Best practices to set up networking for workloads migrated to Azure

12/04/2018 • 27 minutes to read • Contributors

In this article

As you plan and design for migration, in addition to the migration itself, one of the most critical steps is the design and implementation of Azure networking. This article describes best practices for networking when migrating to IaaS and PaaS implementations in Azure.

ⓘ **Important**

The best practices and opinions described in this article are based on the Azure platform and service features available at the time of writing. Features and capabilities change over time. Not all recommendations might be applicable for your deployment, so select those that work for you.

Design virtual networks

Azure provides virtual networks (VNets):

- Azure resources communicate privately, directly, and securely with each other over VNets.
- You can configure endpoint connections on VNets for VMs and services that require internet communication.
- A VNet is a logical isolation of the Azure cloud that's dedicated to your subscription.
- You can implement multiple VNets within each Azure subscription and Azure region.
- Each VNet is isolated from other VNets.

- VNets can contain private and public IP addresses defined in RFC 1918, expressed in CIDR notation. Public IP addresses specified in a VNet's address space are not directly accessible from the internet.
- VNets can connect to each other using VNet peering. Connected VNets can be in the same or different regions. Thus resources in one VNet can connect to resources in other VNets.
- By default, Azure routes traffic between subnets within a VNet, connected VNets, on-premises networks, and the internet.

When planning your VNet topology, you should consider how to arrange IP address spaces, how to implement a hub and spoke network, how to segment VNets into subnets, setting up DNS, and implementing Azure availability zones.

Best practice: Plan IP addressing

When you create VNets as part of your migration, it's important to plan out your VNet IP address space.

- You should assign an address space that isn't larger than a CIDR range of /16 for each VNet. VNets allow for the use of 65536 IP addresses, and assigning a smaller prefix than /16 would result in the loss of IP addresses. It's important not to waste IP addresses, even if they're in the private ranges defined by RFC 1918.
- The VNet address space shouldn't overlap with on-premises network ranges.
- Network Address Translation (NAT) shouldn't be used.
- Overlapping addresses can cause networks that can't be connected and routing that doesn't work properly. If networks overlap, you'll need to redesign the network or use network address translation (NAT).

Learn more:

- Get an overview of Azure VNets.
- Read the networking FAQ.
- Learn about networking limitations.

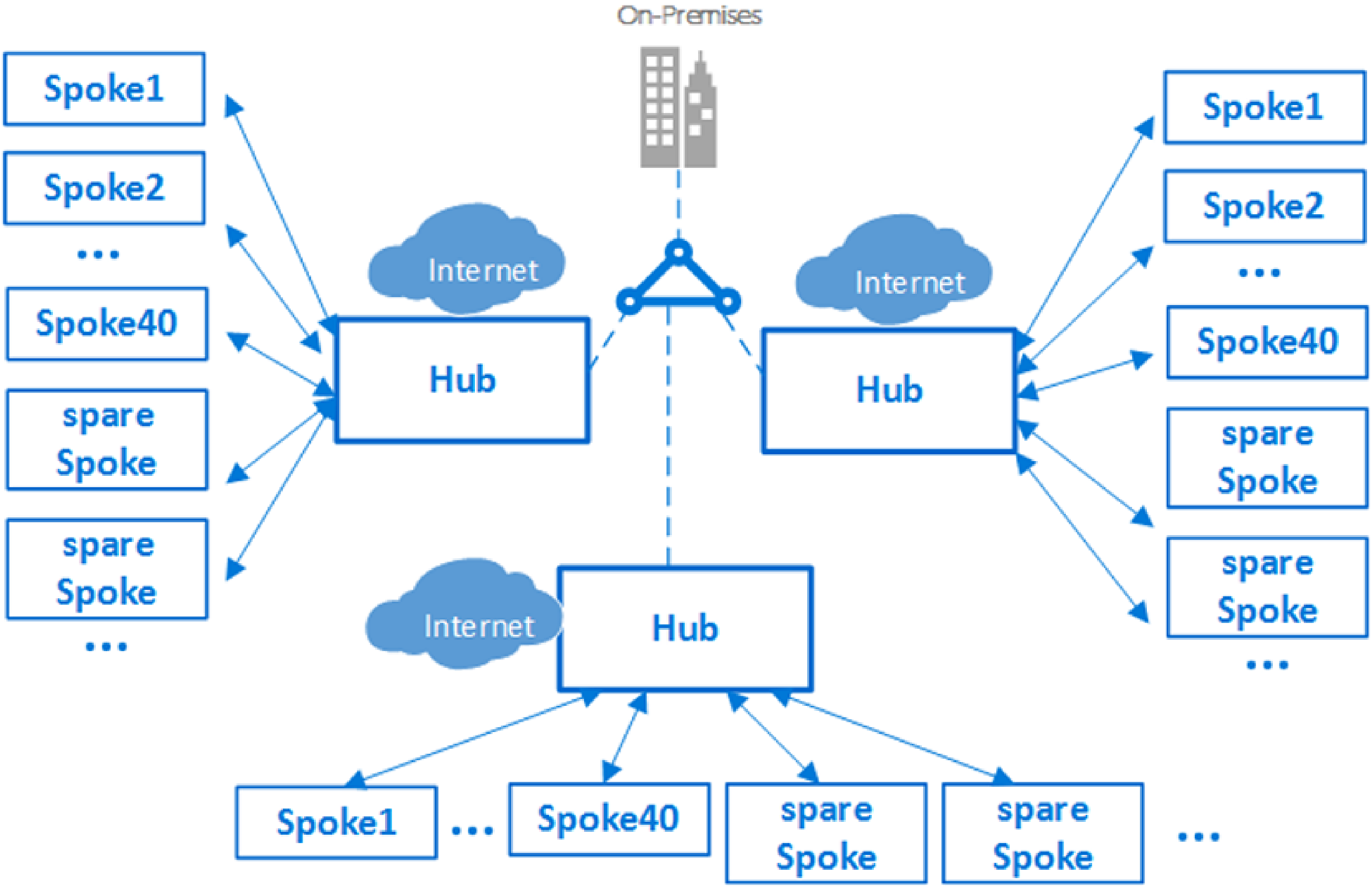
Best practice: Implement a hub and spoke network topology

A hub and spoke network topology isolates workloads while sharing services such as identity and security.

- The hub is an Azure VNet that acts as a central point of connectivity.
- The spokes are VNets that connect to the hub VNet using VNet peering.
- Shared services are deployed in the hub, while individual workloads are deployed as spokes.

Consider the following:

- Implementing a hub and spoke topology in Azure centralizes common services such as connections to on-premises networks, firewalls, and isolation between VNets. The hub VNet provides a central point of connectivity to on-premises networks, and a place to host services use by workloads hosted in spoke VNets.
- A hub and spoke configuration is typically used by larger enterprises. Smaller networks might consider a simpler design to save on costs and complexity.
- Spoke VNets can be used to isolate workloads, with each spoke managed separately from other spokes. Each workload can include multiple tiers, and multiple subnets that are connected with Azure load balancers.
- Hub and spoke VNets can be implemented in different resource groups, and even in different subscriptions. When you peer virtual networks in different subscriptions, the subscriptions can be associated to the same, or different, Azure Active Directory (Azure AD) tenants. This allows for decentralized management of each workload, while sharing services maintained in the hub network.



Hub and spoke topology

Learn more:

- Read about a hub and spoke topology.
- Get network recommendations for running Azure Windows and Linux VMs.
- Learn about VNet peering.

Best practice: Design subnets

To provide isolation within a VNet, you segment it into one or more subnets, and allocate a portion of the VNet's address space to each subnet.

- You can create multiple subnets within each VNet.
- By default, Azure routes network traffic between all subnets in a VNet.
- Your subnet decisions are based on your technical and organizational requirements.
- You create subnets using CIDR notation.
- When deciding on network range for subnets, it's important to note that Azure retains five IP addresses from each subnet that can't be used. For example, if you create the smallest available subnet of /29 (with eight IP addresses), Azure will retain five addresses, so you only have three usable addresses that can be assigned to hosts on the subnet.
- In most cases, using /28 as the smallest subnet is recommended.

Example:

The table shows an example of a VNet with an address space of 10.245.16.0/20 segmented into subnets, for a planned migration.

Subnet	CIDR	Addresses	Use
DEV-FE-EUS2	10.245.16.0/22	1019	Front-end/web tier VMs

Subnet	CIDR	Addresses	Use
DEV-APP-EUS2	10.245.20.0/22	1019	App-tier VMs
DEV-DB-EUS2	10.245.24.0/23	507	Database VMs

Learn more:

- Learn about designing subnets.
- Learn how a fictional company (Contoso) prepared their networking infrastructure for migration.

