SD-WAN with Gateway – VPN Connectivity Architecture & Design

Table of Contents

[Overview 3](#_Toc116554757)

[SASE 5](#_Toc116554758)

[ Secure web gateway (SWG) 6](#_Toc116554759)

[ Cloud access security broker (CASB) 6](#_Toc116554760)

[ Firewall as a service (FWaaS) 6](#_Toc116554761)

[ Zero Trust Network Access (ZTNA) and Total Internet Control (TIC) 7](#_Toc116554762)

[ Centralized and unified management 7](#_Toc116554763)

[GOAL 7](#_Toc116554764)

[Direct Interconnect Model Design 8](#_Toc116554765)

[Direct Interconnect Model Detail Design 9](#_Toc116554766)

[Automation details 9](#_Toc116554767)

[Access control 9](#_Toc116554768)

[Upload branch device information 9](#_Toc116554769)

[Device configuration download and connectivity 9](#_Toc116554770)

[Device configuration file 10](#_Toc116554771)

[Connectivity details 12](#_Toc116554772)

[Initiator 13](#_Toc116554773)

[Responder 13](#_Toc116554774)

[Custom policies for IPsec connectivity 14](#_Toc116554775)

[Direct Interconnect model with NVA-in-VWAN-hub 16](#_Toc116554776)

[Key benefits of NVA 17](#_Toc116554777)

[Partners 17](#_Toc116554778)

[Architecture Design USE-Cases Decisions 19](#_Toc116554779)

[Any-to-any connectivity 19](#_Toc116554780)

[Security provided by Azure Firewall along with connectivity NVA 20](#_Toc116554781)

[Create a VPN gateway 24](#_Toc116554782)

[About the gateway subnet 24](#_Toc116554783)

[Create the gateway 24](#_Toc116554784)

[View the public IP address 29](#_Toc116554785)

[Create a local network gateway 29](#_Toc116554786)

[Configure your VPN device 32](#_Toc116554787)

[Create VPN connections 33](#_Toc116554788)

[To configure additional connection settings (optional) 35](#_Toc116554789)

[Verify the VPN connection 35](#_Toc116554790)

[Connect to a virtual machine 36](#_Toc116554791)

[Optional steps 37](#_Toc116554792)

[Resize a gateway SKU 37](#_Toc116554793)

[Reset a gateway 38](#_Toc116554794)

[Add another connection 38](#_Toc116554795)

[Additional configuration considerations 38](#_Toc116554796)

[GCP VPN Design 39](#_Toc116554797)

[FISGlobal VPN Gateway Tunnel 42](#_Toc116554798)

# Overview

Azure Virtual WAN is a networking service that brings connectivity and security services with a single operational interface. These services include branch (via Site-to-site VPN), remote user (Point-to-site VPN), private (ExpressRoute) connectivity, intra-cloud transitive connectivity for VNets, VPN and ExpressRoute interconnectivity, routing, Azure Firewall, and encryption for private connectivity. For this design and architecture, we are focusing on the planning, delivery, architecture, design, and implementation that is required. The overall goal is to provide connectivity, but ultimately, we want to have an environment here at SMBC that is secure and resilient. Therefore, we want to use a SASE base approach defined throughout this design architecture. With that said, we will make sure in this design document, we cover all the delineated bases.

The Challenge in multi-cloud, multi-vendor is getting connectivity right. Everything will need connectivity technology, such as Azure ExpressRoute, Google Dedicated Interconnect, VMware NSX, and more. They also all have their connectivity requirements and specifics. First and foremost, a detailed network plan before they start building multi-cloud environments.

* Exploring the different connectivity concepts, such as VPN, SD-WAN, SASE, Virtual Wan, and direct connections to the major clouds of Microsoft Azure, Google Cloud Platform, FISGlobal, On-premises
* Designing a network topology addressing cost, security, internet access, and service levels
* Understanding different network protocols that are needed
* Define state for Hub-Spoke Model

Diagram

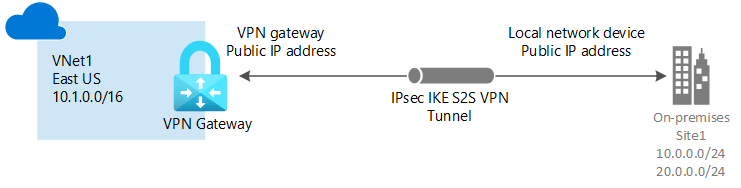
Description automatically generated

Timeline

Description automatically generated

Diagram

Description automatically generated



SASE - **Secure Access Service Edge (SASE)(SASSY)** is a framework for a network architecture that brings cloud-native security technologies—SWG, CASB, ZTNA, and FWaaS in particular—together with wide area network (WAN) capabilities to securely connect users, systems, and endpoints to applications and services anywhere. SASE is a network architecture that rolls software-defined wide area networking (SD-WAN) and security into a cloud service that promises simplified WAN deployment, improved efficiency, and security and provides appropriate bandwidth per application. Because it’s a cloud service, SASE (pronounced “sassy”) can be readily scaled up and scaled down and billed based on usage. As a result, it can be an attractive option in a time of rapid change. A secure access service edge (SASE) is a technology used to deliver wide area network (WAN) and security controls as a cloud computing service directly to the source of connection (user, device, Internet of things (IoT) device, or edge computing location) rather than a data center. It uses cloud and edge computing technologies to reduce the latency that results from backhauling all WAN traffic over long distances to one or a few corporate data centers due to the increased movement off-premises of dispersed users and their applications.[2] This also helps organizations support dispersed users and their devices with digital transformation and application modernization initiatives. Security is based on digital identity, real-time context, and company and regulatory compliance policies rather than a security appliance like a firewall. A digital identity may be attached to anything from a person to a device, cloud service, application software, IoT system, or any computing system. SASE can be broken into six components.

 SD-WAN-**Software-Defined Wide Area Network** (**SD-WAN**) is a wide area network that uses software-defined network technology, such as communicating over the Internet using overlay tunnels encrypted when destined for internal organization locations. If standard tunnel setup and configuration messages are supported by all network hardware vendors, SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. This concept is like how software-defined networking implements virtualization technology to improve data center management and operation. In practice, proprietary protocols are used to set up and manage an SD-WAN, meaning there is no decoupling of the hardware and its control mechanism. A key application of SD-WAN is to allow companies to build higher-performance WANs using lower-cost and commercially available Internet access, enabling businesses to replace more expensive private WAN connection technologies partially or wholly, such as MPLS. When SD-WAN traffic is carried over the Internet, there are no end-to-end performance guarantees. Carrier MPLS VPN WAN services are not carried as Internet traffic but rather over carefully controlled carrier capacity and come with an end-to-end performance guarantee.

## Secure web gateway (SWG)

A secure web gateway is a web security service that filters unauthorized traffic from accessing a particular network. The goal of an SWG is to zero in on threats before they penetrate a virtual perimeter. An SWG accomplishes this by combining technologies like malicious code detection, malware elimination, and URL filtering.

## Cloud access security broker (CASB)

A cloud access security broker is a SaaS application that acts as a security checkpoint between on-premises networks and cloud-based applications and enforces data security policies. A **CASB** protects corporate data through prevention, monitoring, and mitigation techniques. It can also identify malicious behavior and warn administrators about compliance violations.

## Firewall as a service (FWaaS)

Firewall as a service moves firewall protection to the cloud instead of the traditional network perimeter. This enables organizations to securely connect a remote, mobile workforce to the corporate network while still enforcing consistent security policies that reach beyond the organization’s geographic footprint.

## Zero Trust Network Access (ZTNA) and Total Internet Control (TIC)

Zero Trust Network Access is a set of consolidated, cloud-based technologies that operate on a framework in which trust is never implicit and access is granted on a need-to-know, least-privileged basis across all users, devices, and applications. In this model, all users must be authenticated, authorized, and continuously validated before granting access to company private applications and data. ZTNA eliminates the poor user experience, operational complexities, costs, and risks of a traditional VPN.

## Centralized and unified management

A modern SASE platform will allow administrators to manage SD-WAN, SWG, CASB, FWaaS, and ZTNA through centralized and unified management across networking and security. This frees IT team members to focus their energy on other more pressing areas and boosts the user experience for the organization’s hybrid workforce.

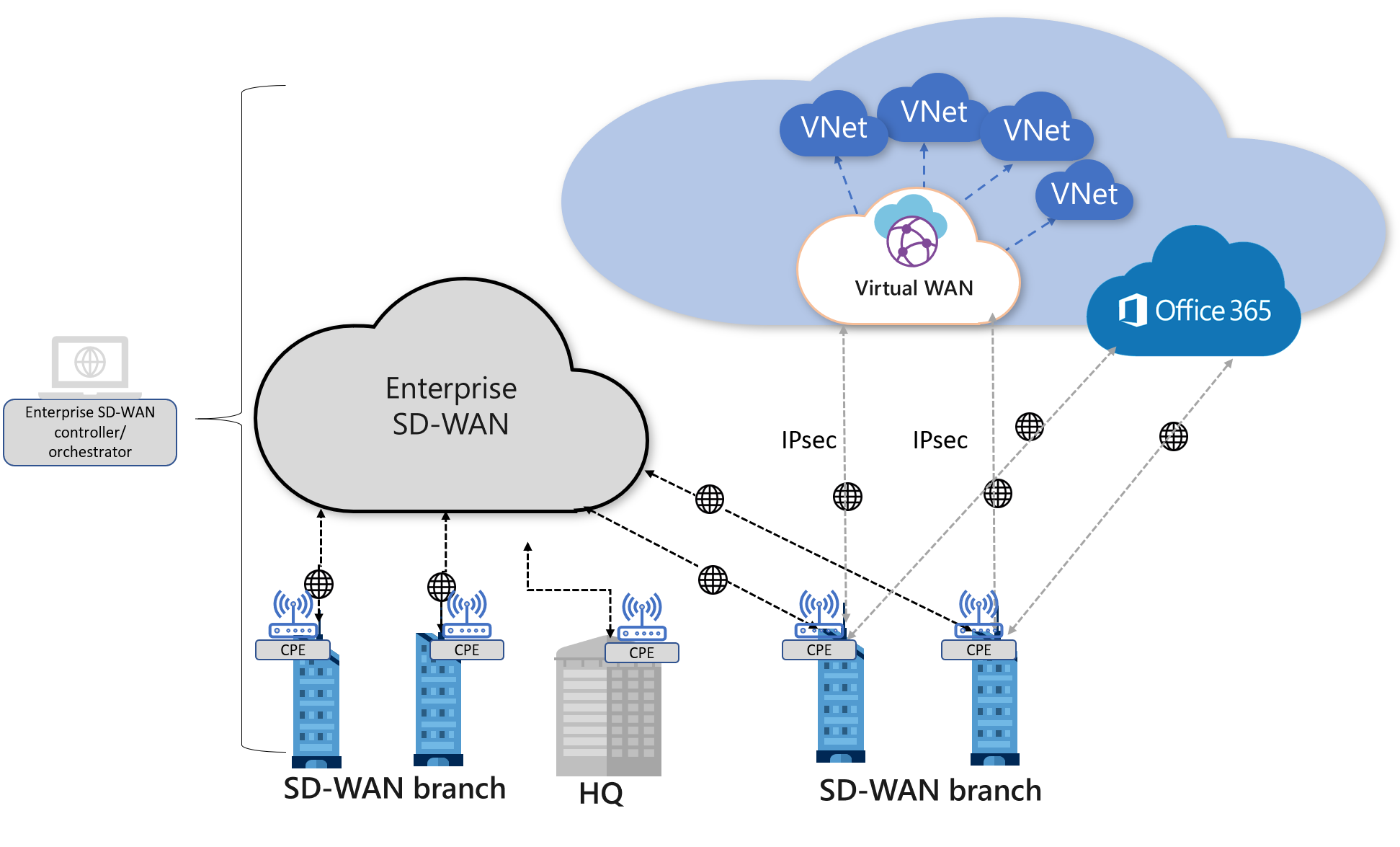
# GOAL

Azure Virtual WAN is a cloud-based SD-WAN that provides a rich suite of Azure first-party connectivity, routing, and security services; Azure Virtual WAN also is designed to enable interconnection with premises-based SD-WAN and SASE technologies and services. The services should be offered by the Virtual WAN ecosystem. From an ecosystem, it is recommended from a connectivity and security design architecture to transform private WAN to SD-WAN using the SASE model to have options when interconnecting their private SD-WAN with Azure Virtual WAN. Here are the options and designs we will go through more in-depth.

