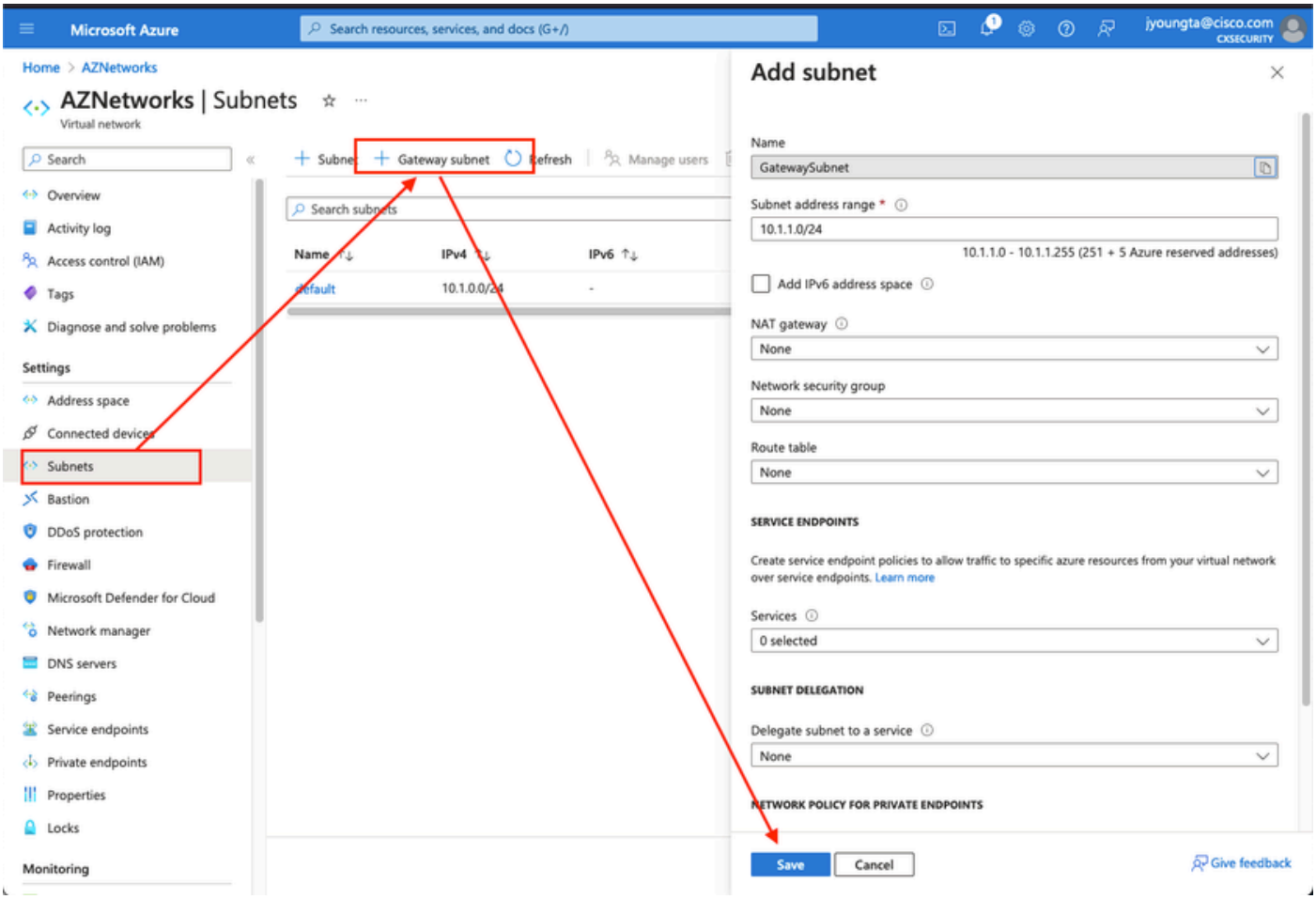
Virtual network



Name	**A Name for the IP Address Space Hosted in the Cloud**
Address Space	The whole CIDR range hosted in Azure. In this example, 10.1.0.0/16 is used.
Subnet Name	The name for the first subnet created within the virtual network to which VMs are usually attached. A subnet called default is usually created.
Subnet Address range	A subnet created within the Virtual Network.

