**AZ-104: Configure and manage virtual networks for Azure administrators**

A virtual network can be segmented into one or more subnets. Subnets provide logical divisions within your network. Subnets can help improve security, increase performance, and make it easier to manage the network.

Each subnet contains a range of IP addresses that fall within the virtual network address space. The range must be unique within the address space for the virtual network. The range can't overlap with other subnet address ranges within the virtual network. The address space must be specified by using Classless Inter-Domain Routing (CIDR) notation.’

**Service requirements**. Each service directly deployed into virtual network has specific requirements for routing and the types of traffic that must be allowed into and out of subnets. A service may require, or create, their own subnet, so there must be enough unallocated space for them to do so. For example, if you connect a virtual network to an on-premises network using an Azure VPN Gateway, the virtual network must have a dedicated subnet for the gateway.

**Virtual appliances**. Azure routes network traffic between all subnets in a virtual network, by default. You can override Azure's default routing to prevent Azure routing between subnets, or to route traffic between subnets through a network virtual appliance. So, if you require that traffic between resources in the same virtual network flow through a network virtual appliance (NVA), deploy the resources to different subnets.

**Service endpoints**. You can limit access to Azure resources such as an Azure storage account or Azure SQL database, to specific subnets with a virtual network service endpoint. Further, you can deny access to the resources from the internet. You may create multiple subnets, and enable a service endpoint for some subnets, but not others.

**Network security groups**. You can associate zero or one network security group to each subnet in a virtual network. You can associate the same, or a different, network security group to each subnet. Each network security group contains rules, which allow or deny traffic to and from sources and destinations.

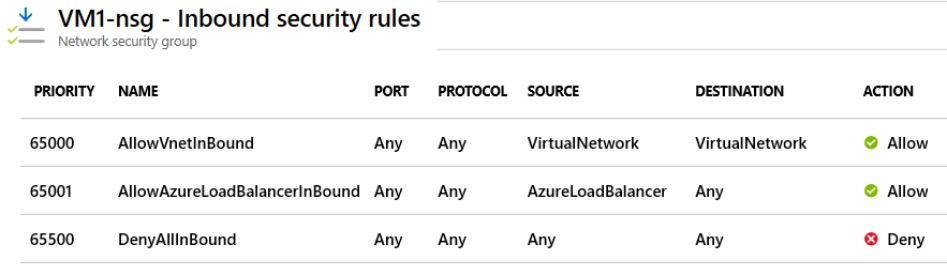
Reserved IP addresses:

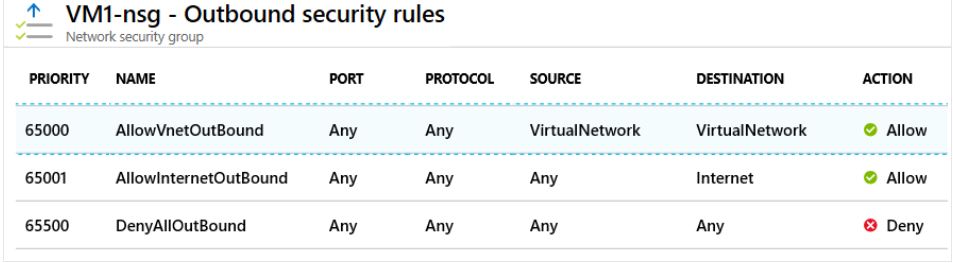
* x.x.x.0: Network address
* x.x.x.1: Reserved by Azure for the default gateway
* x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
* x.x.x.255: Network broadcast address

You can assign IP addresses to Azure resources to communicate with other Azure resources, your on-premises network, and the Internet. There are two types of Azure IP addresses: public and private IP addresses.

* **Private IP addresses**: Used for communication within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure.
* **Public IP addresses**: Used for communication with the Internet, including Azure public-facing services.
* **Dynamic**. Dynamic addresses are assigned only after a public IP address is associated to an Azure resource, and the resource is started for the first time. Dynamic addresses can change if they're assigned to a resource, such as a virtual machine, and the virtual machine is stopped (deallocated), and then restarted. The address remains the same if a virtual machine is rebooted or stopped (but not deallocated). Dynamic addresses are released when a public IP address resource is dissociated from a resource.
* **Static**. Static addresses are assigned when a public IP address is created. Static addresses aren't released until a public IP address resource is deleted. If the address isn't associated to a resource, you can change the assignment method after the address is created. If the address is associated to a resource, you may not be able to change the assignment method. If you select IPv6 for the IP version, the assignment method must be Dynamic for Basic SKU. Standard SKU addresses are Static for both IPv4 and IPv6.