* Direct Interconnect model
* Direct Interconnect model with NVA-in-VWAN-hub
* Indirect Interconnect model
* Managed Hybrid WAN model

In all these cases, the interconnection of Virtual WAN with SD-WAN is similar from the connectivity side but may vary on the orchestration and operational side.

## Direct Interconnect Model Design



In this architecture model, the SD-WAN branch customer-premises equipment (CPE) is directly connected to Virtual WAN hubs via IPsec connections. The branch CPE may also be connected to other branches via the private SD-WAN or use Virtual WAN for branch-to-branch connectivity. Branches that need to access their workloads in Azure will be able to directly and securely access Azure via the IPsec tunnel(s) that are terminated in the Virtual WAN hub(s).

SD-WAN CPE partners/Vendors such as FISGlobal can enable automation to automate the normally tedious and error-prone IPsec connectivity from their respective CPE devices. Automation allows the SD-WAN controller to talk to Azure via the Virtual WAN API to configure the Virtual WAN sites and push necessary IPsec tunnel configuration to the branch CPEs. The SD-WAN CPE continues to be where traffic optimization and path selection are implemented and enforced.

In this model, some vendor proprietary traffic optimization based on real-time traffic characteristics may not be supported because the connectivity to Virtual WAN is over IPsec, and the IPsec VPN is terminated on the Virtual WAN VPN gateway. For example, dynamic path selection at the branch CPE is feasible due to the branch device exchanging various network packet information with another SD-WAN node, hence identifying the best link to use for various prioritized traffic dynamically at the branch. This feature may be useful in areas where last-mile optimization (branch to the closest Microsoft POP) is required.

With Virtual WAN, users can get Azure Path Selection, a policy-based path selection across multiple ISP links from the branch CPE to Virtual WAN VPN gateways. Virtual WAN allows for the setup of multiple links (paths) from the same SD-WAN branch CPE; each link represents a dual tunnel connection from a unique public IP of the SD-WAN CPE to two different instances of Azure Virtual WAN VPN gateway. SD-WAN vendors can implement the most optimal path to Azure based on traffic policies set by their policy engine on the CPE links. On the Azure end, all connections coming in are treated equally.

### Direct Interconnect Model Detail Design

## Automation details

### Access control

SMBC must be able to set up appropriate access control for Virtual WAN in the device UI. This is recommended using an Azure Service Principal. Service principal-based access provides the device controller with appropriate authentication to upload branch information. While this functionality is outside of the Azure Virtual WAN offering, below are the typical steps taken to set up access in Azure, after which the relevant details are inputted into the device management dashboard.

* Create an Azure Active Directory application for your on-premises device controller.
* Get the application ID and authentication key
* Get tenant ID
* Assign application to role "Contributor."

### Upload branch device information

Design the user experience to upload branch (on-premises site) information to Azure. You can use REST APIs for VPNSite to create the site information in Virtual WAN. Provide all branch SDWAN/VPN devices or select device customizations as appropriate.

### Device configuration download and connectivity

This step involves downloading Azure configuration and setting up connectivity from the branch device into Azure Virtual WAN. In this step, a customer not using a provider would manually download the Azure configuration and apply it to their on-premises SDWAN/VPN device. As a provider, you should automate this step. View the download [REST APIs](https://learn.microsoft.com/en-us/rest/api/virtualwan/vpnsitesconfiguration/download) for additional information. The device controller can call the 'GetVpnConfiguration' REST API to download the Azure configuration.

**Configuration notes**

* If Azure VNets are attached to the virtual hub, they will appear as ConnectedSubnets.
* VPN connectivity uses the route-based configuration and supports both IKEv1, and IKEv2 protocols.

## Device configuration file

The device configuration file contains the settings to use when configuring your on-premises VPN device. When you view this file, notice the following information:

* **vpnSiteConfiguration -** This section denotes the device details set up as a site connecting to the virtual WAN. It includes the name and public ip address of the branch device.
* **vpnSiteConnections -** This section provides information about the following:
  + **Address space** of the virtual hub(s) VNet.  
    Example:

"AddressSpace":"10.1.0.0/24"

* **Address space** of the VNets that are connected to the hub.  
  Example:

"ConnectedSubnets":["10.2.0.0/16","10.3.0.0/16"]

* **IP addresses** of the virtual hub VPN gateway. Because the VPN gateway has each connection comprising two tunnels in an active-active configuration, you will see both IP addresses listed in this file. In this example, you see "Instance0" and "Instance1" for each site.  
  Example:

"Instance0":"104.45.18.186"

"Instance1":"104.45.13.195"

**Vpngateway connection configuration details** such as BGP, pre-shared key, etc. The PSK is the pre-shared key that is automatically generated for you. You can always edit the connection on the Overview page for a custom PSK.

**Example device configuration file**

{

"configurationVersion":{

"LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",

"Version":"r403583d-9c82-4cb8-8570-1cbbcd9983b5"

},

"vpnSiteConfiguration":{

"Name":"testsite1",

"IPAddress":"73.239.3.208"

},

"vpnSiteConnections":[

{

"hubConfiguration":{

"AddressSpace":"10.1.0.0/24",

"Region":"West Europe",

"ConnectedSubnets":[

"10.2.0.0/16",

"10.3.0.0/16"

]

},

"gatewayConfiguration":{

"IpAddresses":{

"Instance0":"104.45.18.186",

"Instance1":"104.45.13.195"

}

},

"connectionConfiguration":{

"IsBgpEnabled":false,

"PSK":"bkOWe5dPPqkx0DfFE3tyuP7y3oYqAEbI",

"IPsecParameters":{

"SADataSizeInKilobytes":102400000,

"SALifeTimeInSeconds":3600

}

}

}

]

},

{

"configurationVersion":{

"LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",

"Version":"1f33f891-e1ab-42b8-8d8c-c024d337bcac"

},

"vpnSiteConfiguration":{

"Name":" testsite2",

"IPAddress":"66.193.205.122"

},

"vpnSiteConnections":[

{

"hubConfiguration":{

"AddressSpace":"10.1.0.0/24",

"Region":"West Europe"

},

"gatewayConfiguration":{

"IpAddresses":{

"Instance0":"104.45.18.187",

"Instance1":"104.45.13.195"

}

},

"connectionConfiguration":{

"IsBgpEnabled":false,

"PSK":"XzODPyAYQqFs4ai9WzrJour0qLzeg7Qg",

"IPsecParameters":{

"SADataSizeInKilobytes":102400000,

"SALifeTimeInSeconds":3600

}

}

}

]

},

{

"configurationVersion":{

"LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",

"Version":"cd1e4a23-96bd-43a9-93b5-b51c2a945c7"

},

"vpnSiteConfiguration":{

"Name":" testsite3",

"IPAddress":"182.71.123.228"

},

"vpnSiteConnections":[

{

"hubConfiguration":{

"AddressSpace":"10.1.0.0/24",

"Region":"West Europe"

},

"gatewayConfiguration":{

"IpAddresses":{

"Instance0":"104.45.18.187",

"Instance1":"104.45.13.195"

}

},

"connectionConfiguration":{

"IsBgpEnabled":false,

"PSK":"YLkSdSYd4wjjEThR3aIxaXaqNdxUwSo9",

"IPsecParameters":{

"SADataSizeInKilobytes":102400000,

"SALifeTimeInSeconds":3600

}

}

}

]

## Connectivity details

Your on-premises SDWAN/VPN device or SD-WAN configuration must match or contain the following algorithms and parameters, which specify in the Azure IPsec/IKE policy.

* IKE encryption algorithm
* IKE integrity algorithm
* DH Group
* IPsec encryption algorithm
* IPsec integrity algorithm
* PFS Group

**Note:** When working with Default policies, Azure can act as both initiator and responder during an IPsec tunnel setup. While Virtual WAN VPN supports many algorithm combinations, our recommendation is GCMAES256 for IPSEC Encryption and Integrity for optimal performance. AES256 and SHA256 are considered less performant, and therefore, performance degradation, such as latency and packet drops, can be expected for similar algorithm types.

### Initiator

The following sections list the supported policy combinations when Azure is the initiator for the tunnel.

**Phase-1**

* AES\_256, SHA1, DH\_GROUP\_2
* AES\_256, SHA\_256, DH\_GROUP\_2
* AES\_128, SHA1, DH\_GROUP\_2
* AES\_128, SHA\_256, DH\_GROUP\_2

**Phase-2**

* GCM\_AES\_256, GCM\_AES\_256, PFS\_NONE
* AES\_256, SHA\_1, PFS\_NONE
* AES\_256, SHA\_256, PFS\_NONE
* AES\_128, SHA\_1, PFS\_NONE

### Responder

The following sections list the supported policy combinations when Azure is the responder for the tunnel.

**Phase-1**

* AES\_256, SHA1, DH\_GROUP\_2
* AES\_256, SHA\_256, DH\_GROUP\_2
* AES\_128, SHA1, DH\_GROUP\_2
* AES\_128, SHA\_256, DH\_GROUP\_2

**Phase-2**

* GCM\_AES\_256, GCM\_AES\_256, PFS\_NONE
* AES\_256, SHA\_1, PFS\_NONE
* AES\_256, SHA\_256, PFS\_NONE
* AES\_128, SHA\_1, PFS\_NONE
* AES\_256, SHA\_1, PFS\_1
* AES\_256, SHA\_1, PFS\_2
* AES\_256, SHA\_1, PFS\_14
* AES\_128, SHA\_1, PFS\_1
* AES\_128, SHA\_1, PFS\_2
* AES\_128, SHA\_1, PFS\_14
* AES\_256, SHA\_256, PFS\_1
* AES\_256, SHA\_256, PFS\_2
* AES\_256, SHA\_256, PFS\_14
* AES\_256, SHA\_1, PFS\_24
* AES\_256, SHA\_256, PFS\_24
* AES\_128, SHA\_256, PFS\_NONE
* AES\_128, SHA\_256, PFS\_1
* AES\_128, SHA\_256, PFS\_2
* AES\_128, SHA\_256, PFS\_14

### Custom policies for IPsec connectivity

When working with custom IPsec policies, keep in mind the following requirements:

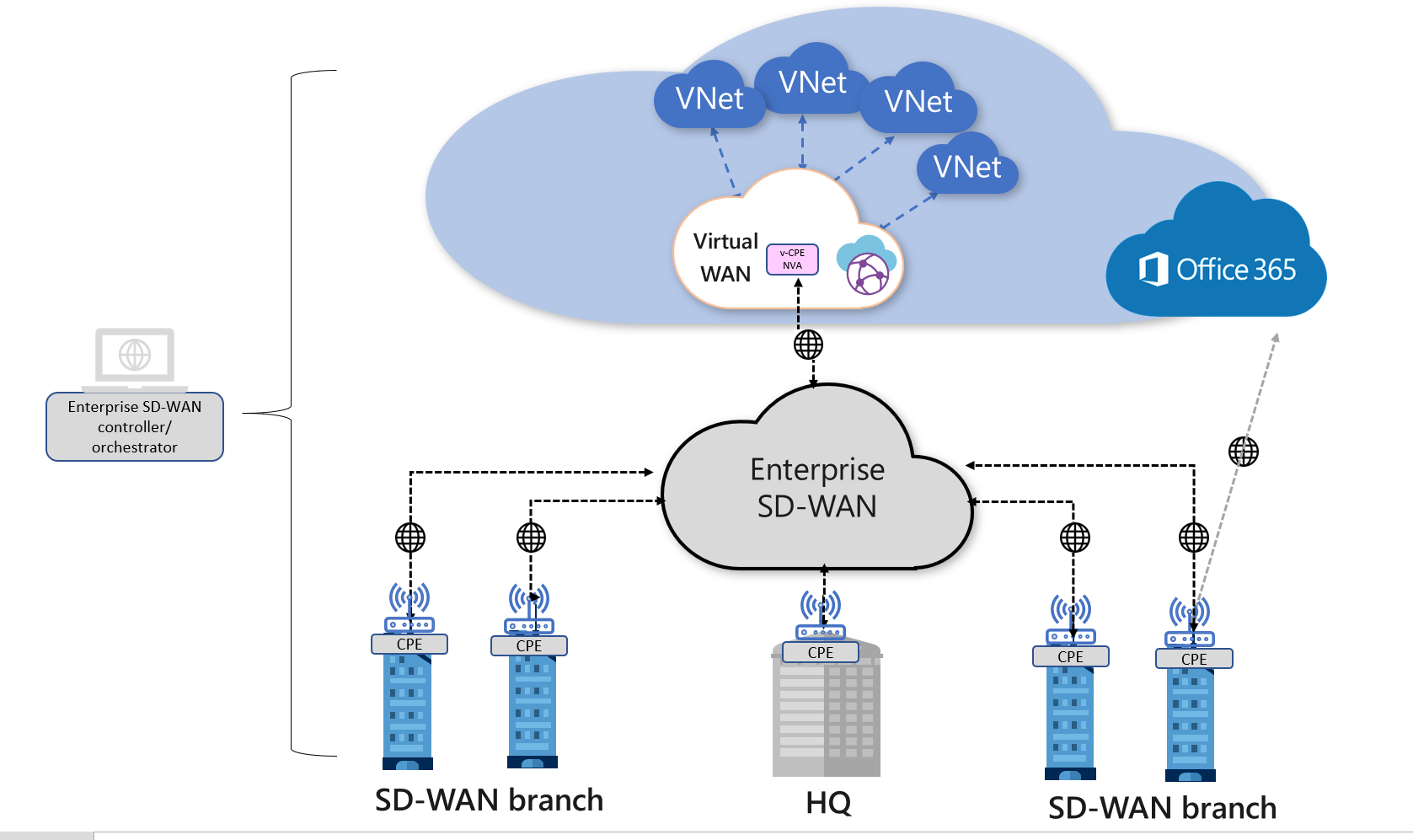
* **IKE** - For IKE, you can select any parameter from IKE Encryption, plus any parameter from IKE Integrity, plus any parameter from DH Group.
* **IPsec** - For IPsec, you can select any parameter from IPsec Encryption, plus any parameter from IPsec Integrity, plus PFS. If any of the parameters for IPsec Encryption or IPsec Integrity is GCM, then the parameters for both settings must be GCM.

**Note:** With Custom IPsec policies, there is no concept of responder and initiator (unlike Default IPsec policies). Both sides (on-premises and Azure VPN gateway) will use the same settings for IKE Phase 1 and IKE Phase 2. Both IKEv1 and IKEv2 protocols are supported.

**Available settings and parameter**

| **Setting** | **Parameters** |
| --- | --- |
| IKE Encryption | GCMAES256, GCMAES128, AES256, AES128 |
| IKE Integrity | SHA384, SHA256 |
| DH Group | ECP384, ECP256, DHGroup24, DHGroup14 |
| IPsec Encryption | GCMAES256, GCMAES128, AES256, AES128, None |
| IPsec Integrity | GCMAES256, GCMAES128, SHA256 |
| PFS Group | ECP384, ECP256, PFS24, PFS14, None |
| SA Lifetime | integer; min. 300/ default 3600 seconds |

# Direct Interconnect model with NVA-in-VWAN-hub



This architecture model supports the deployment of a third-party Network Virtual Appliance (NVA) directly into the virtual hub. This can allow SMBC to connect branch CPE to the same brand NVA in the virtual hub so that they can take advantage of proprietary end-to-end SD-WAN capabilities when connecting to Azure workloads.

Several Virtual WAN Partners have worked to provide an experience configuring the NVA automatically as part of the deployment process. Once the NVA has been provisioned into the virtual hub, any additional configuration required for the NVA must be done via the NVA partners portal or management application. Direct access to the NVA isn't available. The NVAs available to be deployed directly into the Azure Virtual WAN hub is engineered specifically to be used in the virtual hub.

The SD-WAN CPE continues to be where traffic optimization and path selection are implemented and enforced. Vendor proprietary traffic optimization based on real-time traffic characteristics is supported because the connectivity to Virtual WAN is via the SD-WAN NVA in the hub.

SMBC can deploy select Network Virtual Appliances (NVAs) directly into a Virtual WAN hub in a solution jointly managed by Microsoft Azure and third-party Network Virtual Appliance vendors. Not all Network Virtual Appliances in Azure Marketplace can be deployed into a Virtual WAN hub. For a full list of the available partner below

### Key benefits of NVA

When an NVA is deployed into a Virtual WAN hub, it can serve as a third-party gateway with various functionalities. It could serve as an SD-WAN gateway, Firewall, or a combination of both.

Deploying NVAs into a Virtual WAN hub provides the following benefits:

* **Pre-defined and pre-tested selection of infrastructure choices (**[**NVA Infrastructure Units**](https://learn.microsoft.com/en-us/azure/virtual-wan/about-nva-hub#units)**)**: Microsoft and the partner work together to validate throughput and bandwidth limits before making the solution available to customers.
* **Built-in availability and resiliency**: Virtual WAN NVA deployments are Availability Zone (AZ) aware and are automatically configured to be highly available.
* **No-hassle provisioning and bootstrapping**: A managed application is pre-qualified for provisioning and bootstrapping for the Virtual WAN platform. This managed application is available through the Azure Marketplace link.
* **Simplified routing**: Leverage Virtual WAN's intelligent routing systems. NVA solutions peer with the Virtual WAN hub router and participate in the Virtual WAN routing decision process similarly to Microsoft Gateways.
* **Integrated support**: Partners have a special support agreement with Microsoft Azure Virtual WAN to diagnose and resolve customer problems quickly.
* **Platform-provided lifecycle management**: Upgrades and patches are a part of the Azure Virtual WAN service. This removes the complexity of lifecycle management from a customer deploying Virtual Appliance solutions.
* **Integrated with platform features**: Transit connectivity with Microsoft gateways and Virtual Networks, Encrypted ExpressRoute (SD-WAN overlay running over an ExpressRoute circuit), and Virtual hub route tables interact seamlessly.

## Partners

The following SD-WAN connectivity Network Virtual Appliances can be deployed in the Virtual WAN hub.

| **Partners** | **Configuration/How-to/Deployment guide** | **Dedicated support model** |
| --- | --- | --- |
| [Barracuda Networks](https://azuremarketplace.microsoft.com/marketplace/apps/barracudanetworks.barracuda_cloudgenwan_gateway?tab=Overviewus/marketplace/apps/barracudanetworks.barracuda_cloudgenwan_gateway?tab=Overview) | [Barracuda CloudGen WAN deployment guide](https://campus.barracuda.com/product/cloudgenwan/doc/91980640/deployment/) | Yes |
| [Cisco Cloud Service Router(CSR) VWAN](https://aka.ms/ciscoMarketPlaceOffer) | The integration of the Cisco SD-WAN solution with Azure virtual WAN enhances Cloud OnRamp for Multi-Cloud deployments and enables configuring Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) as a network virtual appliance (NVA) in Azure Virtual WAN hubs. [View Cisco SD-WAN Cloud OnRamp, Cisco IOS XE Release 17.x configuration guide](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/cloudonramp/ios-xe-17/cloud-onramp-book-xe/cloud-onramp-multi-cloud.html#Cisco_Concept.dita_c61e0e7a-fff8-4080-afee-47b81e8df701) | Yes |
| [VMware SD-WAN](https://sdwan.vmware.com/partners/microsoft) | [VMware SD-WAN in Virtual WAN hub deployment guide](https://kb.vmware.com/s/article/82746). The managed application for deployment can be found at this [Azure Marketplace link](https://azuremarketplace.microsoft.com/marketplace/apps/velocloud.vmware_sdwan_in_vwan). | Yes |
| [Versa Networks](https://versa-networks.com/partners/microsoft-azure.php) | If you're an existing Versa Networks customer, log on to your Versa account and access the deployment guide using the following link [Versa Deployment Guide](https://docs.versa-networks.com/Special:AuthenticationProviders?returntotitle=Getting_Started%2FDeployment_and_Initial_Configuration%2FBranch_Deployment%2FInitial_Configuration%2FInstall_a_VOS_Cloud_Gateway_on_an_Azure_Virtual_WAN). If you're a new Versa customer, sign-up using the [Versa preview sign-up link](https://versa-networks.com/demo/). | Yes |
| [Fortinet SD-WAN](https://www.fortinet.com/products/next-generation-firewall) | [Fortinet SD-WAN deployment guide](https://aka.ms/fortinetsdwandeploy). The managed application for this deployment can be found at this [Azure Marketplace Link](https://portal.azure.com/#create/fortinet.fortigate_vwan_nvamanagedfgtvwan). | No |
| [Aruba EdgeConnect](https://www.arubanetworks.com/products/sd-wan/edgeconnect) | [Aruba EdgeConnect SD-WAN deployment guide](https://aka.ms/arubasdwandeploy). | No |

The following security Network Virtual Appliance can be deployed in the Virtual WAN hub. This Virtual Appliance can be used to inspect all North-South, East-West, and Internet-bound traffic.

| **Partners** | **Configuration/How-to/Deployment guide** | **Dedicated support model** |
| --- | --- | --- |
| [Check Point CloudGuard Network Security (CGNS) Firewall](https://pages.checkpoint.com/cgns-vwan-hub-ea.html) | To access the preview of Check Point CGNS Firewall deployed in the Virtual WAN hub, reach out to DL-vwan-support-preview@checkpoint.com with your subscription ID. | No |
| [Fortinet Next-Generation Firewall (NGFW)](https://www.fortinet.com/products/next-generation-firewall) | To access the preview of Fortinet NGFW deployed in the Virtual WAN hub, reach out to azurevwan@fortinet.com with your subscription ID. For more information about the offering, see the [Fortinet blog post](https://www.fortinet.com/blog/business-and-technology/fortigate-vm-first-ngfw-and-secure-sd-wan-integration-in-microsoft-azure-virtual-wan). | No |

The following dual-role SD-WAN connectivity and security (Next-Generation Firewall) Network Virtual Appliances can be deployed in the Virtual WAN hub. These Virtual Appliances can be used to inspect all North-South, East-West, and Internet-bound traffic.