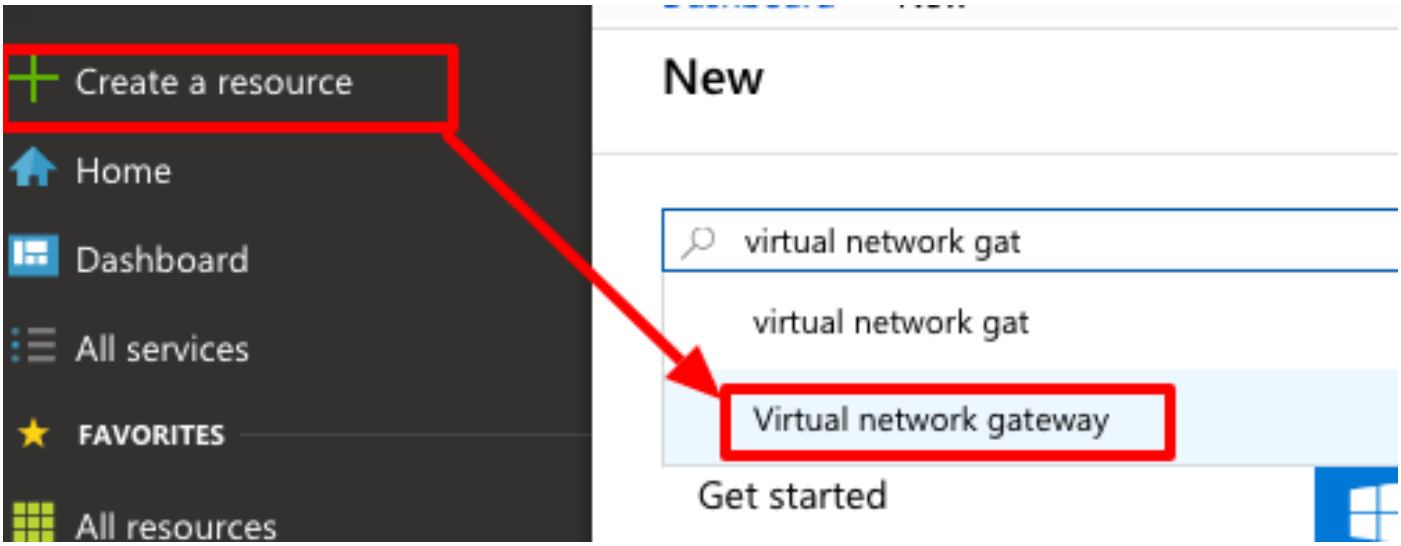
Step 2. Modify the Virtual Network in order to create a Gateway Subnet.