Best practice: Set up a DNS server

Azure adds a DNS server by default when you deploy a VNet. This allows you to rapidly build VNets and deploy resources. However, this DNS server only provides services to the resources on that VNet. If you want to connect multiple VNets together, or connect to an on-premises server from VNets, you need additional name resolution capabilities. For example, you might need Active Directory to resolve DNS names between virtual networks. To do this, you deploy your own custom DNS server in Azure.

- DNS servers in a VNet can forward DNS queries to the recursive resolvers in Azure. This enables you to resolve host names within that VNet. For example, a domain controller running in Azure can respond to DNS queries for its own domains, and forward all other queries to Azure.

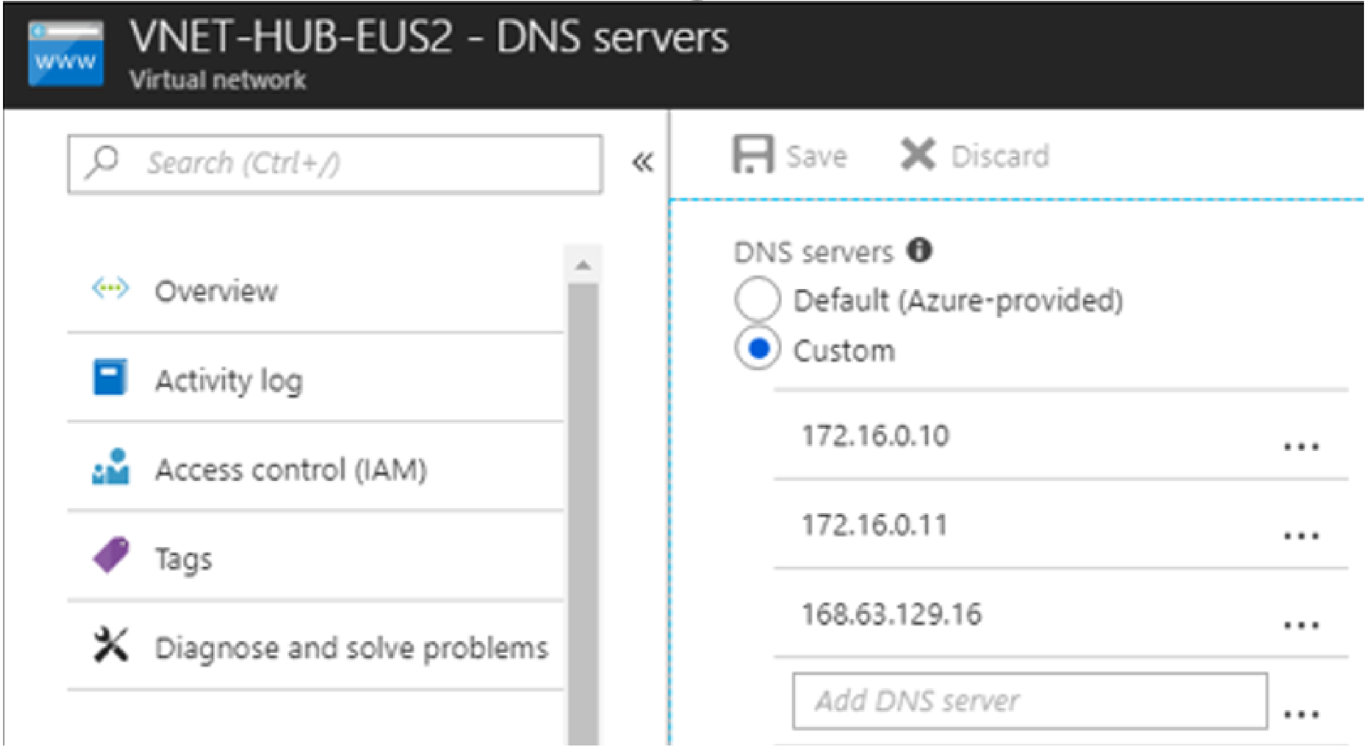
- DNS forwarding allows VMs to see both your on-premises resources (via the domain controller) and Azure-provided host names (using the forwarder). Access to the recursive resolvers in Azure is provided using the virtual IP address 168.63.129.16.

- DNS forwarding also enables DNS resolution between VNets, and allows on-premises machines to resolve host names provided by Azure.
  - To resolve a VM host name, the DNS server VM must reside in the same VNet, and be configured to forward host name queries to Azure.
  - Because the DNS suffix is different in each VNet, you can use conditional forwarding rules to send DNS queries to the correct VNet for resolution.

- When you use your own DNS servers, you can specify multiple DNS servers for each VNet. You can also specify multiple DNS servers per network interface (for Azure Resource Manager), or per cloud service (for the classic deployment model).

- DNS servers specified for a network interface or cloud service take precedence over DNS servers specified for the VNet.

- In the Azure Resource Manager deployment model, you can specify DNS servers for a VNet and a network interface, but the best practice is to use the setting only on VNets.



VNET-HUB-EUS2 - DNS servers

Virtual network

DNS servers

○ Default (Azure-provided)

● Custom

172.16.0.10

172.16.0.11

168.63.129.16

DNS servers for VNet

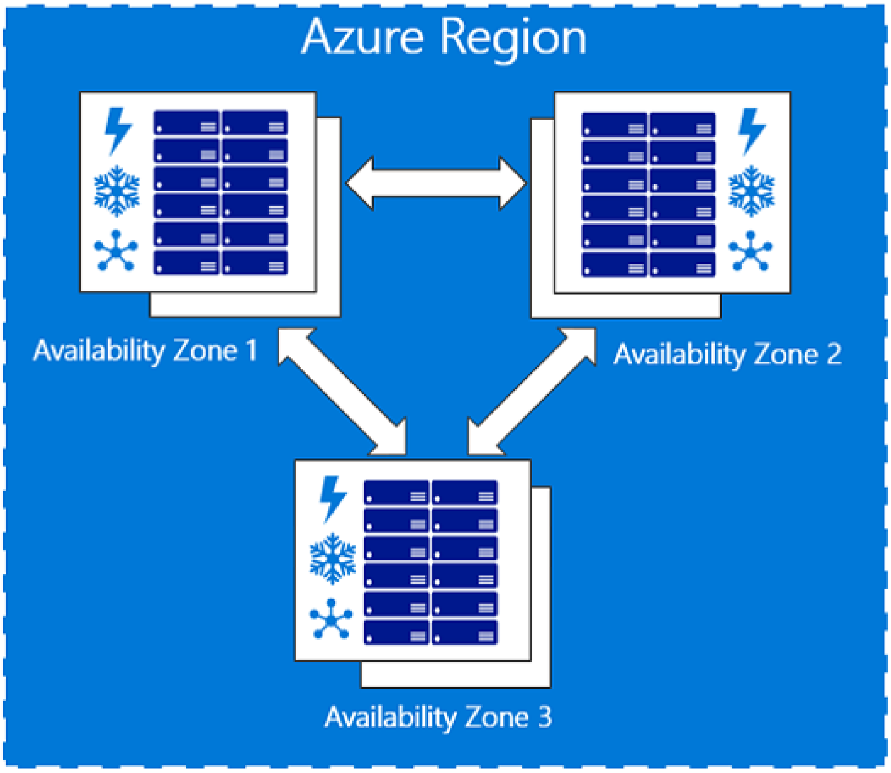
Learn more:

- Learn about name resolution when you use your own DNS server.
- Learn about DNS naming rules and restrictions.

Best practice: Set up availability zones

Availability zones increase high-availability to protect your apps and data from datacenter failures.