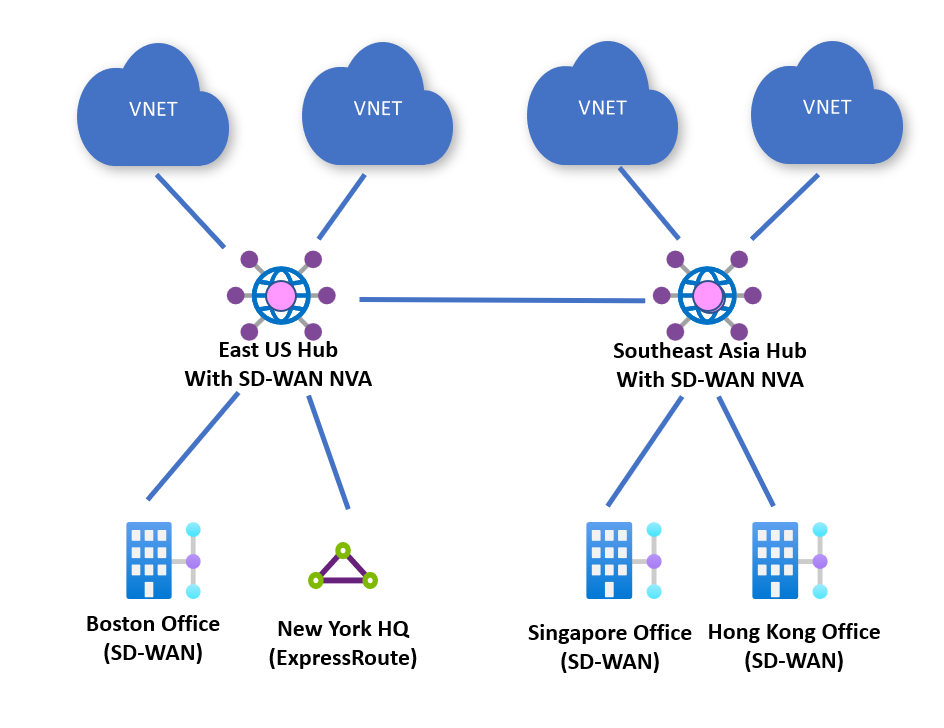
| **Partners** | **Configuration/How-to/Deployment guide** | **Dedicated support model** |
| --- | --- | --- |
| [Fortinet Next-Generation Firewall (NGFW)](https://www.fortinet.com/products/next-generation-firewall) | To access the preview of Fortinet NGFW deployed in the Virtual WAN hub, reach out to azurevwan@fortinet.com with your subscription ID. For more information about the offering, see the [Fortinet blog post](https://www.fortinet.com/blog/business-and-technology/fortigate-vm-first-ngfw-and-secure-sd-wan-integration-in-microsoft-azure-virtual-wan). | No |

# Architecture Design USE-Cases Decisions

## Any-to-any connectivity

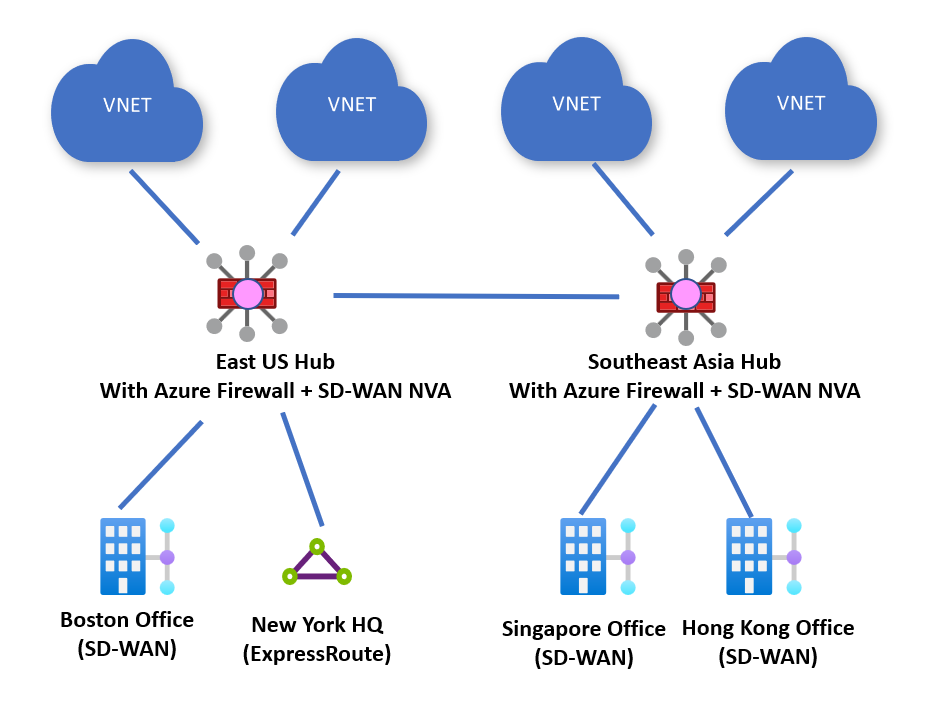
SMBC can deploy an NVA in every Azure region where they have a footprint. Branch sites are connected to Azure via SD-WAN tunnels terminating on the closest NVA deployed in an Azure Virtual WAN hub.

Branch sites can then access workloads in Azure deployed in virtual networks in the same region or other regions through the Microsoft global backbone. SD-WAN related sites can also communicate with other branches that are connected to Azure via ExpressRoute, Site-to-site VPN, or Remote User connectivity.

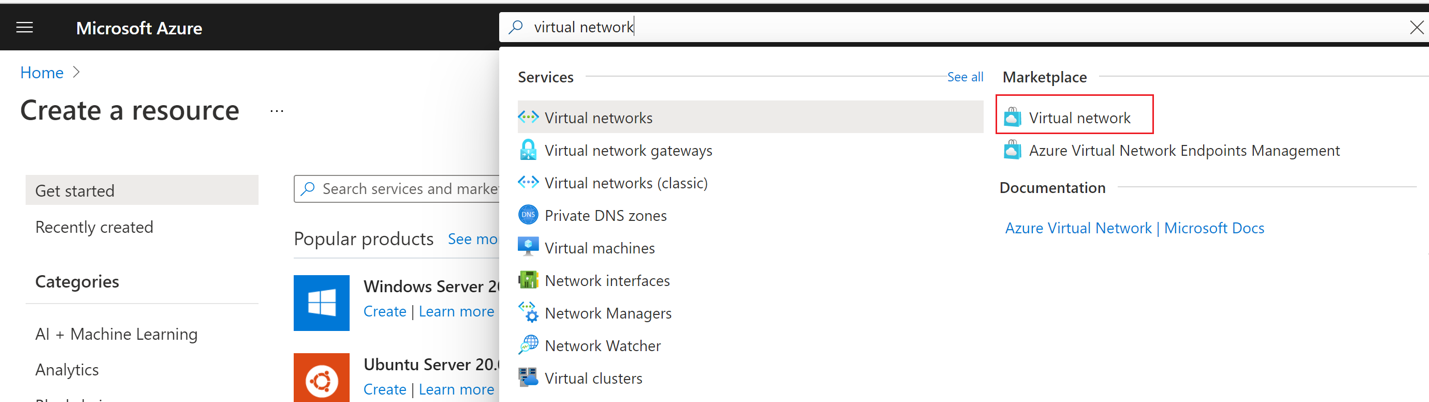


## Security provided by Azure Firewall along with connectivity NVA

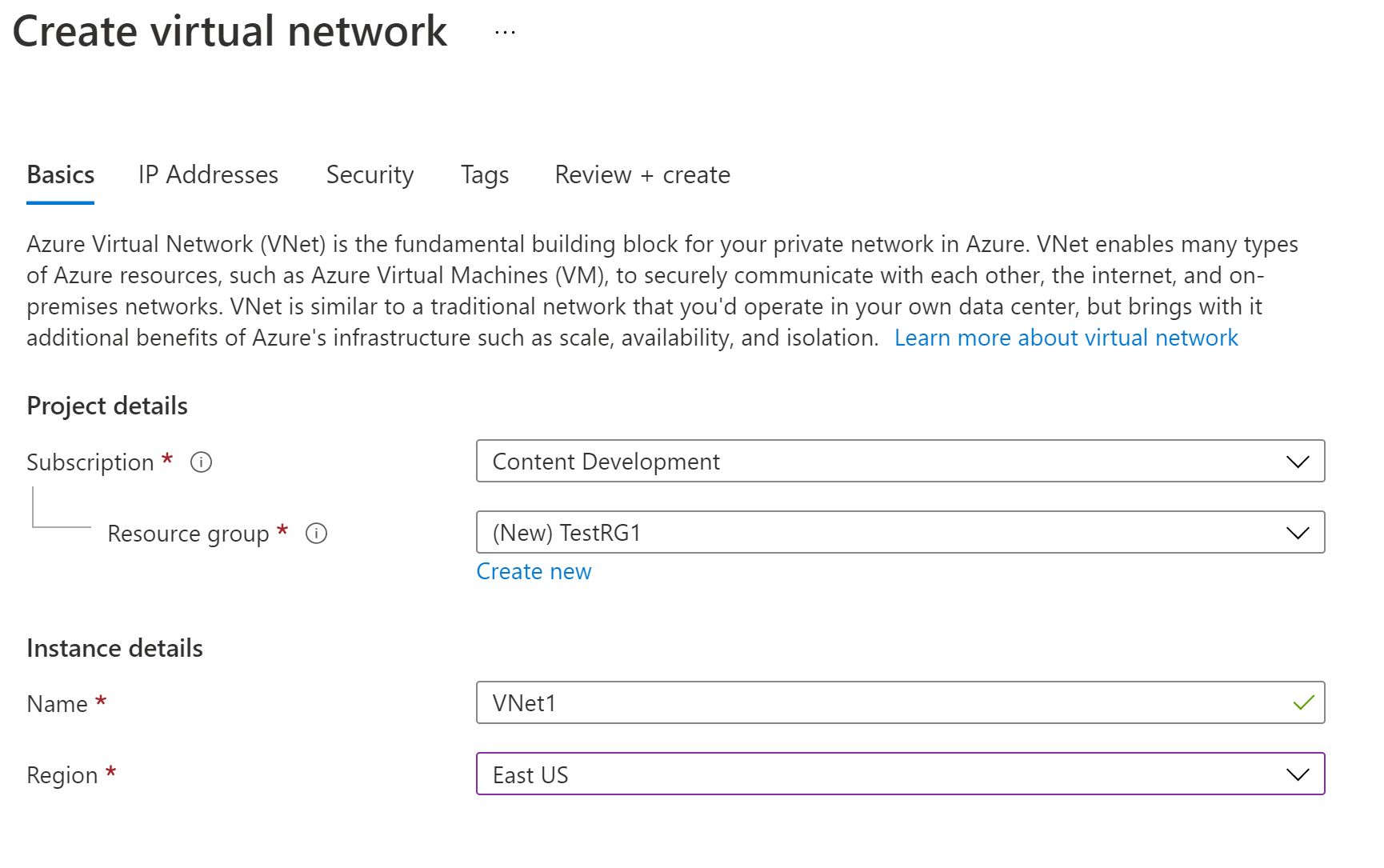
SMBC can deploy an Azure Firewall alongside their connectivity-based NVAs. Virtual WAN routing can be configured to send all traffic to Azure Firewall for inspection. Will also need to configure Virtual WAN to send all internet-bound traffic to Azure Firewall for inspection. The following are uses as examples scenarios.



1. In **Search resources, service, and docs (G+/)**, type ***virtual network***. Select **Virtual network** from the **Marketplace** results to open the **Virtual network** page.