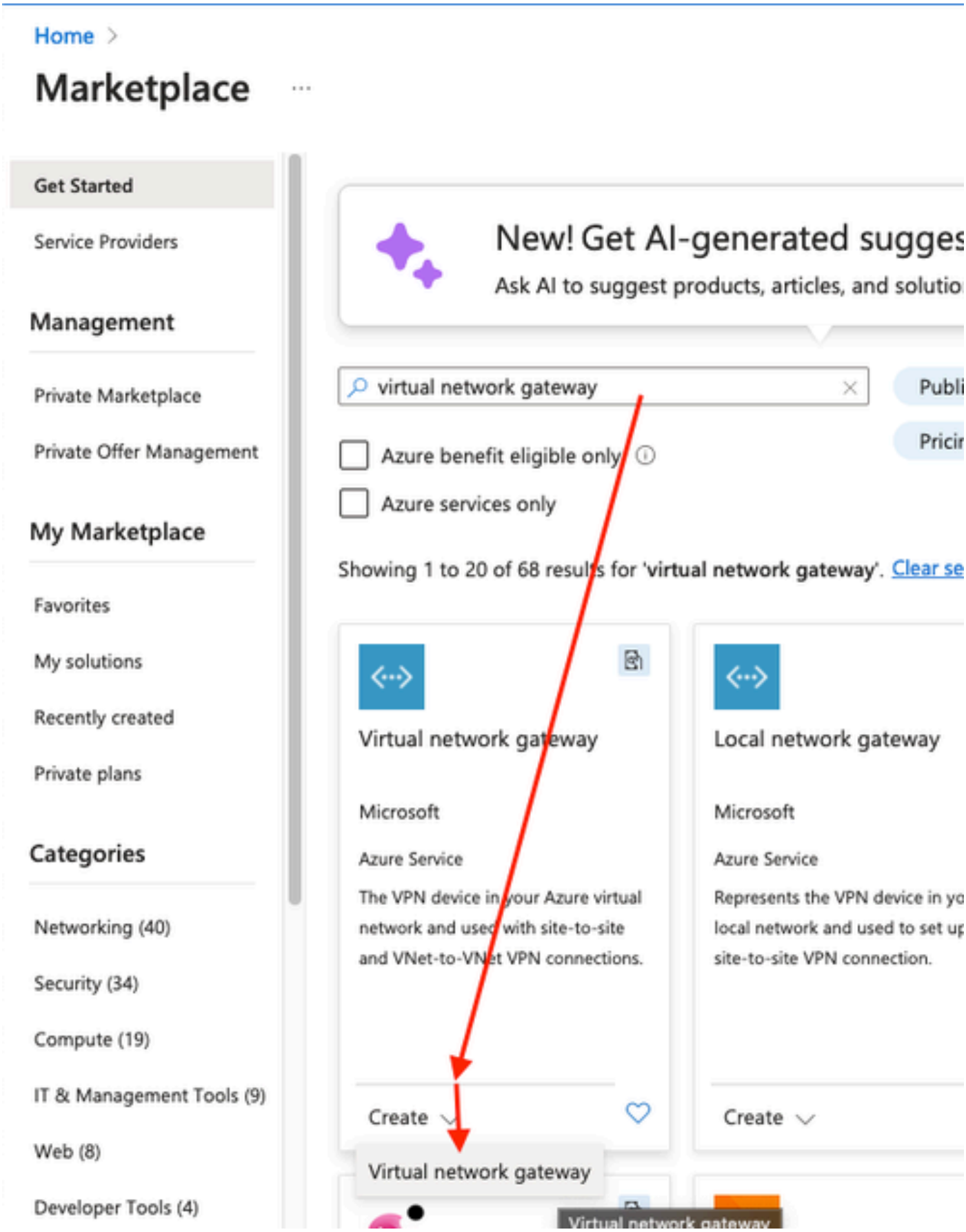
Navigate to the **Virtual network** and add a **gateway subnet**. In this example, 10.1.1.0/24 is used.



Step 3. Create a Virtual Network Gateway.

This is the VPN endpoint that is hosted in the cloud. This is the device that the ASA builds the IPsec tunnel with. This step also creates a public IP which is assigned to the Virtual network gateway. This step can take 15 - 20 minutes to complete.


Create a resource
Home
Dashboard
All services
FAVORITES
All resources
New
virtual network gat
virtual network gat
Virtual network gateway
Get started