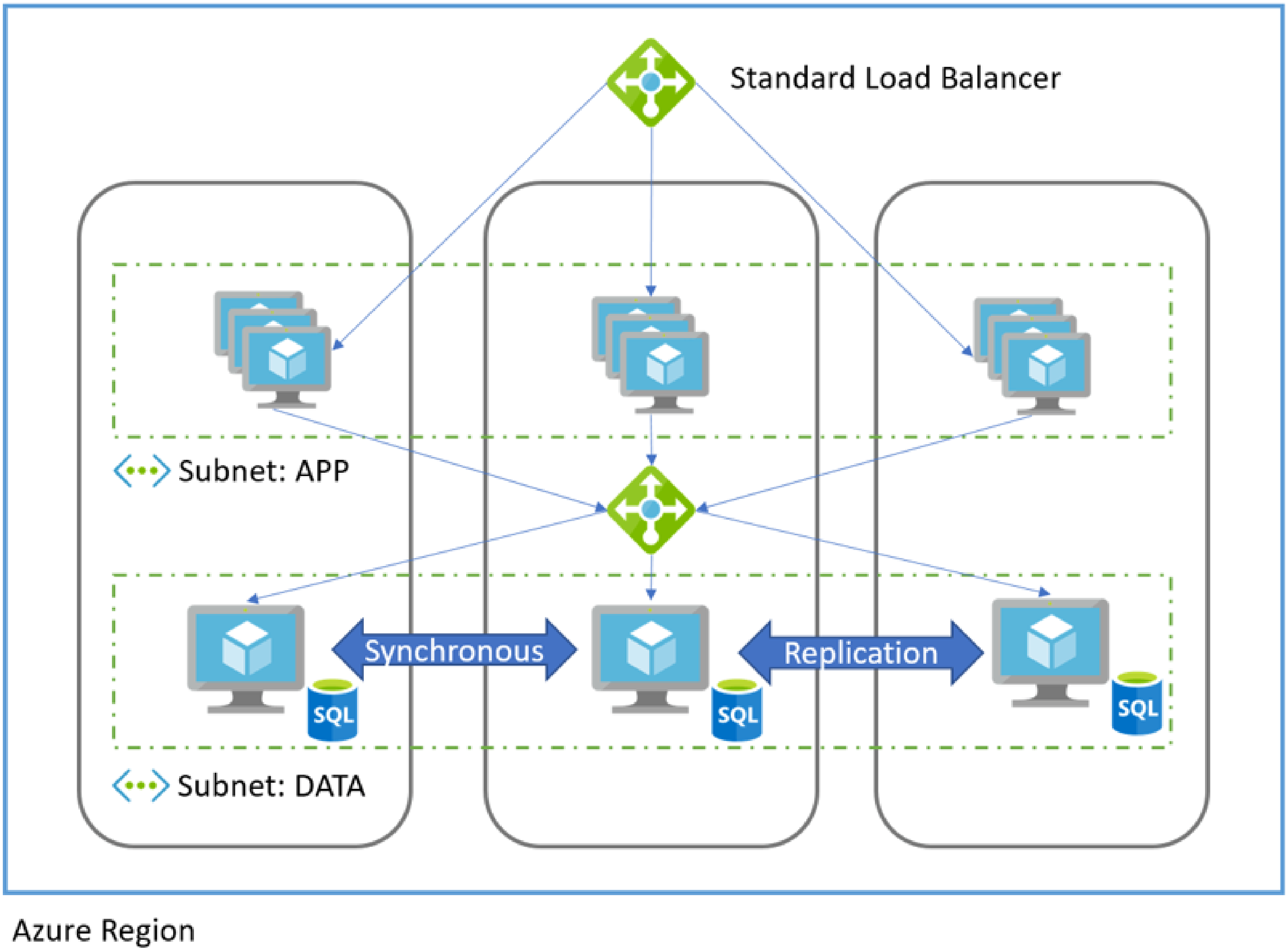
- Availability Zones are unique physical locations within an Azure region.
- Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.
- To ensure resiliency, there's a minimum of three separate zones in all enabled regions.
- The physical separation of availability zones within a region protects applications and data from datacenter failures.
- Zone-redundant services replicate your applications and data across availability zones to protect from single points of failure. - - With availability zones, Azure offers an SLA of 99.99% VM uptime.



Availability zone

- You can plan and build high-availability into your migration architecture by colocating compute, storage, networking, and data resources within a zone, and replicating them in other zones. Azure services that support availability zones fall into two categories:
    - Zonal services: You associate a resource with a specific zone. For example VMs, managed disks, IP addresses).
    - Zone-redundant services: The resource replicates automatically across zones. For example, zone-redundant storage, Azure SQL Database.

- You can deploy a standard Azure load balanced with internet-facing workloads or app tiers, to provide zonal fault tolerance.



Load balancer

Learn more:

- Get an overview of availability zones.

Design hybrid cloud networking

For a successful migration, it's critical to connect on-premises corporate networks to Azure. This creates an always-on connection known as a hybrid-cloud network, where services are provided from the Azure cloud to corporate users. There are two options for creating this type of network:

- **Site-to-site VPN:** You establish a site-to-site connection between your compatible on-premises VPN device and an Azure VPN gateway that's deployed in a VNet. Any authorized on-premises resource can access VNets. Site-to-site communications are sent through an encrypted tunnel over the internet.
- **Azure ExpressRoute:** You establish an Azure ExpressRoute connection between your on-premises network and Azure, through an ExpressRoute partner. This connection is private, and traffic doesn't go over the internet.

Learn more:

- Learn more about hybrid-cloud networking.

Best practice: Implement a highly available site-to-site VPN

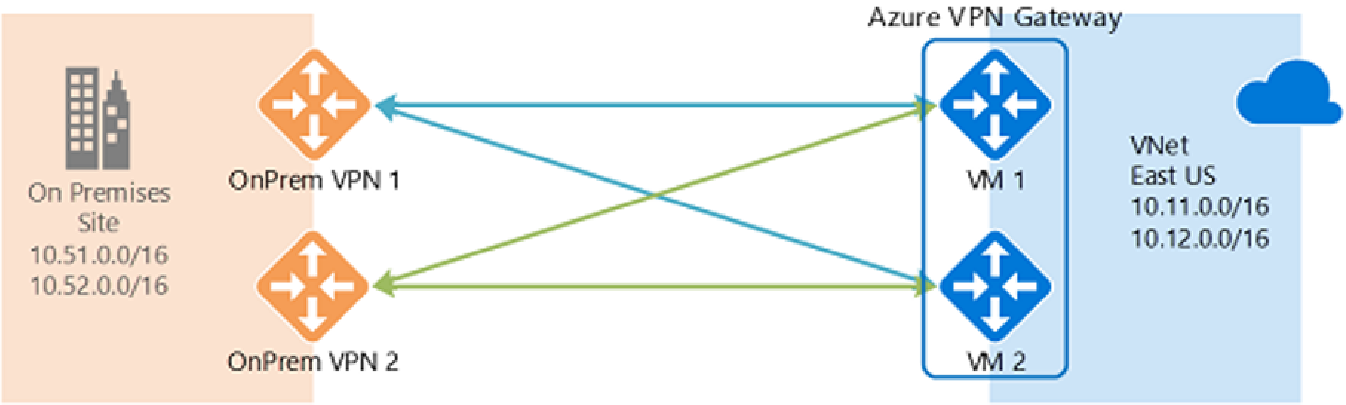
To implement a site-to-site VPN, you set up a VPN gateway in Azure.

- A VPN gateway is a specific type of VNet gateway that's used to send encrypted traffic between an Azure VNet and an on-premises location over the public Internet.
- You can also use a VPN gateway to send encrypted traffic between Azure VNets over the Microsoft network.
- Each VNet can have only one VPN gateway.

- You can create multiple connections to the same VPN gateway. When you create multiple connections, all VPN tunnels share the available gateway bandwidth.
- Every Azure VPN gateway consists of two instances in an active-standby configuration.
  - For planned maintenance or unplanned disruption to the active instance, failover occurs and the standby instance takes over automatically, and resumes the site-to-site or VNet-to-VNet connection.
  - The switchover causes a brief interruption.
  - For planned maintenance, connectivity should be restored within 10 to 15 seconds.
  - For unplanned issues, the connection recovery takes longer, about one to 1.5 minutes in the worst case.
  - Point-to-site (P2S) VPN client connections to the gateway will be disconnected, and the users will need to reconnect from client machines.

When setting up a site-to-site VPN, you do the following:

- You need a VNet whose address range doesn't overlap with the on-premises network to which the VPN will connect.
- You create a gateway subnet in the network.
- You create a VPN gateway, specify the gateway type (VPN) and whether the gateway is policy-based or route-based. A RouteBased VPN is recommended as more capable and future-proof.
- You create a local network gateway on-premises, and configure your on-premises VPN device.
- You create a failover site-to-site VPN connection between the VNet gateway and the on-premises device. Using route-based VPN allows for either active-passive or active-active connections to Azure. Route-based also supports both site-to-site (from any computer) and point-to-site (from a single computer) connections concurrently.
- You specify the gateway SKU that you want to use. This will depend on your workload requirements, throughputs, features, and SLAs.
- Border gateway protocol (BGP) is an optional feature you can use with Azure ExpressRoute and route-based VPN gateways to propagate your on-premises BGP routes to your VNets.



Site-to-site VPN

Learn more:

- Review compatible on-premises VPN devices.
- Get an overview of VPN gateways.
- Learn about highly available VPN connections.
- Learn about planning and designing a VPN gateway.
- Review VPN gateway settings.
- Review gateway SKUs.
- Read about setting up BGP with Azure VPN gateways.

Best practice: Configure a gateway for VPN Gateways

When you create a VPN gateway in Azure, you must use a special subnet named GatewaySubnet. When creating this subnet note these best practices:

- The prefix length of the gateway subnet can have a maximum prefix length of 29 (for example, 10.119.255.248/29). The current recommendation is that you use a prefix length of 27 (for example, 10.119.255.224/27).
- When you define the address space of the gateway subnet, use the very last part of the VNet address space.
- When using the Azure GatewaySubnet, never deploy any VMs or other devices such as Application Gateway to the gateway subnet.
- Don't assign a network security group (NSG) to this subnet. It will cause the gateway to stop functioning.