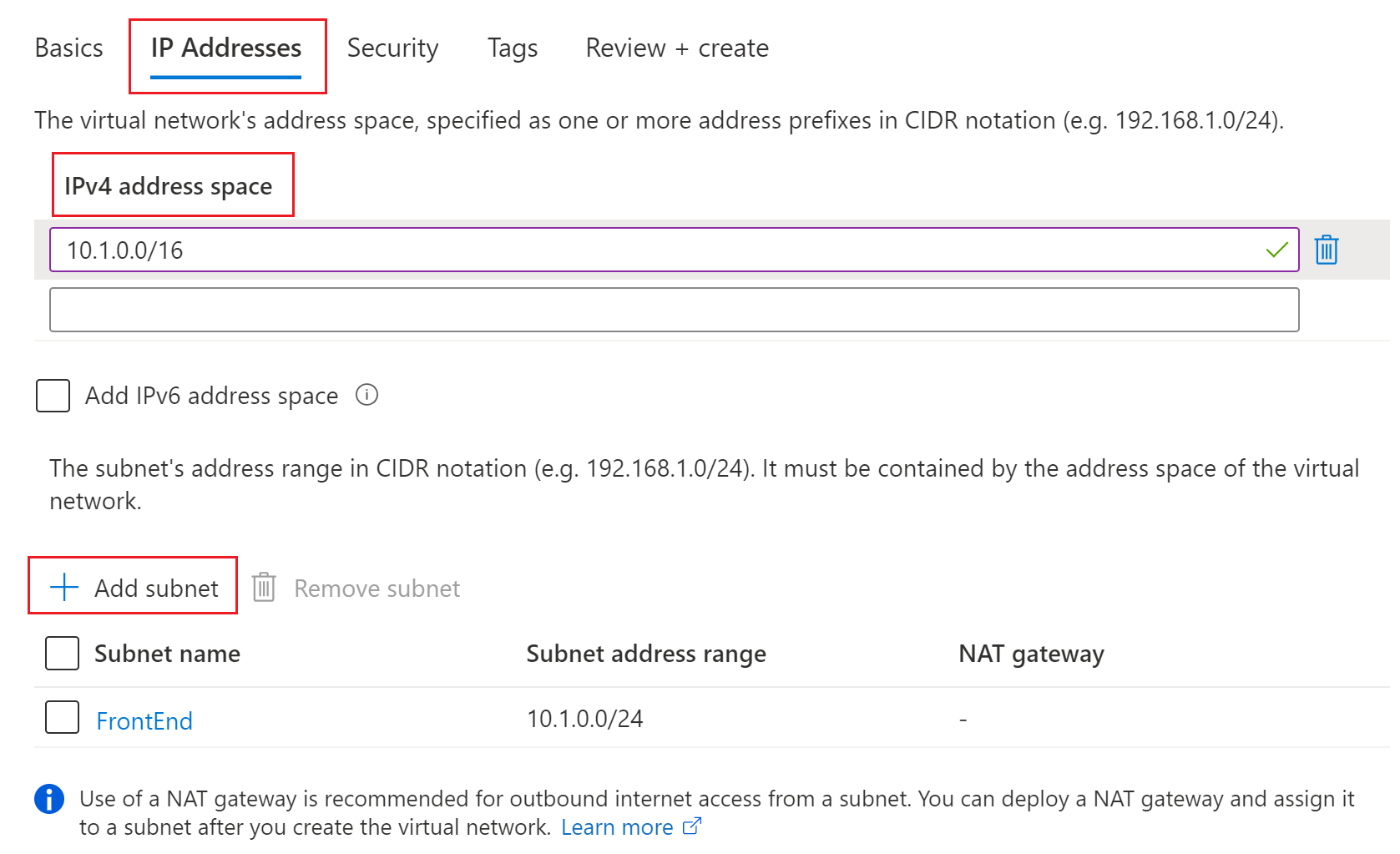
[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-basic-vnet-rm-portal-include/marketplace-expand.png#lightbox)

1. On the **Virtual network** page, select **Create**. This opens the **Create virtual network** page.
2. On the **Basics** tab, configure the VNet settings for **Project details** and **Instance details**. You'll see a green check mark when the values you enter are validated. The values shown in the example can be adjusted according to the settings that you require.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-basic-vnet-rm-portal-include/basics.png#lightbox)

* + **Subscription**: Verify that the subscription listed is the correct one. You can change subscriptions by using the drop-down.
  + **Resource group**: Select an existing resource group, or select **Create new** to create a new one. For more information about resource groups, see [Azure Resource Manager overview](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview#resource-groups).
  + **Name**: Enter the name for your virtual network.
  + **Region**: Select the location for your VNet. The location determines where the resources that you deploy to this VNet will live.

1. Select **IP Addresses** to advance to the IP Addresses tab. On the IP Addresses tab, configure the settings. The values shown in the example can be adjusted according to the settings that you require.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-basic-vnet-rm-portal-include/addresses.png#lightbox)

* + **IPv4 address space**: By default, an address space is automatically created. You can select the address space and adjust it to reflect your own values. You can also add more address spaces by selecting the box below the existing address space and specifying the values for the additional address space.
  + **+ Add subnet**: If you use the default address space, a default subnet is created automatically. If you change the address space, you need to add a subnet. Select **+ Add subnet** to open the **Add subnet** window. Configure the following settings, then select **Add** at the bottom of the page to add the values.
    - **Subnet name**: In this example, we named the subnet "FrontEnd".
    - **Subnet address range**: The address range for this subnet.

1. Select **Security** to advance to the Security tab. At this time, leave the default values.
   * **BastionHost**: Disable
   * **DDoS Protection Standard**: Disable
   * **Firewall**: Disable
2. Select **Review + create** to validate the virtual network settings.
3. After the settings have been validated, select **Create** to create the virtual network.

## Create a VPN gateway

In this step, you create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

### About the gateway subnet

The virtual network gateway uses a specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration to create. Some configurations require more IP addresses than others. We recommend that it creates a gateway subnet that uses a /27 or /28.

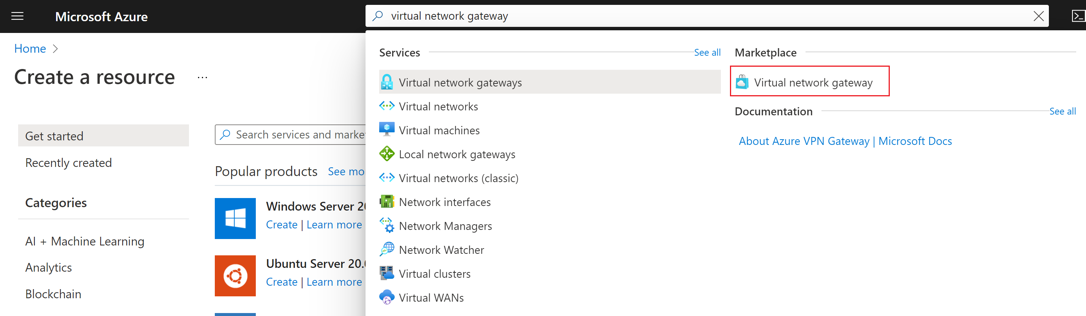
If you see an error that specifies that the address space overlaps with a subnet or that the subnet isn't contained within the address space for your virtual network, check your VNet address range. You may not have enough IP addresses available in the address range you created for your virtual network. For example, if your default subnet encompasses the entire address range, there are no IP addresses left to create additional subnets. You can either adjust your subnets within the existing address space to free up IP addresses or specify an additional address range and create the gateway subnet there.

### Create the gateway

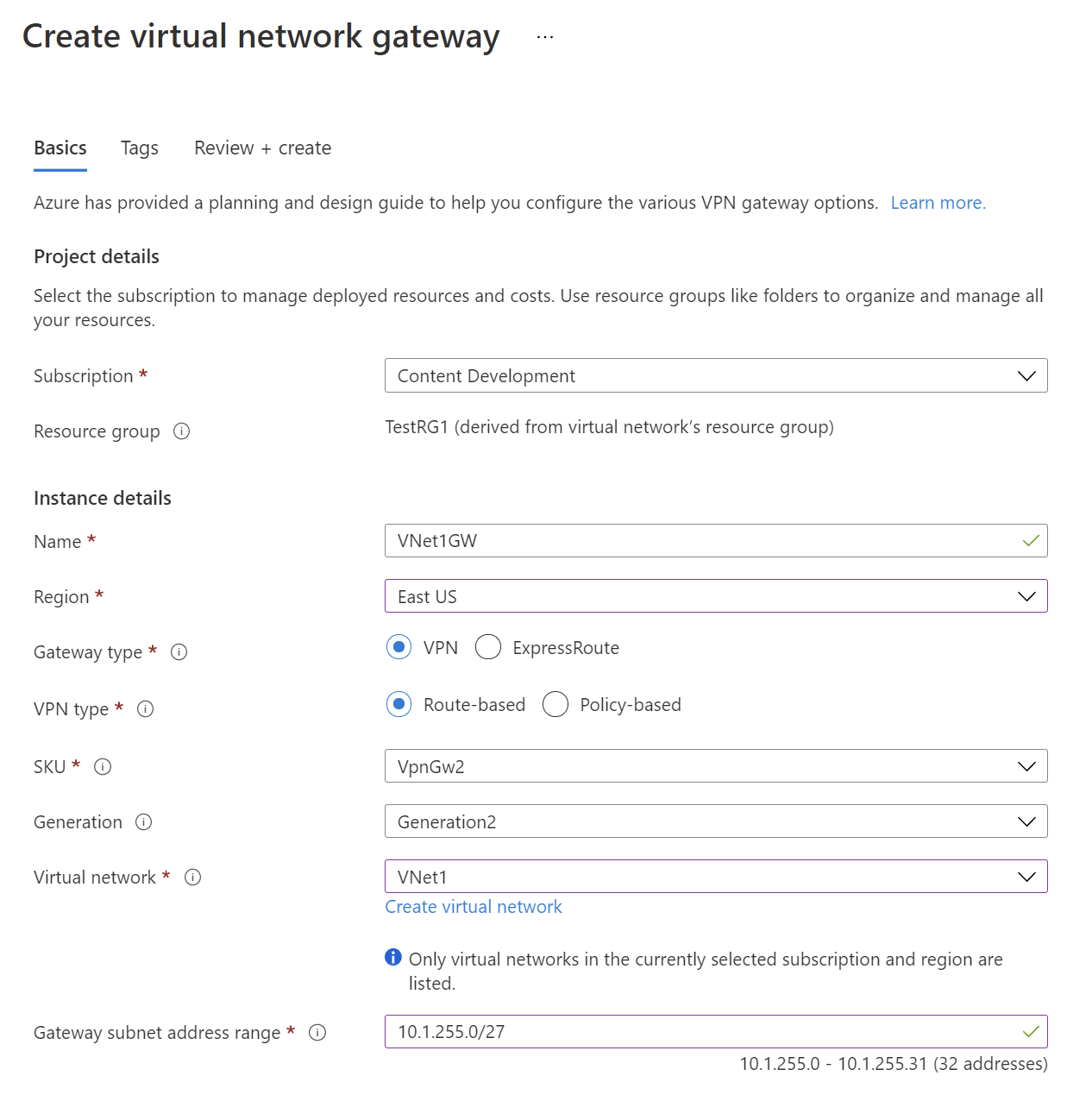
Create a virtual network gateway (VPN gateway) using the following values:

* **Name:** VNet1GW
* **Region:** East US
* **Gateway type:** VPN
* **VPN type:** Route-based
* **SKU:** VpnGw2
* **Generation:** Generation 2
* **Virtual network:** VNet1
* **Gateway subnet address range:** 10.1.255.0/27
* **Public IP address:** Create new
* **Public IP address name:** VNet1GWpip
* **Enable active-active mode:** Disabled
* **Configure BGP:** Disabled

1. In **Search resources, services, and docs (G+/)** type **virtual network gateway**. Locate **Virtual network gateway** in the Marketplace search results and select it to open the **Create virtual network gateway** page.