You can limit network traffic to resources in a virtual network using a network security group (NSG). A network security group contains a list of security rules that allow or deny inbound or outbound network traffic. An NSG can be associated to a subnet or a network interface. A network security group can be associated multiple times.





Service. Service specifies the destination protocol and port range for this rule. You can choose a predefined service, like HTTPS and SSH. When you select a service, the Port range is automatically completed. Choose custom to provide your own port range.

Port ranges. Port ranges can include a single port, a port range, or a comma-separated list of ports. The ports designate the traffic will be allowed or denied by this rule. Provide an asterisk (\*) to allow traffic on any port.

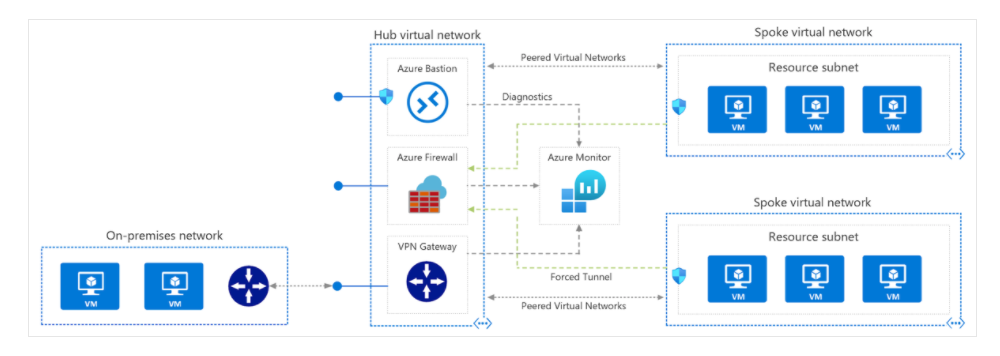
Priority. Rules are processed in priority order. The lower the number, the higher the priority. We recommend leaving gaps between rules to make it easier to add new rules. The value is between 100-4096 and unique for all security rules within the network security group.

**The comptroller wants to simplify network security group rules by using service tags. Which of the following is a valid service tag?**

**VirtualNetwork**

**That's correct. VirtualNetwork is a valid service tag. Service tags represent a group of IP addresses. Other service tags are Internet, SQL, Storage, AzureLoadBalancer, and AzureTrafficManager.**

* **Built-in high availability**. High availability is built in, so additional load balancers aren't required. There's nothing you need to configure.
* **Availability Zones**. Azure Firewall can be configured during deployment to span multiple Availability Zones for increased availability.
* **Unrestricted cloud scalability**. Azure Firewall can scale up as much as you need to accommodate changing network traffic flows, so you don't need to budget for your peak traffic.
* **Application FQDN filtering rules**. You can limit outbound HTTP/S traffic or Azure SQL traffic to a specified list of fully qualified domain names (FQDN) including wild cards.
* **Network traffic filtering rules**. You can centrally create allow or deny network filtering rules by source and destination IP address, port, and protocol. Azure Firewall is fully stateful, so it can distinguish legitimate packets for different types of connections. Rules are enforced and logged across multiple subscriptions and virtual networks.
* **Threat intelligence**. Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed.
* **Multiple public IP addresses**. You can associate multiple public IP addresses (up to 100) with your firewall.



The Domain Name System is a hierarchy of domains. The hierarchy starts from the 'root' domain, whose name is simply '.'. Below this come top-level domains, such as 'com', 'net', 'org', 'uk' or 'jp'. Below these top-level domains are second-level domains, such as 'org.uk' or 'co.jp'. And so on. The domains in the DNS hierarchy are hosted using separate DNS zones. These zones are globally distributed, hosted by DNS name servers around the world.

There are two types of DNS servers:

* An *authoritative* DNS server hosts DNS zones. It answers DNS queries for records in those zones only.
* A *recursive* DNS server doesn't host DNS zones. It answers all DNS queries by calling authoritative DNS servers to gather the data it needs.