Learn more:

- Use this tool to determine your IP address space.

Best practice: Implement Azure Virtual WAN for branch offices

For multiple VPN connections, Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch connectivity through Azure.

- Virtual WAN allows you to connect and configure branch devices to communicate with Azure. This can be done manually, or by using preferred provider devices through a Virtual WAN partner.
- Using preferred provider devices allows for simple use, connectivity, and configuration management.
- The Azure WAN built-in dashboard provides instant troubleshooting insights that save time, and provide an easy way to track large-scale site-to-site connectivity.

Learn more: Learn about Azure Virtual WAN.

Best practice: Implement ExpressRoute for mission-critical connections

The Azure ExpressRoute service extends your on-premises infrastructure into the Microsoft cloud by creating private connections between the virtual Azure datacenter and on-premises networks.

- ExpressRoute connections can be over an any-to-any (IP VPN) network, a point-to-point Ethernet network, or through a connectivity provider. They don't go over the public internet.
- ExpressRoute connections offer higher security, reliability, and higher speeds (up to 10 Gbps), along with consistent latency.
- ExpressRoute is useful for virtual datacenters, as customers can get the benefits of compliance rules associated with private connections.
- With ExpressRoute Direct you can connect directly to Microsoft routers at 100Gbps, for larger bandwidth needs.
- ExpressRoute uses BGP to exchange routes between on-premises networks, Azure instances, and Microsoft public addresses.

Deploying ExpressRoute connections usually involves engaging with an ExpressRoute service provider. For a quick start, it's common to initially use a site-to-site VPN to establish connectivity between the virtual datacenter and on-premises resources, and then migrate to an ExpressRoute connection when a physical interconnection with your service provider is established.

Learn more:

- Read an overview of ExpressRoute.
- Learn about ExpressRoute Direct.

Best practice: Optimize ExpressRoute routing with BGP communities

When you have multiple ExpressRoute circuits, you have more than one path to connect to Microsoft. As a result, suboptimal routing can happen and your traffic might take a longer path to reach Microsoft, and Microsoft to your network. The longer the network path,the higher the latency. Latency has direct impact on app performance and user experience.

Example:

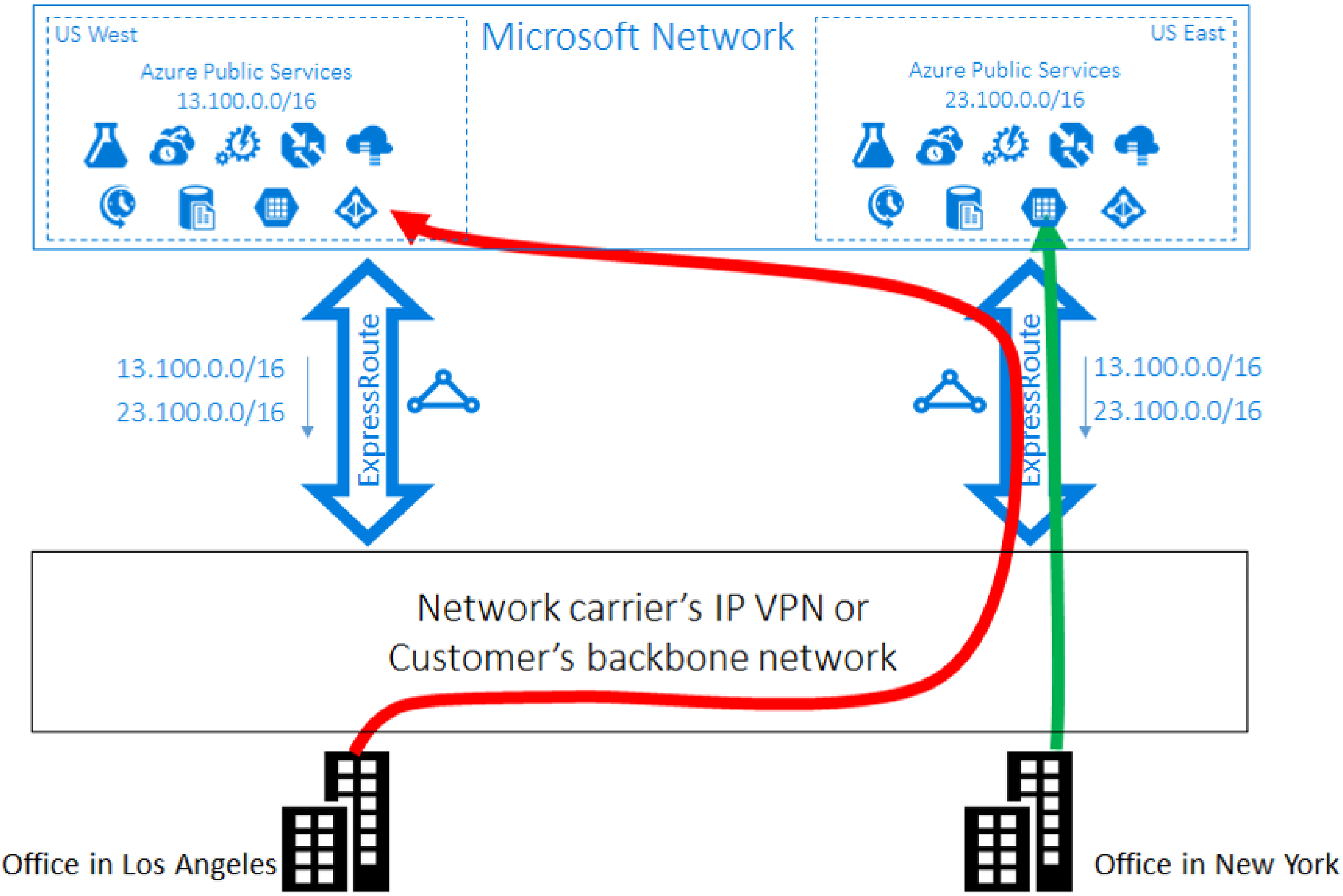
Let's review an example:

- You have two offices in the US, one in Los Angeles and one in New York.
- Your offices are connected on a WAN, which can be either your own backbone network or your service provider's IP VPN.
- You have two ExpressRoute circuits, one in US West and one in US East, that are also connected on the WAN. Obviously, you have two paths to connect to the Microsoft network.

Problem:

Now imagine you have an Azure deployment (for example, Azure App Service) in both US West and US East.

- You want users in each office to access their nearest Azure services for an optimal experience.
- Thus you want to connect users in Los Angeles to Azure US West and users in New York to Azure US East.
- This works for east coast users, but not for the west. The problem is as follows:
    - On each ExpressRoute circuit, we advertise both prefixes in Azure US East (23.100.0.0/16) and Azure US West (13.100.0.0/16).
    - Without knowing which prefix is from which region, prefixes aren't treated differently.
    - Your WAN network can assume that both prefixes are closer to US East than US West, and thus route users from both offices to the ExpressRoute circuit in US East, providing a suboptimal experience for users in the Los Angeles office.