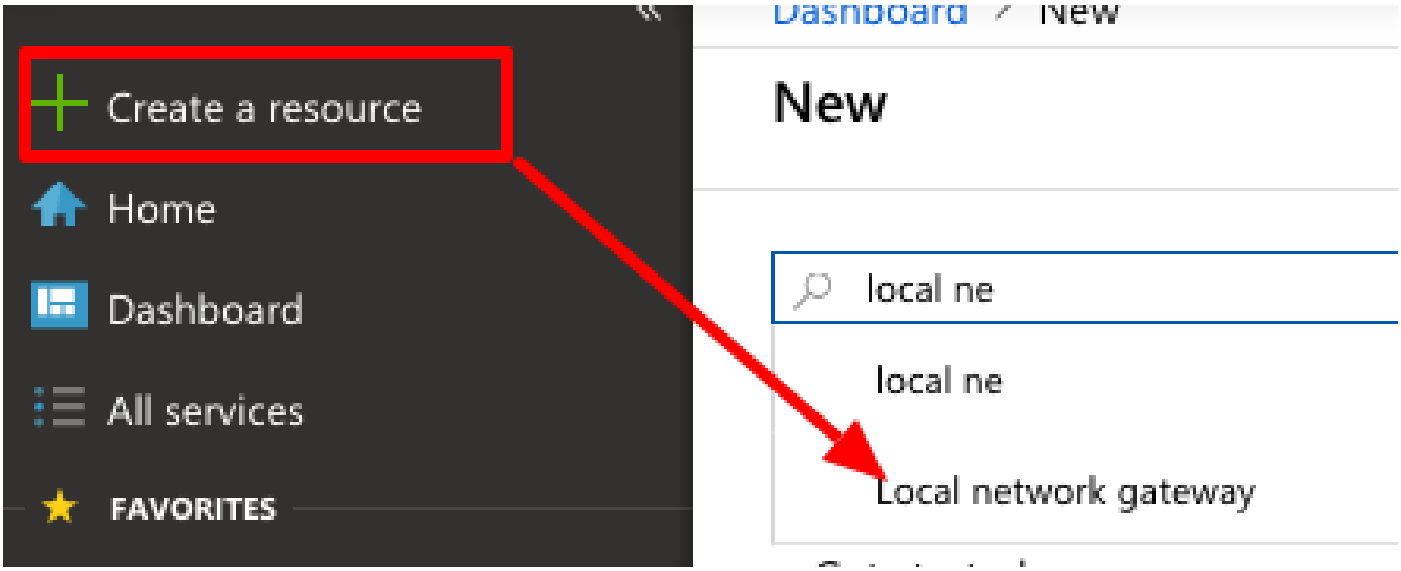


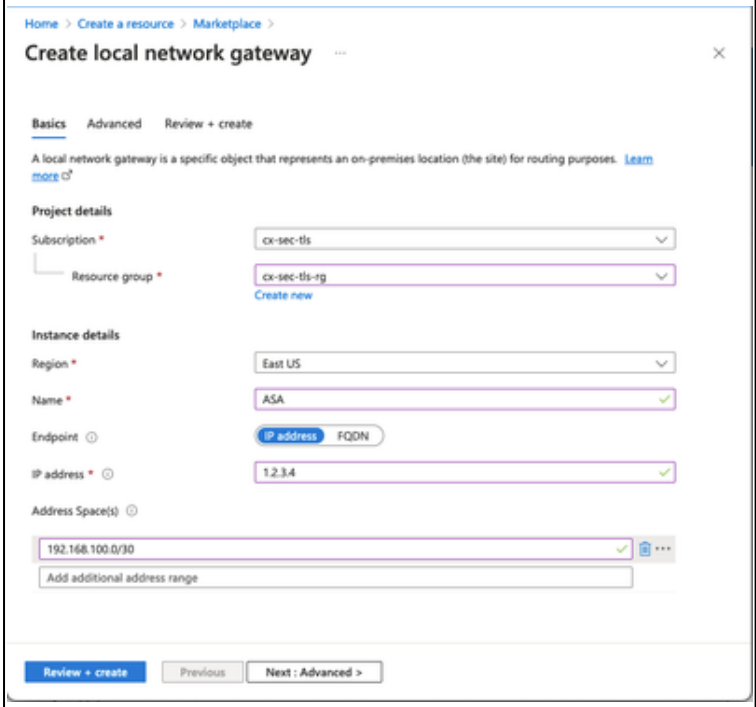
Name	**Name for the Virtual Network Gateway**