**DNS Subdomain:** *maps*.google.com, *images*.google.com

**DNS Zones:** A zone is a subsect of a domain that contains specific logic for the resources inside of it. For instance, a zone might contain maps.google.com, while another zone could contain images.google.com AND mail.google.com. All the information for a zone is stored in what’s called a DNS zone file, which is the key to understanding how a DNS zone operates. A zone file is a plain text file stored in a DNS server that contains an actual representation of the zone and contains all the records for every domain within the zone. Zone files must always start with a [Start of Authority (SOA) record](https://www.cloudflare.com/learning/dns/dns-records/dns-soa-record/), which contains important information including contact information for the zone administrator.

**DNS Delegation:** How does a parent zone 'point' to the name servers for a child zone? It does this using a special type of DNS record called an NS record (NS stands for 'name server'). For example, the root zone contains NS records for 'com' and shows the name servers for the 'com' zone. In turn, the 'com' zone contains NS records for 'contoso.com', which shows the name servers for the 'contoso.com' zone. Setting up the NS records for a child zone in a parent zone is called delegating the domain.

**DNS Record Sets:**

**DNS record types:**

Azure DNS supports all common DNS record types: A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV, and TXT.

**A**: Returns a 32-bit [IPv4](https://en.wikipedia.org/wiki/IPv4) address, most commonly used to map [hostnames](https://en.wikipedia.org/wiki/Hostname) to an IP address of the host, but it is also used for [DNSBLs](https://en.wikipedia.org/wiki/DNSBL), storing [subnet masks](https://en.wikipedia.org/wiki/Subnet_mask) in RFC 1101, etc.

**AAAA**: Returns a 128-bit [IPv6](https://en.wikipedia.org/wiki/IPv6) address, most commonly used to map [hostnames](https://en.wikipedia.org/wiki/Hostname) to an IP address of the host. The A or AAAA record maps an IP address to a domain. Multiple IP addresses are known as a record set.

**CAA**: [DNS Certification Authority Authorization](https://en.wikipedia.org/wiki/DNS_Certification_Authority_Authorization), constraining acceptable CAs for a host/domain

**CNAME**: Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.

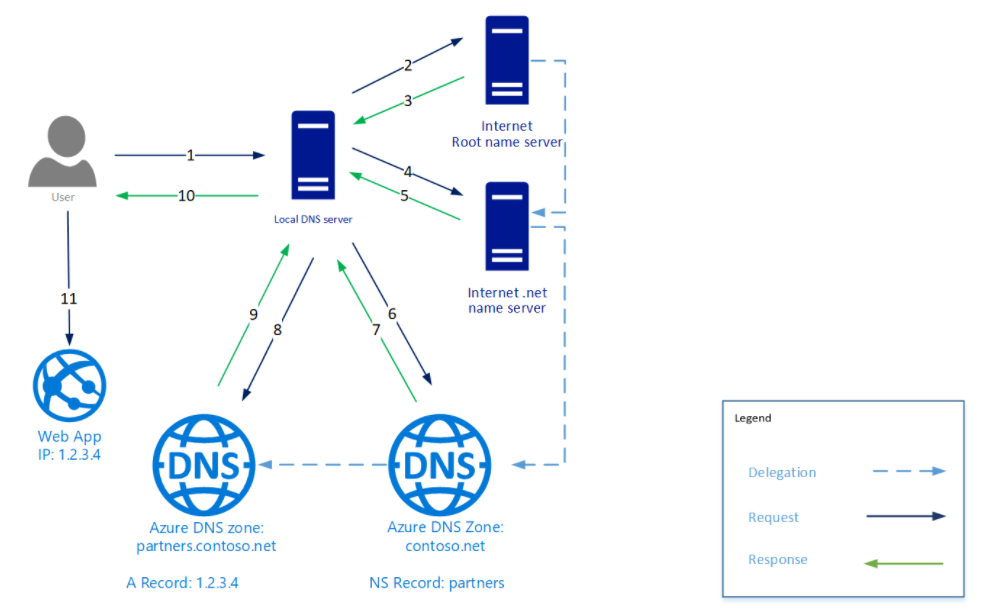
**MX**: Maps a domain name to a list of [message transfer agents](https://en.wikipedia.org/wiki/Message_transfer_agent) for that domain

**NS**: Delegates a [DNS zone](https://en.wikipedia.org/wiki/DNS_zone) to use the given [authoritative name servers](https://en.wikipedia.org/wiki/Authoritative_name_server)

**PTR**: Pointer to a [canonical name](https://en.wikipedia.org/wiki/Canonical_name). Unlike a CNAME, DNS processing stops and just the name is returned. The most common use is for implementing [reverse DNS lookups](https://en.wikipedia.org/wiki/Reverse_DNS_lookup), but other uses include such things as [DNS-SD](https://en.wikipedia.org/wiki/Zero_configuration_networking#Apple's_protocol:_Multicast_DNS/DNS-SD).