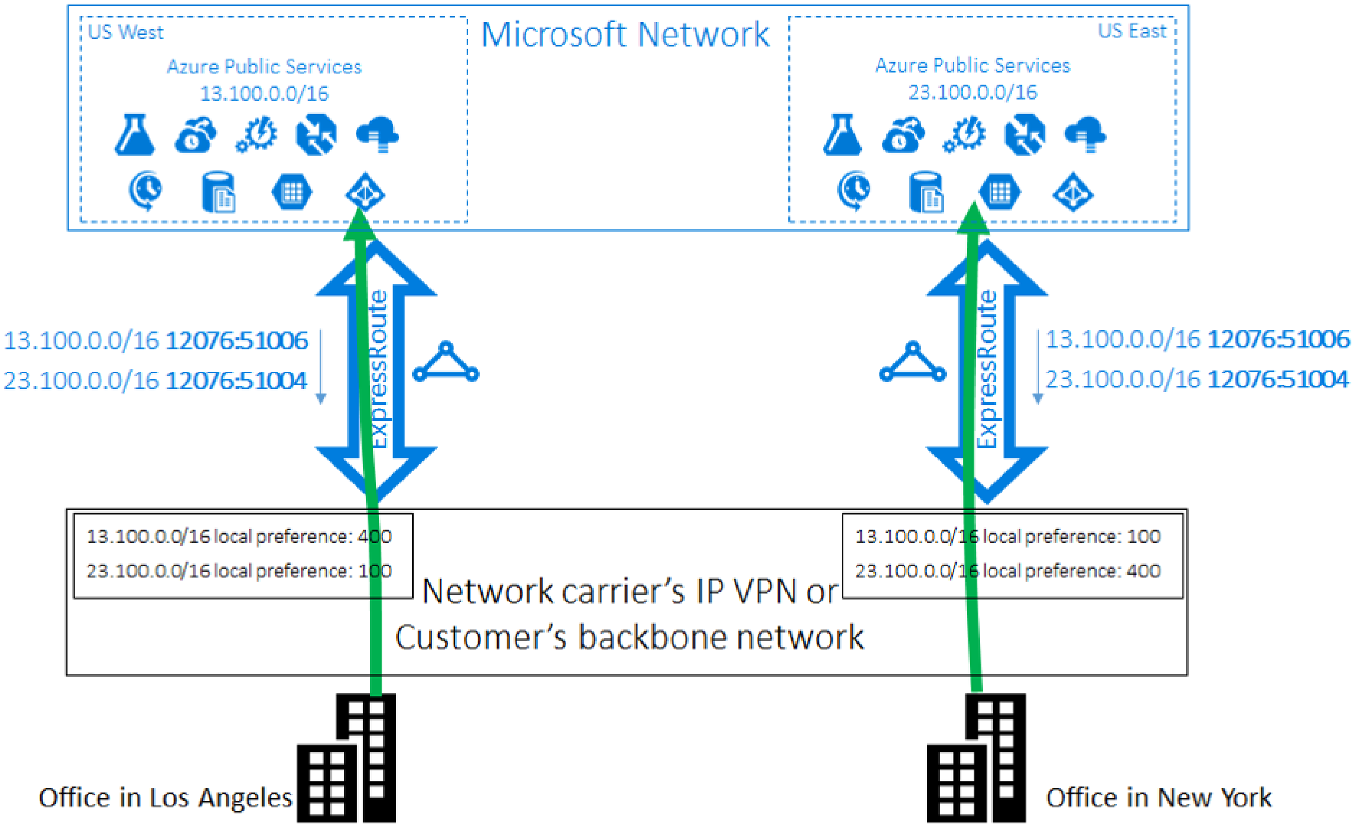


BGP communities unoptimized connection

Solution:

To optimize routing for both office users, you need to know which prefix is from Azure US West and which is from Azure US East. You can encode this information by using BGP community values.

- You assign a unique BGP community value to each Azure region. For example, 12076:51004 for US East; 12076:51006 for US West.
- Now that it's clear which prefix belongs to which Azure region, you can configure a preferred ExpressRoute circuit.
- Because you're using BGP to exchange routing information, you can use BGP's local preference to influence routing.
- In our example, you assign a higher local preference value to 13.100.0.0/16 in US West than in US East, and similarly, a higher local preference value to 23.100.0.0/16 in US East than in US West.
- This configuration ensures that when both paths to Microsoft are available, users in Los Angeles will connect to Azure US West using the west circuit, and users New York connect to Azure US East using the east circuit. Routing is optimized on both sides.



BGP communities optimized connection

Learn more:

- Learn about optimizing routing.

Securing VNets

The responsibility for securing VNets is shared between Microsoft and you. Microsoft provides many networking features, as well as services that help keep resources secure. When designing security for VNets, best practices you should follow include implementing a perimeter network, using filtering and security groups, securing access to resources and IP addresses, and implementing attack protection.

Learn more:

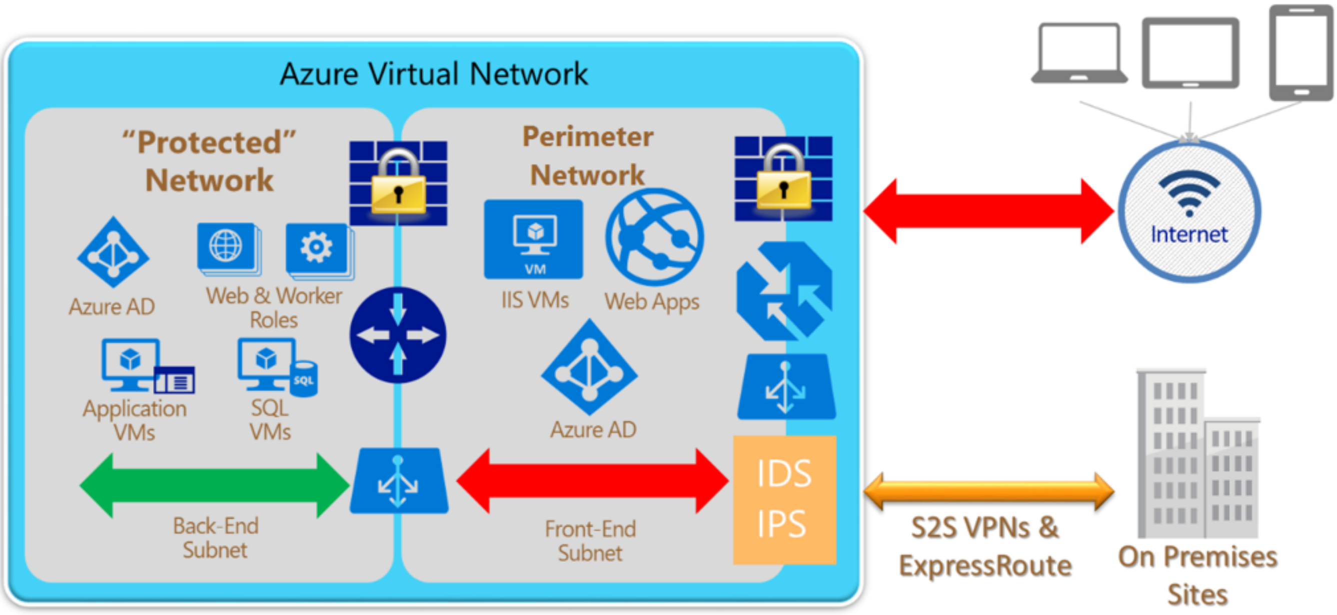
- Get an overview of best practices for network security.
- Learn how to design for secure networks.

Best practice: Implement an Azure perimeter network

Although Microsoft invests heavily in protecting the cloud infrastructure, you must also protect your cloud services and resource groups. A multilayered approach to security provides the best defense. Putting a perimeter network in place is an important part of that defense strategy.

- A perimeter network protects internal network resources from an untrusted network.
- It's the outermost layer that's exposed to the internet. It generally sits between the internet and the enterprise infrastructure, usually with some form of protection on both sides.
- In a typical enterprise network topology, the core infrastructure is heavily fortified at the perimeters, with multiple layers of security devices. The boundary of each layer consists of devices and policy enforcement points.
- Each layer can include a combination of the network security solutions that include firewalls, Denial of Service (DoS) prevention, intrusion detection/intrusion protection systems (IDS/IPS), and VPN devices.
- Policy enforcement on the perimeter network can use firewall policies, access control lists (ACLs), or specific routing.
- As incoming traffic arrives from the internet, it's intercepted and handled by a combination of defense solution to block attacks and harmful traffic, while allowing legitimate requests into the network.
- Incoming traffic can route directly to resources in the perimeter network. The perimeter network resource can then communicate with other resources deeper in the network, moving traffic forward into the network after validation.

The following figure shows an example of a single subnet perimeter network in a corporate network, with two security boundaries.



Perimeter network deployment

Learn more:

- Learn about deploying a perimeter network between Azure and your on-premises datacenter.

Best practice: Filter VNet traffic with NSGs

Network security groups (NSG) contain multiple inbound and outbound security rules that filter traffic going to and from resources. Filtering can be by source and destination IP address, port, and protocol.

- NSGs contain security rules that allow or deny inbound network traffic to (or outbound network traffic from) several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.
- NSG rules are evaluated by priority using five-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic.

- A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record.
- A flow record allows an NSG to be stateful. For example, if you specify an outbound security rule to any address over port 80, you don't need an inbound security rule to respond to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally.
- The opposite is also true. If inbound traffic is allowed over a port, you don't need to specify an outbound security rule to respond to traffic over the port.
- Existing connections aren't interrupted when you remove a security rule that enabled the flow. Traffic flows are interrupted when connections are stopped, and no traffic is flowing in either direction, for at least a few minutes.
- When creating NSGs, create as few as possible but as many that are necessary.

Best practice: Secure north/south and east/west traffic

When securing VNets, it's important to consider attack vectors.

- Using only subnet NSGs simplifies your environment, but only secures traffic into your subnet. This is known as north/south traffic.
- Traffic between VMs on the same subnet is known as east/west traffic.
- It's important to use both forms of protection, so that if a hacker gains access from the outside they'll be stopped when trying to attach machines located in the same subnet.

Use service tags on NSGs

A service tag represents a group of IP address prefixes. Using a service tag helps minimize complexity when you create NSG rules.

- You can use service tags instead of specific IP addresses when you create rules.
- Microsoft manages the address prefixes associated with a service tag, and automatically updates the service tag as addresses change.
- You can't create your own service tag, or specify which IP addresses are included within a tag.