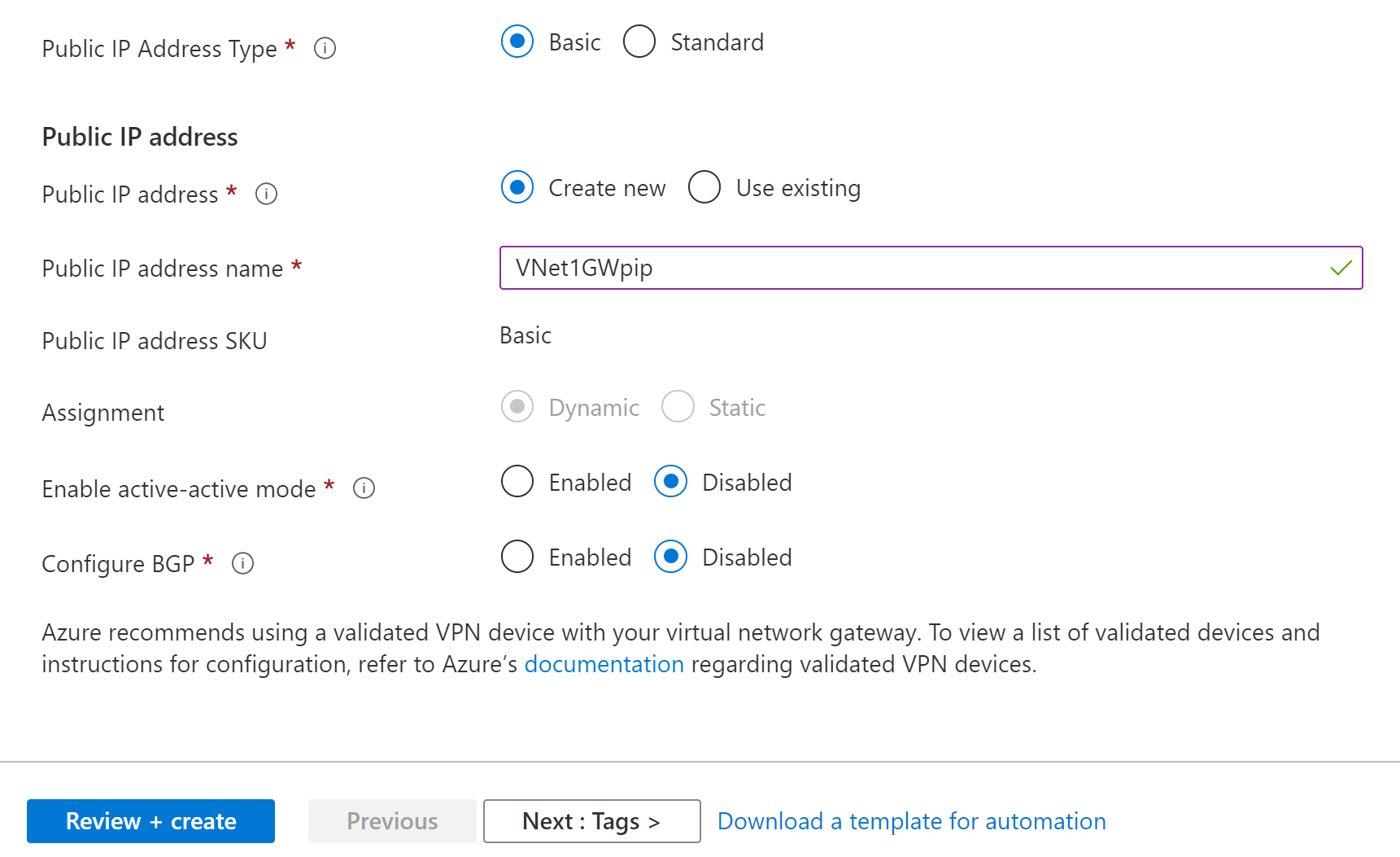
[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-add-gw-portal/search-expand.png#lightbox)

1. On the **Basics** tab, fill in the values for **Project details** and **Instance details**.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-add-gw-portal/instance-details.png#lightbox)

* + **Subscription**: Select the subscription you want to use from the dropdown.
  + **Resource Group**: This setting is autofilled when you select your virtual network on this page.
  + **Name**: Name your gateway. Naming your gateway not the same as naming a gateway subnet. It's the name of the gateway object you're creating.
  + **Region**: Select the region in which you want to create this resource. The region for the gateway must be the same as the virtual network.
  + **Gateway type**: Select **VPN**. VPN gateways use the virtual network gateway type **VPN**.
  + **VPN type**: Select the VPN type that is specified for your configuration. Most configurations require a Route-based VPN type.
  + **SKU**: Select the gateway SKU you want to use from the dropdown. The SKUs listed in the dropdown depend on the VPN type you select. Make sure to select a SKU that supports the features you want to use. For more information about gateway SKUs, see [Gateway SKUs](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsku).
  + **Generation**: Select the generation you want to use. For more information, see [Gateway SKUs](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku).
  + **Virtual network**: From the dropdown, select the virtual network to which you want to add this gateway. If you can't see the VNet for which you want to create a gateway, make sure you selected the correct subscription and region in the previous settings.
  + **Gateway subnet address range**: This field only appears if your VNet doesn't have a gateway subnet. It's best to specify /27 or larger (/26,/25 etc.). This allows enough IP addresses for future changes, such as adding an ExpressRoute gateway. We don't recommend creating a range any smaller than /28. If you already have a gateway subnet, you can view GatewaySubnet details by navigating to your virtual network. Select **Subnets** to view the range. If you want to change the range, you can delete and recreate the GatewaySubnet.

1. Specify in the values for **Public IP address**. These settings specify the public IP address object that gets associated to the VPN gateway. The public IP address is dynamically assigned to this object when the VPN gateway is created. The only time the Public IP address changes is when the gateway is deleted and re-created. It doesn't change across resizing, resetting, or other internal maintenance/upgrades of your VPN gateway.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-add-gw-pip-portal/pip-details.png#lightbox)

* + **Public IP address type**: In most cases, you want to use the Basic Public IP address type. If you don't see this field on the portal page, you may have selected a gateway SKU that pre-selects this value for you.
  + **Public IP address**: Leave **Create new** selected.
  + **Public IP address name**: In the text box, type a name for your public IP address instance.
  + **Public IP address SKU**: This field is controlled by the **Public IP Address Type** setting.
  + **Assignment**: VPN gateway supports only Dynamic.
  + **Enable active-active mode**: Only select **Enable active-active mode** if you're creating an active-active gateway configuration. Otherwise, leave this setting **Disabled**.
  + Leave **Configure BGP** as **Disabled**, unless your configuration specifically requires this setting. If you do require this setting, the default ASN is 65515, although this value can be changed.

1. Select **Review + create** to run validation.
2. Once validation passes, select **Create** to deploy the VPN gateway.

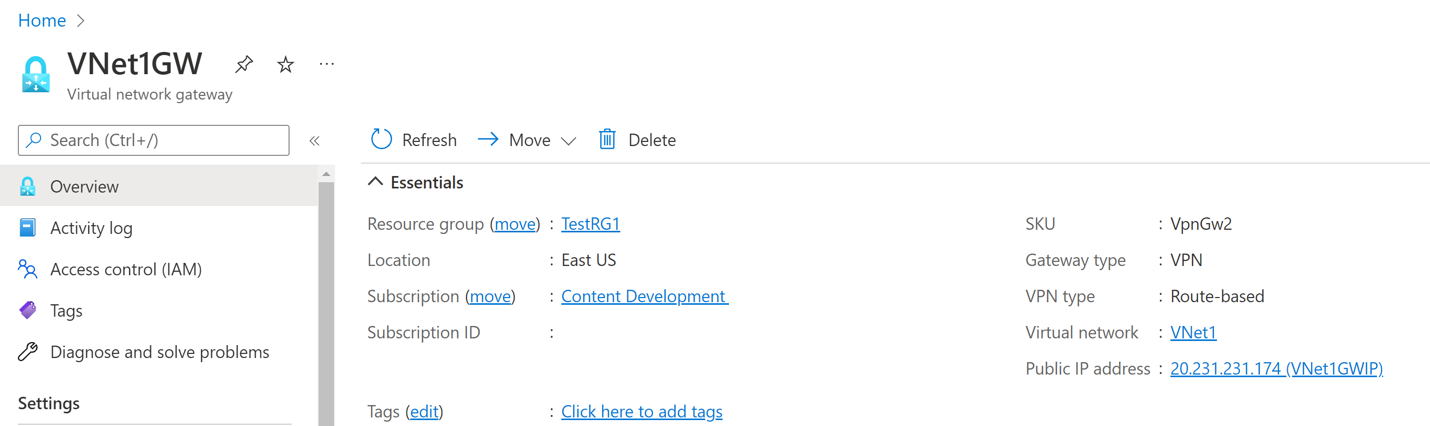
You can see the deployment status on the Overview page for your gateway. A gateway can take up to 45 minutes to fully create and deploy. After the gateway is created, you can view the IP address that has been assigned to it by looking at the virtual network in the portal. The gateway appears as a connected device.

**Important**

When working with gateway subnets, avoid associating a network security group (NSG) to the gateway subnet. Associating a network security group to this subnet may cause your virtual network gateway (VPN and Express Route gateways) to stop functioning as expected.

### View the public IP address

You can view the gateway public IP address on the **Overview** page for your gateway.

[](https://learn.microsoft.com/en-us/azure/vpn-gateway/media/tutorial-create-gateway-portal/address.png#lightbox)

To see additional information about the public IP address object, select the name/IP address link next to **Public IP address**.

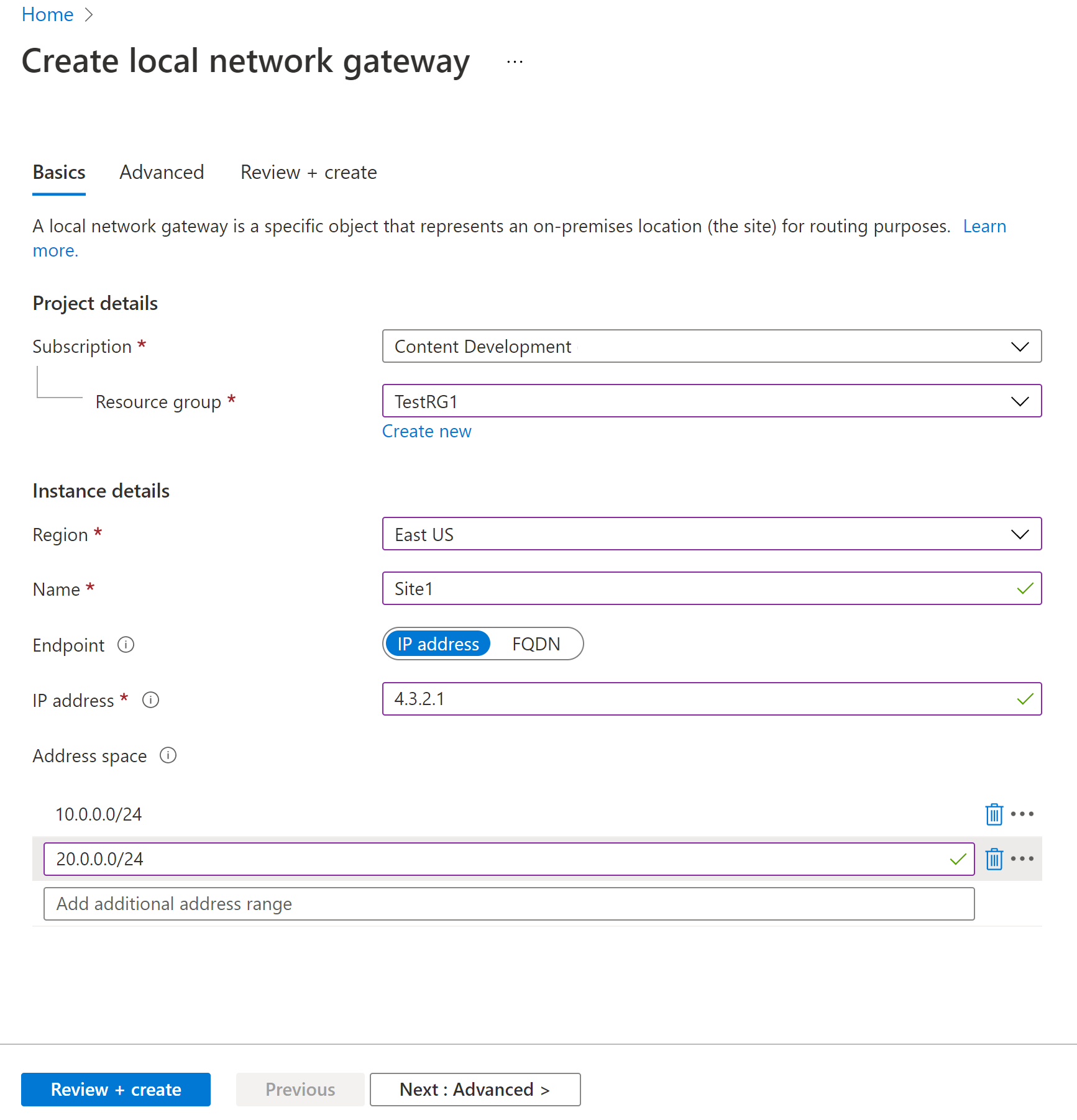
## Create a local network gateway

A local network gateway is a specific object representing your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you'll create a connection. You also specify the IP address prefixes routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. SMBC on-premises network changes or need to change the public IP address for the VPN device can easily update the values later.