Gateway Type	Select VPN as this is an IPsec VPN.
VPN Type	Select Route-based because this is a VTI. Policy-based is used when a crypto map VPN is done.
SKU	Need to select VpnGw1 or greater based on the amount of traffic needed. Basic does not support Border Gateway Protocol (BGP).
Enabled active/active mode	Do not enable. At the time of posting, the ASA does not have the capability to source the BGP session from a loopback or inside the interface. Azure only allows 1 IP address for the BGP peering.
Public IP address	Create a new IP address and assign a name to the resource.
Configure BGP ASN	Check this box to enable BGP on the link.
ASN	Leave this as the default 65515. This is the ASN Azure that presents itself.

Step 4. Create a Local Network Gateway.

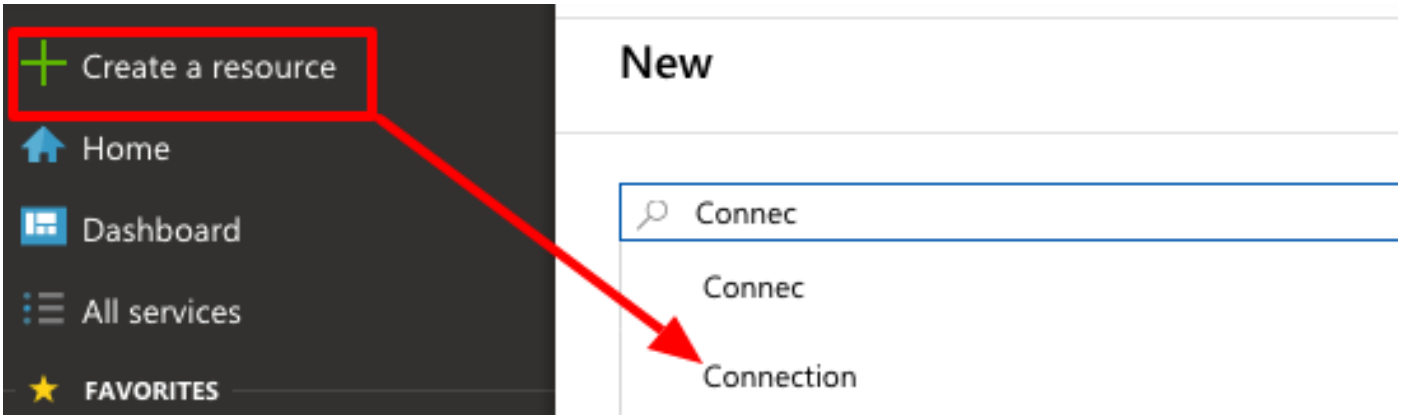
A Local network gateway is the resource that represents the ASA.





Name	A Name for the ASA
IP Address	The public IP address of the ASA's outside interface.
Address Space	The subnet is configured on the VTI later.
Configure BGP Settings	Check this to enable BGP.
ASN	This ASN is configured on the ASA.
BGP peer IP address	The IP address is configured on the ASA VTI interface.

Step 5. Create a new connection between the Virtual network gateway and the Local network gateway as shown in the image.



Home > Create a resource > Marketplace >

Create connection

Basics | Settings | Tags | Review + create

Create a secure connection to your virtual network by using VPN Gateway or ExpressRoute.
Learn more about VPN Gateway
Learn more about ExpressRoute

Project details

Subscription * cx-sec-tls

Resource group * cx-sec-tls-rg
Create new

Instance details

Connection type * Site-to-site (IPsec)

Name * VPNTunnel1

Region * East US

Review + create | Previous | Next : Settings > | Download a template for automation | Give feedback

Create connection - Microsoft A | Duo Security - Two-Factor Auth

https://portal.azure.com/#create/Microso

Getting Started | Getting Started | Lightning GIT | ASA License Gener... | ASA License Gener... | Cisco SecureX

Micros | Search resources, services, and docs (G+/) | jyoungta@cisco.com CXSECURITY

Home > Create a resource > Marketplace >

Create connection

Basics | Settings | Tags | Review + create

Virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway.