Service tags take the manual work out of assigning a rule to groups of Azure services. For example, if you want to allow a VNet subnet containing web servers access to an Azure SQL Database, you could create an outbound rule to port 1433, and use the **Sql** service tag.

- This **Sql** tag denotes the address prefixes of the Azure SQL Database and Azure SQL Data Warehouse services.
- If you specify **Sql** as the value, traffic is allowed or denied to Sql.
- If you only want to allow access to **Sql** in a specific region, you can specify that region. For example, if you want to allow access only to Azure SQL Database in the East US region, you can specify **Sql.EastUS** as a service tag.
- The tag represents the service, but not specific instances of the service. For example, the tag represents the Azure SQL Database service, but doesn't represent a particular SQL database or server.
- All address prefixes represented by this tag are also represented by the **Internet** tag.

Learn more:

- Read about NSGs.
- Review the service tags available for NSGs.

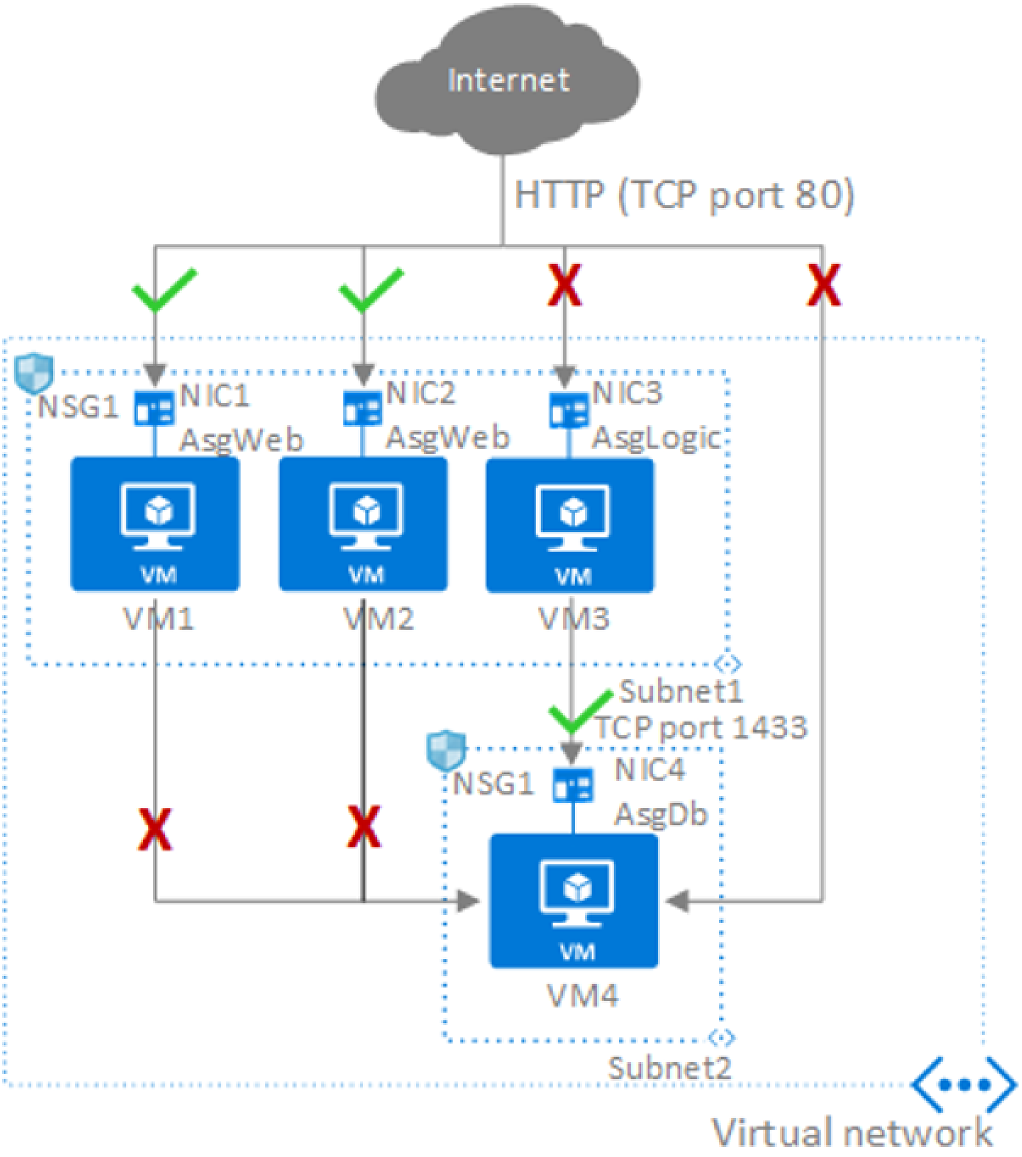
Best practice: Use application security groups

Application security groups enable you to configure network security as a natural extension of an app structure.

- You can group VMs and define network security policies based on application security groups.
- Application security groups enable you to reuse your security policy at scale without manual maintenance of explicit IP addresses.

- Application security groups handle the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

Example:



Application security group example

Network interface	Application security group
NIC1	AsgWeb
NIC2	AsgWeb
NIC3	AsgLogic
NIC4	AsgDb

- In our example, each network interface belongs to only one application security group, but in fact an interface can belong to multiple groups, in accordance with Azure limits.
- None of the network interfaces have an associated NSG. NSG1 is associated to both subnets and contains the following rules.

Copy

```
**Rule name** | **Purpose** | **Details**
--- | --- | ---
Allow-HTTP-Inbound-Internet | Allow traffic from the internet to the web servers. Inbound traf-
fic from the internet is denied by the DenyAllInbound default security rule, so no additional
```

```
rule is needed for the AsgLogic or AsgDb application security groups. | Priority: 100<br/><br/>
Source: internet<br/><br/> Source port: *<br/><br/> Destination: AsgWeb<br/><br/> Destination
port: 80<br/><br/> Protocol: TCP<br/><br/> Access: Allow.
Deny-Database-All | AllowVNetInBound default security rule allows all communication between re-
sources in the same VNet, this rule is needed to deny traffic from all resources. | Priority:
120<br/><br/> Source: *<br/><br/> Source port: *<br/><br/> Destination: AsgDb<br/><br/> Desti-
nation port: 1433<br/><br/> Protocol: All<br/><br/> Access: Deny.
Allow-Database-BusinessLogic | Allow traffic from the AsgLogic application security group to
the AsgDb application security group. The priority for this rule is higher than the Deny-Data-
base-All rule, and is processed before that rule, so traffic from the AsgLogic application se-
curity group is allowed, and all other traffic is blocked. | Priority: 110<br/><br/> Source:
AsgLogic<br/><br/> Source port: *<br/><br/> Destination: AsgDb<br/><br/> Destination port:
1433<br/><br/> Protocol: TCP<br/><br/> Access: Allow.
```

- The rules that specify an application security group as the source or destination are only applied to the network interfaces that are members of the application security group. If the network interface is not a member of an application security group, the rule is not applied to the network interface, even though the network security group is associated to the subnet.