Create a local network gateway using the following values:

* **Name:** Site1
* **Resource Group:** TestRG1
* **Location:** East US

1. From the [Azure portal](https://portal.azure.com/), in **Search resources, services, and docs (G+/)** type **local network gateway**. Locate **local network gateway** under **Marketplace** in the search results and select it. This opens the **Create local network gateway** page.
2. On the **Create local network gateway page**, on the **Basics** tab, specifiy the values for your local network gateway.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-add-local-network-gateway-portal-include/basics.png#lightbox)

* + **Subscription:** Verify that the correct subscription is showing.
  + **Resource Group:** Select the resource group that you want to use. You can either create a new resource group, or select one that you've already created.
  + **Region:** Select the region that this object will be created in. You may want to select the same location that your VNet resides in, but you aren't required to do so.
  + **Name:** Specify a name for your local network gateway object.
  + **Endpoint:** Select the endpoint type for the on-premises VPN device - **IP address** or **FQDN (Fully Qualified Domain Name)**.
    - **IP address**: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN device that you want Azure VPN gateway to connect to. If you don't have the IP address right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure won't be able to connect.
    - **FQDN**: If you have a dynamic public IP address that could change after certain period of time, often determined by your Internet service provider, you can use a constant DNS name with a Dynamic DNS service to point to your current public IP address of your VPN device. Your Azure VPN gateway will resolve the FQDN to determine the public IP address to connect to.
  + **Address Space** refers to the address ranges for the network that this local network represents. You can add multiple address space ranges. Make sure that the ranges you specify here don't overlap with ranges of other networks that you want to connect to. Azure will route the address range that you specify to the on-premises VPN device IP address. Use your own values here if you want to connect to your on-premises site, not the values shown in the example.

**Note**

* + Azure VPN supports only one IPv4 address for each FQDN. If the domain name resolves to multiple IP addresses, Azure VPN Gateway will use the first IP address returned by the DNS servers. To eliminate the uncertainty, we recommend that your FQDN always resolve to a single IPv4 address. IPv6 is not supported.
  + Azure VPN Gateway maintains a DNS cache refreshed every 5 minutes. The gateway tries to resolve the FQDNs for disconnected tunnels only. Resetting the gateway will also trigger FQDN resolution.

1. On the **Advanced** tab, you can configure BGP settings if needed.
2. When you have finished specifying the values, select **Review + create** at the bottom of the page to validate the page.
3. Select **Create** to create the local network gateway object.

## Configure your VPN device

Site-to-site connections to an on-premises network require a VPN device. In this step, you configure your VPN device. When configuring your VPN device, you need the following values:

* A shared key. This is the same shared key that you specify when creating your site-to-site VPN connection. In our examples, we use a basic shared key. We recommend that you generate a more complex key to use.
* The Public IP address of your virtual network gateway. You can view the public IP address by using the Azure portal, PowerShell, or CLI. To find the Public IP address of your VPN gateway using the Azure portal, go to **Virtual network gateways**, then select the name of your gateway.

**To download VPN device configuration scripts:**

Depending on the VPN device that you have, you may be able to download a VPN device configuration script. For more information, see [Download VPN device configuration scripts](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-download-vpndevicescript).

**See the following links for additional configuration information:**

* For information about compatible VPN devices, see [VPN Devices](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices).
* Before configuring your VPN device, check for any [Known device compatibility issues](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#known) for the VPN device that you want to use.
* For links to device configuration settings, see [Validated VPN Devices](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#devicetable). The device configuration links are provided on a best-effort basis. It's always best to check with your device manufacturer for the latest configuration information. The list shows the versions we've tested. If your OS isn't on that list, it's still possible that the version is compatible. Check with your device manufacturer to verify that OS version for your VPN device is compatible.
* For an overview of VPN device configuration, see [Overview of 3rd party VPN device configurations](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-3rdparty-device-config-overview).
* For information about editing device configuration samples, see [Editing samples](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#editing).
* For cryptographic requirements, see [About cryptographic requirements and Azure VPN gateways](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-compliance-crypto).
* For information about IPsec/IKE parameters, see [About VPN devices and IPsec/IKE parameters for site-to-site VPN gateway connections](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices#ipsec). This link shows information about IKE version, Diffie-Hellman Group, Authentication method, encryption and hashing algorithms, SA lifetime, PFS, and DPD, in addition to other parameter information that you need to complete your configuration.
* For IPsec/IKE policy configuration steps, see [Configure IPsec/IKE policy for S2S VPN or VNet-to-VNet connections](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-ipsecikepolicy-rm-powershell).
* To connect multiple policy-based VPN devices, see [Connect Azure VPN gateways to multiple on-premises policy-based VPN devices using PowerShell](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps).

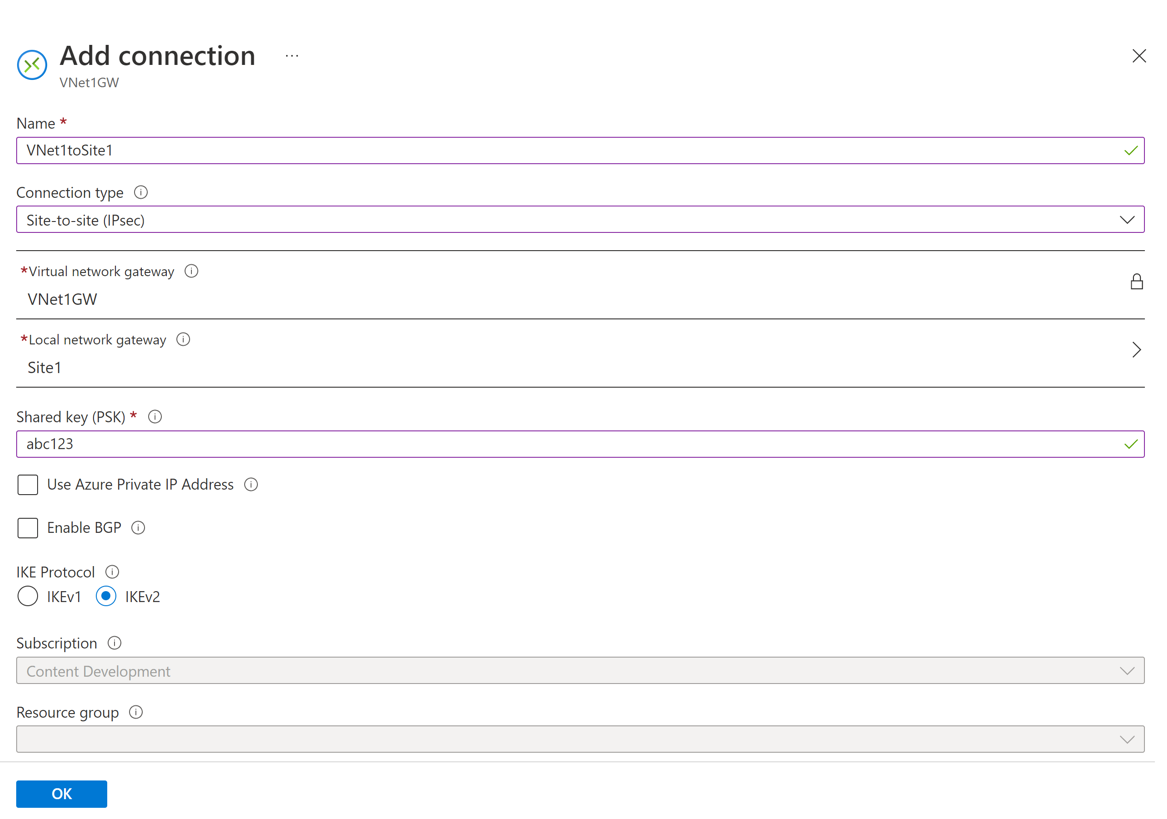
## Create VPN connections

Create a site-to-site VPN connection between your virtual network gateway and your on-premises VPN device.

Create a connection using the following values:

* **Local network gateway name:** Site1
* **Connection name:** VNet1toSite1
* **Shared key:** For this example, we use abc123. But, you can use whatever is compatible with your VPN hardware. The important thing is that the values match on both sides of the connection.

1. Go to your virtual network. On your VNet page, select **Connected devices** on the left. Locate your VPN gateway and click to open it.
2. On the page for the gateway, select **Connections**. At the top of the Connections page, select **+Add** to open the **Add connection** page.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-add-site-to-site-connection-portal-include/connection.png#lightbox)

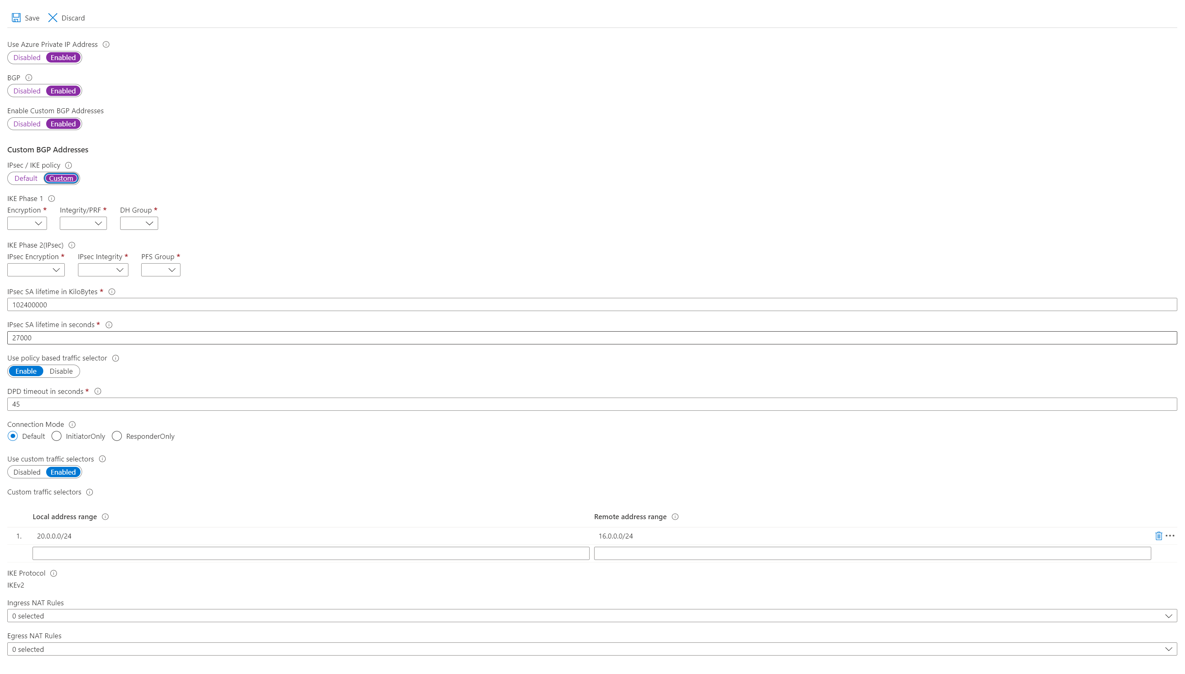
1. On the **Add connection** page, configure the values for your connection.
   * **Name:** Name your connection.
   * **Connection type:** Select **Site-to-site (IPSec)**.
   * **Virtual network gateway:** The value is fixed because you're connecting from this gateway.
   * **Local network gateway:** Select **Choose a local network gateway** and select the local network gateway that you want to use.
   * **Shared Key:** the value here must match the value that you're using for your local on-premises VPN device. The example uses 'abc123', but you can (and should) use something more complex. It's important that the value you specify here is the same value that you specify when configuring your VPN device.
   * Leave **Use Azure Private IP Address** unchecked.
   * Leave **Enable BGP** unchecked.
   * Select **IKEv2**.
2. Select **OK** to create your connection. You'll see Creating Connection flash on the screen.
3. You can view the connection in the **Connections** page of the virtual network gateway. The Status will go from Unknown to Connecting, and then to Succeeded.