Virtual network gateway *	VNGW1
Local network gateway *	ASA
Shared key (PSK) *	••••••••••••••••
IKE Protocol	IKEv1 / IKEv2
Use Azure Private IP Address	☐
Enable BGP	☑

To enable BGP, the SKU has to be Standard or higher.

IPsec / IKE policy: Default | Custom

When using custom IPSec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel establishment and rekey.

IKE Phase 1	Encryption *	Integrity/PRF *	DH Group *
	GCMAES256	SHA384	DHGroup14
IKE Phase 2(IPsec)	IPsec Encryption *	IPsec Integrity *	PFS Group *
	AES256	SHA256	None

IPsec SA lifetime in KiloBytes *	0
IPsec SA lifetime in seconds *	27000
Use policy based traffic selector	Enable / Disable
DPD timeout in seconds *	45
Connection Mode	Default / InitiatorOnly / ResponderOnly

Review + create | Previous | Next : Tags > | Download a template for automation | Give feedback

Step 6. Configure the ASA.

that points to 10.1.2.254 out the VTI Tunnel. In this example, 192.168.100.2 is within the same subnet as the VTI. Even though no device has that IP address, the ASA installs the route that points out the VTI interface.

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

Then, configure **BGP** on the ASA. The network 192.168.2.0/24 is the ASA's inside interface and a route that is propagated into the cloud. In addition, the networks configured in Azure are advertised to the ASA.

```
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
```

Option 2. Configure **static routing -** statically configure routes on both the ASA and Azure. Configure the **ASA** to send traffic to the Azure networks over the VTI tunnel.

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

Modify the Local Network Gateway created in Step 4 with networks that exist behind the ASA and the subnet on the tunnel interface, and add the prefixes under the **Add Additional Network Spaces** section.

Verify

Use this section in order to confirm that your configuration works properly.

Step 1. Verify that an IKEv2 session is established with command **show crypto ikev2 sa**.

<#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
```

Step 2. Verify that an IPsec SA is also negotiated with the use of the **show crypto ipsec sa** command.

<#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#
```

Step 3. Verify connectivity over the tunnel to the BGP remote router with the use of **ping and ping tcp** in order to validate layer 3 routing and layer 4 connectivity for BGP or the endpoint resources if you use static routing.

<#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#
```

Step 4. When you use BGP, verify BGP connectivity routes received and advertised to Azure and the routing table of the ASA.

<#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
```

Step 5. Ping a device over the tunnel. In this example, it is an Ubuntu VM that runs in Azure.

<#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
```

View the effective routes on the remote VM now. They must show the routes the ASA advertised to the cloud as shown in the image.

Dashboard > Resource groups > CX-SecurityTLs-ResourceGroup > jyoungta-ubuntu-azure - Diagnose and solve problems > Effective routes

Effective routes

Download Refresh

Showing only top 200 records, click Download above to see all.

Scope: Virtual machine (jyoungta-ubuntu-azure)

Network interface: jyoungta-ubuntu-azur956

Effective routes

SOURCE	STATE	ADDRESS PREFIXES	NEXT HOP TYPE	NEXT HOP TYPE IP ADDRESS
Default	Active	10.1.0.0/16	Virtual network	-
Virtual network gateway	Active	192.168.100.0/30	Virtual network gateway	A.A.A.A
Virtual network gateway	Active	192.168.100.1/32	Virtual network gateway	A.A.A.A
Virtual network gateway	Active	192.168.2.0/24	Virtual network gateway	A.A.A.A
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	100.64.0.0/10	None	-
Default	Active	172.16.0.0/12	None	-
Default	Active	192.168.0.0/16	None	-

Troubleshoot

There is currently no specific information available to troubleshoot this configuration.