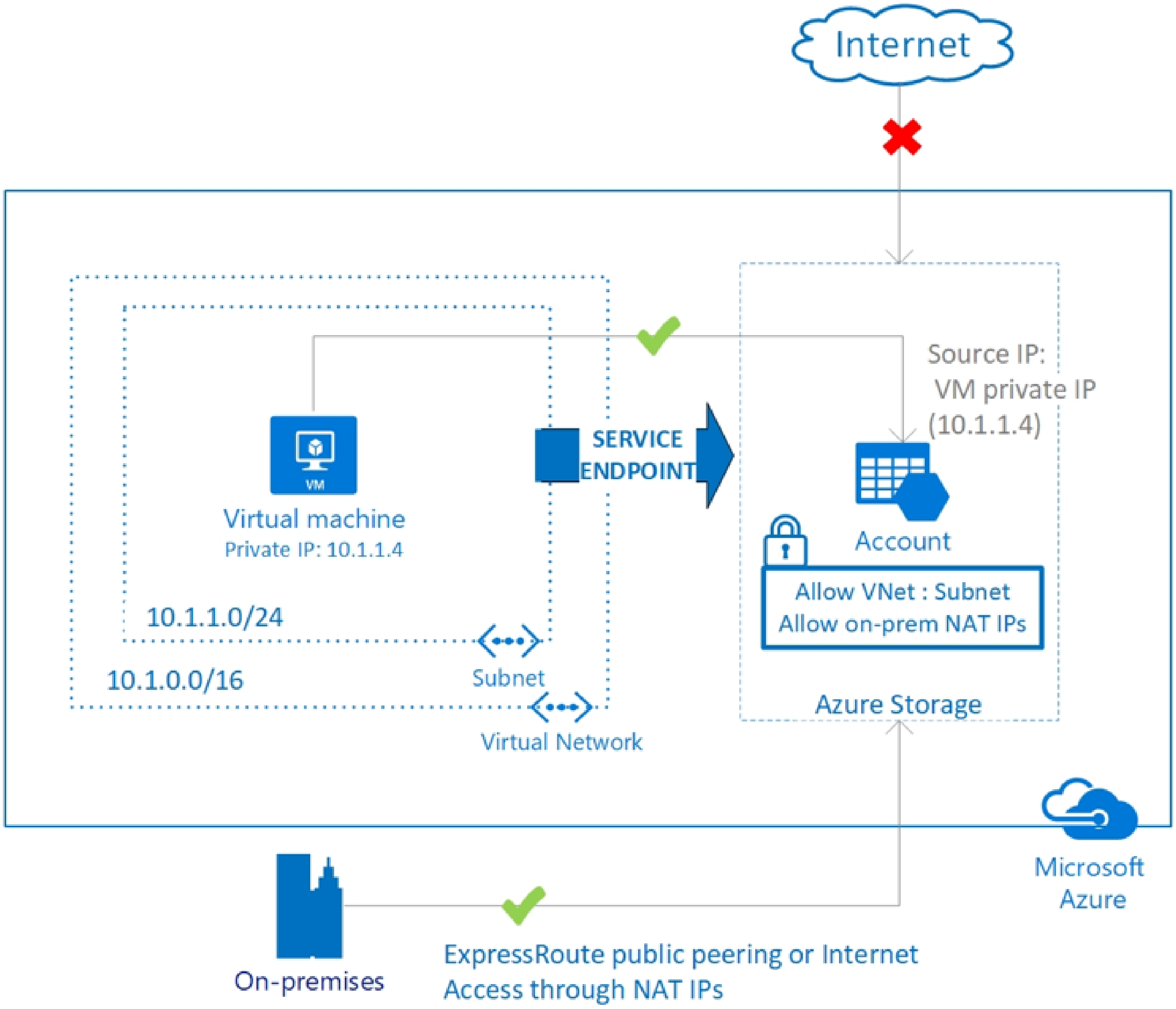
Learn more:

- Learn about application security groups.

Best practice: Secure access to PaaS using VNet service endpoints

VNet service endpoints extend your VNet private address space and identity to Azure services over a direct connection.

- Endpoints allow you to secure critical Azure service resources to your VNets only. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.
- VNet private address space can be overlapping and thus cannot be used to uniquely identify traffic originating from a VNet.
- After service endpoints are enabled in your VNet, you can secure Azure service resources by adding a VNet rule to the service resources. This provides improved security by fully removing public internet access to resources, and allowing traffic only from your VNet.



Service endpoints

Learn more:

- Learn about VNet service endpoints.

Best practice: Control public IP addresses

Public IP addresses in Azure can be associated with VMs, load balancers, application gateways, and VPN gateways.

- Public IP addresses allow internet resources to communicate inbound to Azure resources, and Azure resources to communicate outbound to the internet.
- Public IP addresses are created with a basic or standard SKU, which have several differences. Standard SKUs can be assigned to any service, but are most usually configured on VMs, load balancers, and application gateways.
- It's important to note that a basic public IP address doesn't have an NSG automatically configured. You need to configure your own and assign rules to control access. Standard SKU IP addresses have an NSG and rules assigned by default.
- As a best practice, VMs shouldn't be configured with a public IP address.
  - If you need a port opened, it should only be for web services such as port 80 or 443.
  - Standard remote management ports such as SSH (22) and RDP (3389) should be set to deny, along with all other ports, using NSGs.
- A better practice is to put VMs behind an Azure load balancer or application gateway. Then if access to remote management ports is needed, you can use just-in-time VM access in the Azure Security Center.

Learn more:

- Learn about public IP addresses in Azure.

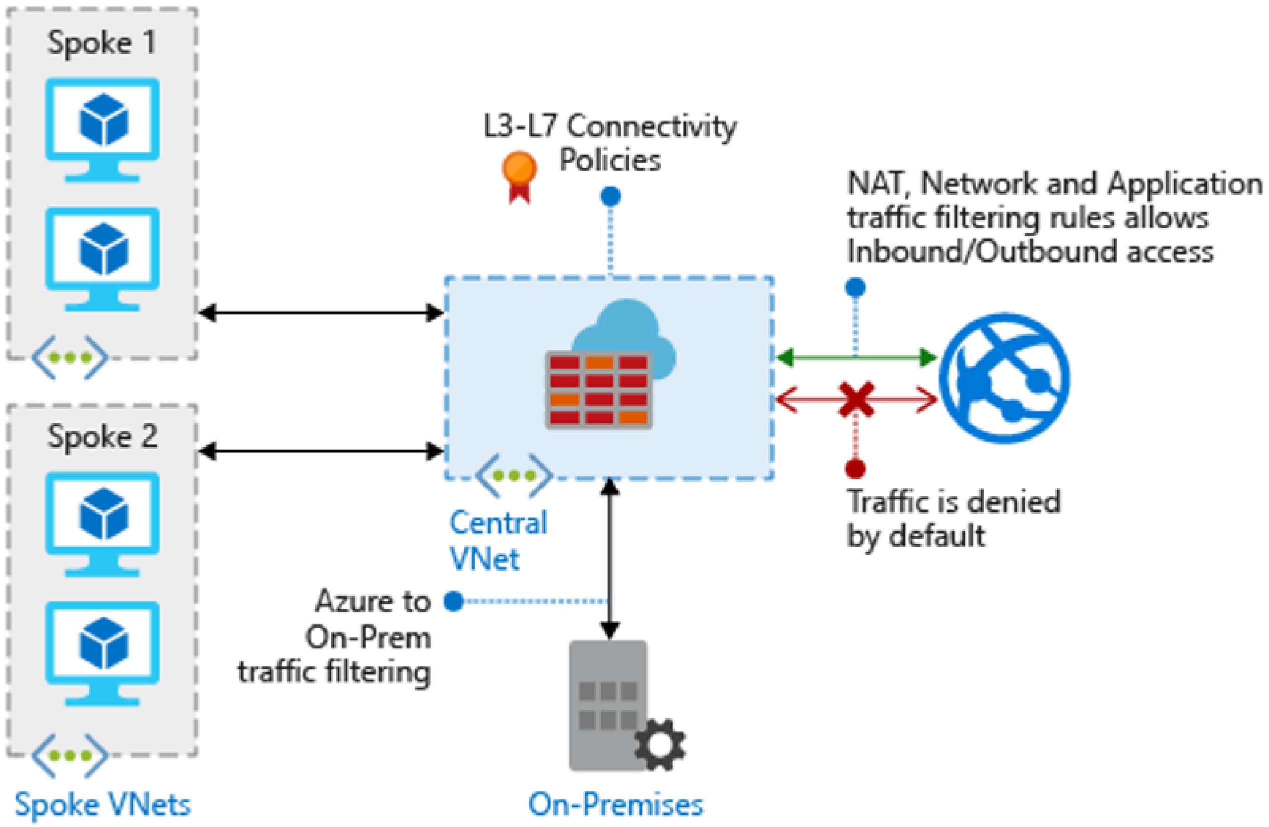
- Read more on just-in-time VM access in the Azure Security Center.

Take advantage of Azure security features for networking

Azure has platform security features that are easy to use, and provide rich countermeasures to common network attacks. These include Azure Firewall, web application firewall, and Network Watcher.

Best Practice: Deploy Azure Firewall

Azure Firewall is a managed cloud-based network security service that protects your VNet resources. It is a fully stateful managed firewall with built-in high availability and unrestricted cloud scalability.


Spoke 1
Spoke 2
Spoke VNets
L3-L7 Connectivity Policies
NAT, Network and Application traffic filtering rules allows Inbound/Outbound access
Traffic is denied by default
Central VNet
Azure to On-Prem traffic filtering
On-Premises

Azure Firewall

- Azure Firewall can centrally create, enforce, and log application and network connectivity policies across subscriptions and VNets.
- Azure Firewall uses a static public IP address for your VNet resources, allowing outside firewalls to identify traffic originating from your VNet.
- Azure Firewall is fully integrated with Azure Monitor for logging and analytics.
- As a best practice when creating Azure Firewall rules, use the FQDN tags to create rules.
  - An FQDN tag represents a group of FQDNs associated with well-known Microsoft services.
  - You can use an FQDN tag to allow the required outbound network traffic through the firewall.
- For example, to manually allow Windows Update network traffic through your firewall, you would need to create multiple application rules. Using FQDN tags, you create an application rule, and include the Windows Updates tag. With this rule in place, network traffic to Microsoft Windows Update endpoints can flow through your firewall.

Learn more:

- Get an overview of Azure Firewall.
- Learn about FQDN tags.