### To configure additional connection settings (optional)

You can configure additional settings for your connection, if necessary. Otherwise, skip this section and leave the defaults in place.

1. Go to your virtual network gateway and select **Connections** to open the Connections page.
2. Select the name of the connection you want to configure to open the **Connection** page.
3. On the Connection page left side, select **Configuration** to open the Configuration page. Make any necessary changes, then **Save**.

In the following screenshot, we've enabled all the settings to show you the configuration settings available in the portal. Click the screenshot to see the expanded view. When you configure your connections, only configure the settings that you require. Otherwise, leave the default settings in place.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-connection-settings-portal-include/configuration.png#lightbox)

## Verify the VPN connection

In the Azure portal, you can view the connection status of a VPN gateway by navigating to the connection. The following steps show one way to navigate to your connection and verify.

1. In the [Azure portal](https://portal.azure.com/) menu, select **All resources** or search for and select **All resources** from any page.
2. Select to your virtual network gateway.
3. On the blade for your virtual network gateway, click **Connections**. You can see the status of each connection.
4. Click the name of the connection that you want to verify to open **Essentials**. In Essentials, you can view more information about your connection. The **Status** is 'Succeeded' and 'Connected' when you have made a successful connection.

## Connect to a virtual machine

You can connect to a VM that is deployed to your VNet by creating a Remote Desktop Connection to your VM. The best way to initially verify that you can connect to your VM is to connect by using its private IP address, rather than computer name. That way, you're testing to see if you can connect, not whether name resolution is configured properly.

1. Locate the private IP address. You can find the private IP address of a VM by either looking at the properties for the VM in the Azure portal, or by using PowerShell.
   * Azure portal - Locate your virtual machine in the Azure portal. View the properties for the VM. The private IP address is listed.
   * PowerShell - Use the example to view a list of VMs and private IP addresses from your resource groups. You don't need to modify this example before using it.

$VMs = Get-AzVM

$Nics = Get-AzNetworkInterface | Where VirtualMachine -ne $null

foreach($Nic in $Nics)

{

$VM = $VMs | Where-Object -Property Id -eq $Nic.VirtualMachine.Id

$Prv = $Nic.IpConfigurations | Select-Object -ExpandProperty PrivateIpAddress

$Alloc = $Nic.IpConfigurations | Select-Object -ExpandProperty PrivateIpAllocationMethod

Write-Output "$($VM.Name): $Prv,$Alloc"

}

1. Verify that you're connected to your VNet.
2. Open **Remote Desktop Connection** by typing "RDP" or "Remote Desktop Connection" in the search box on the taskbar, then select Remote Desktop Connection. You can also open Remote Desktop Connection using the 'mstsc' command in PowerShell.
3. In Remote Desktop Connection, enter the private IP address of the VM. "Show Options" to adjust additional settings, then connect.

**Troubleshoot a connection**

If you're having trouble connecting to a virtual machine over your VPN connection, check the following:

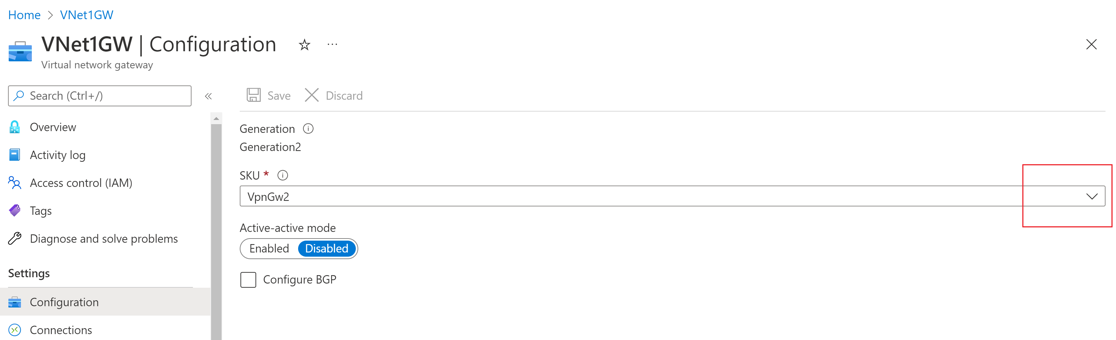
* Verify that your VPN connection is successful.
* Verify that you're connecting to the private IP address for the VM.
* If you can connect to the VM using the private IP address, but not the computer name, verify that you have configured DNS properly. For more information about how name resolution works for VMs, see [Name Resolution for VMs](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances).
* For more information about RDP connections, see [Troubleshoot Remote Desktop connections to a VM](https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-rdp-connection).

## Optional steps

### Resize a gateway SKU

There are specific rules regarding resizing vs. changing a gateway SKU. In this section, we'll resize the SKU. For more information, see [Gateway settings - resizing and changing SKUs](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#resizechange).

1. Go to the **Configuration** page for your virtual network gateway.
2. On the right side of the page, click the dropdown arrow to show the available gateway SKUs.

[](https://learn.microsoft.com/en-us/azure/includes/media/vpn-gateway-resize-portal/resize.png#lightbox)

1. Select the SKU from the dropdown.

### Reset a gateway

Resetting an Azure VPN gateway is helpful if you lose cross-premises VPN connectivity on one or more site-to-site VPN tunnels. In this situation, your on-premises VPN devices are all working correctly, but aren't able to establish IPsec tunnels with the Azure VPN gateways.

1. In the portal, go to the virtual network gateway that you want to reset.
2. On the **Virtual network gateway** page, in the left pane, scroll down to the **Support + Troubleshooting** section and select **Reset**.
3. On the **Reset** page, click **Reset**. Once the command is issued, the current active instance of the Azure VPN gateway is rebooted immediately. Resetting the gateway will cause a gap in VPN connectivity, and may limit future root cause analysis of the issue.

### Add another connection

You can create a connection to multiple on-premises sites from the same VPN gateway. If you want to configure multiple connections, the address spaces can’t overlap between any of the connections.

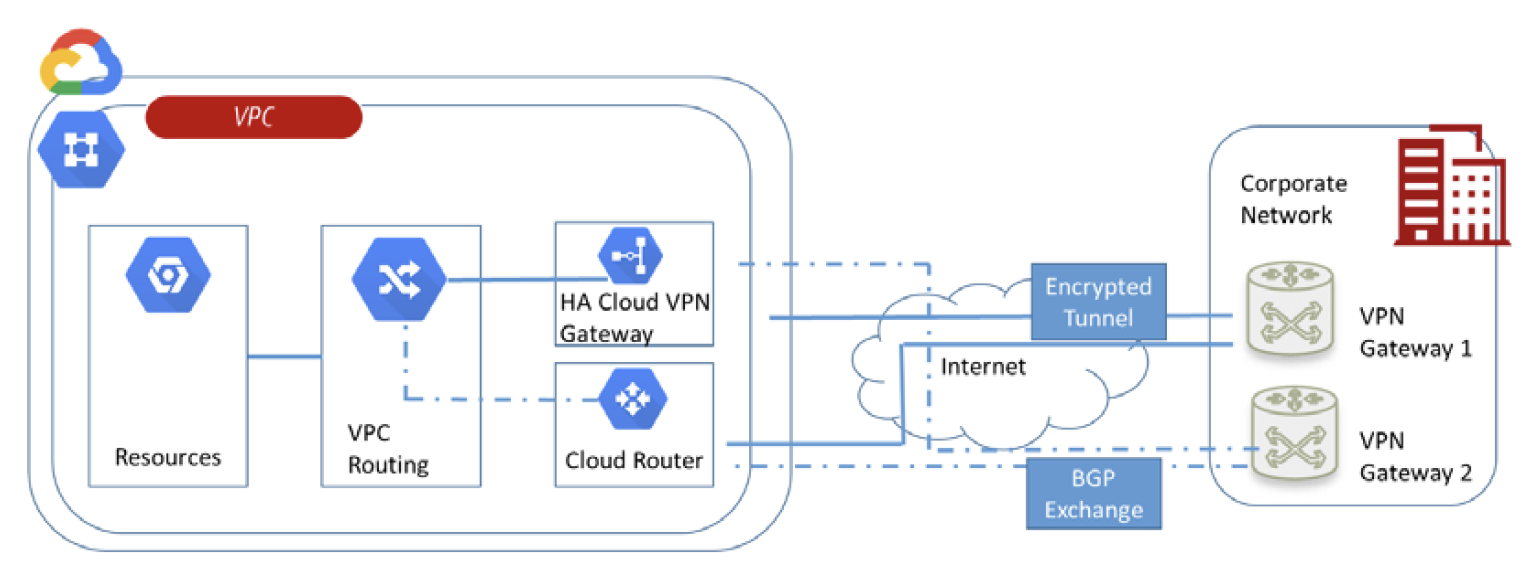
1. To add an additional connection, go to the VPN gateway, then select **Connections** to open the Connections page.
2. Select **+Add** to add your connection. Adjust the connection type to reflect either VNet-to-VNet (if connecting to another VNet gateway), or Site-to-site.
3. If you're connecting using Site-to-site and you haven't already created a local network gateway for the site you want to connect to, you can create a new one.
4. Specify the shared key that you want to use, then select **OK** to create the connection.

### Additional configuration considerations

S2S configurations can be customized in a variety of ways. For more information, see the following articles:

* For information about BGP, see the [BGP Overview](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview) and [How to configure BGP](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps).
* For information about forced tunneling, see [About forced tunneling](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm).
* For information about Highly Available Active-Active connections, see [Highly Available cross-premises and VNet-to-VNet connectivity](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable).
* For information about how to limit network traffic to resources in a virtual network, see [Network Security](https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview).
* For information about how Azure routes traffic between Azure, on-premises, and Internet resources, see [Virtual network traffic routing](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview).

# GCP VPN Design



Where HA VPN utilizes two interfaces, the Classic VPN gateway—the target VPN

gateway, as is referred to by Google—has only one with a single external IP address. One

major difference between the two setups is that with Classic VPN, you need to specify

forwarding rules in your GCP environment, whereas HA VPN takes care of that by

default. The following diagram shows the Classic VPN setup, including the routing table that is needed to direct traffic within the GCP environment:

Graphical user interface, diagram, application

Description automatically generated

Graphical user interface, application

Description automatically generated

# Global VPN Gateway Tunnel

Diagram

Description automatically generated

Graphical user interface, application

Description automatically generated

A picture containing timeline

Description automatically generated

Diagram

Description automatically generated