Best practice: Deploy a web application firewall (WAF)

Web applications are increasingly targets of malicious attacks that exploit commonly known vulnerabilities. Exploits include SQL injection attacks and cross-site scripting attacks. Preventing such attacks in application code can be challenging, and can require rigorous maintenance, patching and monitoring at multiple layers of the application topology. A centralized web application firewall helps make security management much simpler and helps app administrators guard against threats or intrusions. A web app firewall can react to security threats faster, by patching known vulnerabilities at a central location, instead of securing individual web applications. Existing application gateways can be converted to a web application firewall enabled application gateway easily.

The web application firewall (WAF) is a feature of Azure Application Gateway.

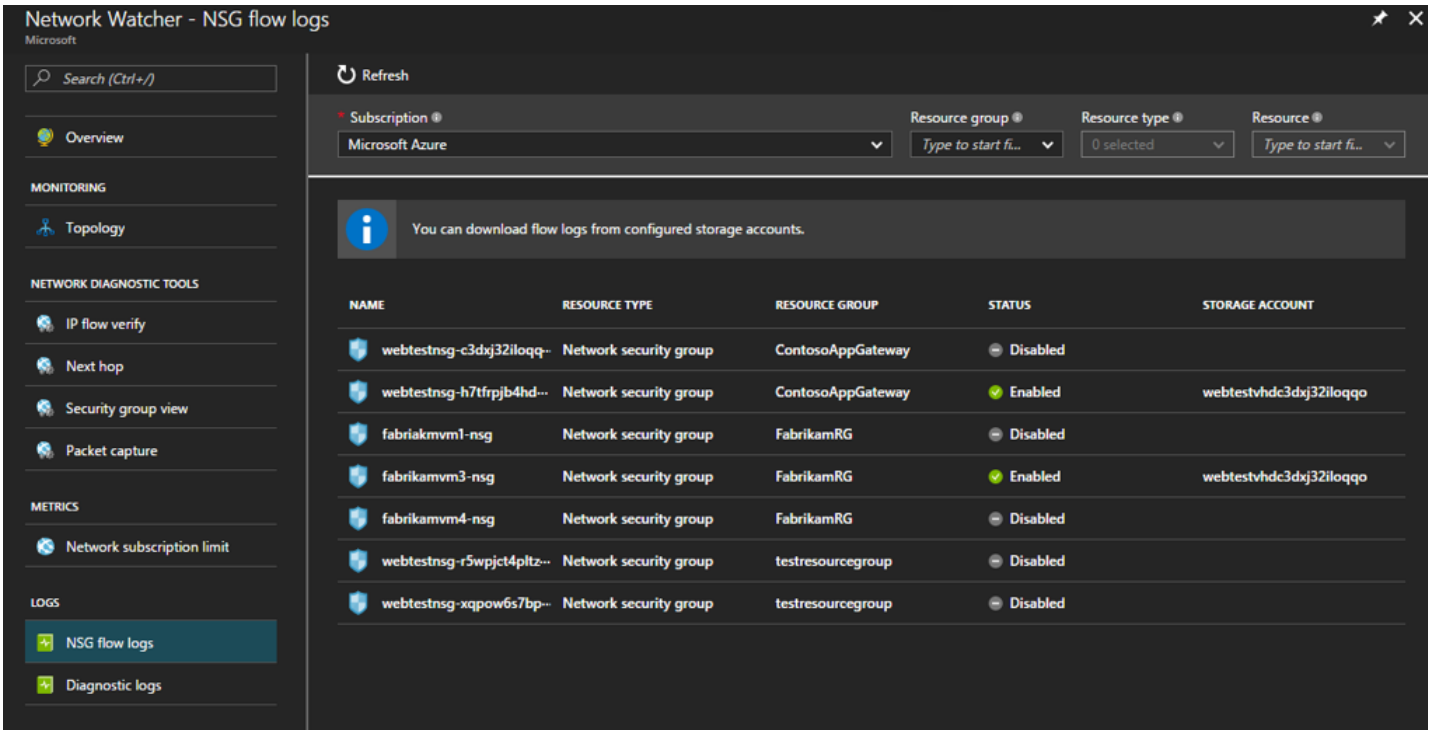
- WAF provides centralized protection of your web applications, from common exploits and vulnerabilities.
- WAF protects without modification to back-end code.
- It can protect multiple web apps at the same time behind an application gateway.
- WAF is integrated with Azure Security Center.
- You can customize WAF rules and rule groups to suit your app requirements.
- As a best practice, you should use a WAF in front on any web-facing app, including apps on Azure VMs or as an Azure App Service.

Learn more:

- Learn about WAF.
- Review WAF limitations and exclusions.

Best practice: Implement Azure Network Watcher

Azure Network Watcher provides tools to monitor resources and communications in an Azure VNet. For example, you can monitor communications between a VM and an endpoint such as another VM or FQDN, view resources and resource relationships in a VNet, or diagnose network traffic issues.



Subscription: Microsoft Azure
Resource group: Type to start fi...
Resource type: 0 selected
Resource: Type to start fi...

You can download flow logs from configured storage accounts.

NAME	RESOURCE TYPE	RESOURCE GROUP	STATUS	STORAGE ACCOUNT
webtestnsg-c3dxj32iloqq-...	Network security group	ContosoAppGateway	Disabled	
webtestnsg-h7tfrpjb4hd-...	Network security group	ContosoAppGateway	Enabled	webtestvhdc3dxj32iloqqo
fabriakmvm1-nsg	Network security group	FabrikamRG	Disabled	
fabrikamvm3-nsg	Network security group	FabrikamRG	Enabled	webtestvhdc3dxj32iloqqo
fabrikamvm4-nsg	Network security group	FabrikamRG	Disabled	
webtestnsg-r5wpjct4pltz-...	Network security group	testresourcegroup	Disabled	
webtestnsg-xqpow6s7bp-...	Network security group	testresourcegroup	Disabled	

Network Watcher

- With Network Watcher you can monitor and diagnose networking issues without logging into VMs.
- You can trigger packet capture by setting alerts, and gain access to real-time performance information at the packet level. When you see an issue, you can investigate it in detail.
- As a best practice, use Network Watcher to review NSG flow logs.

- NSG flow logs in Network Watcher allow you to view information about ingress and egress IP traffic through an NSG.
  - Flow logs are written in JSON format.
  - Flow logs show outbound and inbound flows on a per-rule basis, the network interface (NIC) to which the flow applies, 5-tuple information about the flow (source/destination IP, source/destination port, and protocol), and whether the traffic was allowed or denied.

Learn more:

- Get an overview of Network Watcher.
- Learn more about NSG flow Logs.

Use partner tools in the Azure Marketplace

For more complex network topologies, you might use security products from Microsoft partners, in particular network virtual appliances (NVAs).

- An NVA is a VM that performs a network function, such as a firewall, WAN optimization, or other network function.
- NVAs bolster VNet security and network functions. They can be deployed for highly available firewalls, intrusion prevention, intrusion detection, web application firewalls (WAFs), WAN optimization, routing, load balancing, VPN, certificate management, Active Directory, and multi-factor authentication.
- NVA is available from numerous vendors in the Azure Marketplace.

Best practice: Implement firewalls and NVAs in hub networks

In the hub, the perimeter network (with access to the internet) is normally managed through an Azure firewall, a firewall farm, or a web application firewall (WAF). Consider the following comparisons.

Firewall type	Details
WAFs	Web applications are common, and tend to suffer from vulnerabilities and potential exploits. WAFs are designed to detect attacks against web applications (HTTP/HTTPS), more specifically than a generic firewall. Compared with traditional firewall technology, WAFs have a set of specific features that protect internal web servers from threats.
Azure Firewall	Like NVA firewall farms, Azure Firewall uses a common administration mechanism, and a set of security rules to protect workloads hosted in spoke networks, and to control access to on-premises networks. The Azure Firewall has built-in scalability.
NVA firewalls	Like Azure Firewall NVA firewall farms have common administration mechanism, and a set of security rules to protect workloads hosted in spoke networks, and to control access to on-premises networks. NVA firewalls can be manually scaled behind a load balancer. Though an NVA firewall has less specialized software than a WAF, it has broader application scope to filter and inspect any type of traffic in egress and ingress. If you want to use NVA you can find them in the Azure Marketplace.

We recommend using one set of Azure Firewalls (or NVAs) for traffic originating on the internet, and another for traffic originating on-premises.

- Using only one set of firewalls for both is a security risk, as it provides no security perimeter between the two sets of network traffic.
- Using separate firewall layers reduces the complexity of checking security rules, and it's clear which rules correspond to which incoming network request.

Learn more:

- Learn about using NVAs in an Azure VNet.

Next steps

Review other best practices:

- Best practices for security and management after migration.
- Best practices for cost management after migration.