**SOA**: Specifies *authoritative* information about a [DNS zone](https://en.wikipedia.org/wiki/DNS_zone), including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.

**SRV**: Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.



Regional VNet peering connects Azure virtual networks in the same region.

Global VNet peering connects Azure virtual networks in different regions. When creating a global peering, the peered virtual networks can exist in any Azure public cloud region or China cloud regions, but not in Government cloud regions. You can only peer virtual networks in the same region in Azure Government cloud regions.

* **Initiated**: When you create the peering to the second virtual network from the first virtual network, the peering status is Initiated.
* **Connected**: When you create the peering from the second virtual network to the first virtual network, its peering status is Connected. When you view the peering status for the first virtual network, you see its status changed from Initiated to Connected. The peering is not successfully established until the peering status for both virtual network peerings is Connected.

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.

Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway. When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

When you create a virtual network gateway, you need to specify several settings. One of the required settings, '-GatewayType', specifies whether the gateway is used for ExpressRoute, or VPN traffic. The two gateway types are:

* **Vpn** - To send encrypted traffic across the public Internet, you use the gateway type 'Vpn'. This is also referred to as a VPN gateway. Site-to-Site, Point-to-Site, and VNet-to-VNet connections all use a VPN gateway.
* **ExpressRoute** - To send network traffic on a private connection, you use the gateway type 'ExpressRoute'. This is also referred to as an ExpressRoute gateway and is the type of gateway used when configuring ExpressRoute.

Site to site:

A site-to-site virtual private network (VPN) is **a connection between two or more networks**, such as a corporate network and a branch office network. Many organizations use site-to-site VPNs to leverage an internet connection for private traffic as an alternative to using private MPLS circuits

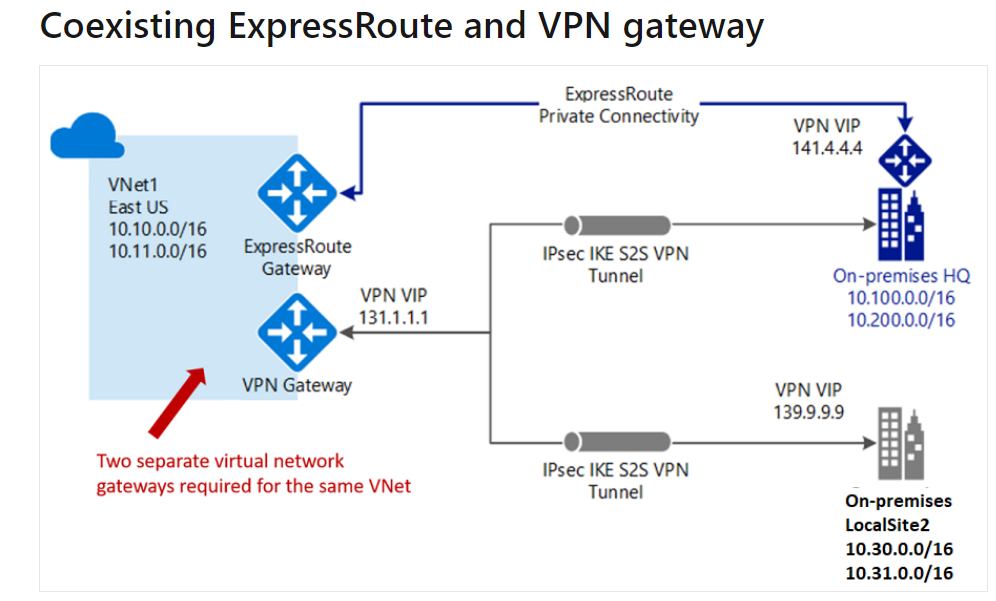
Virtual network to virtual network: Connecting two azure virtual networks. How is this different than vnet peering?

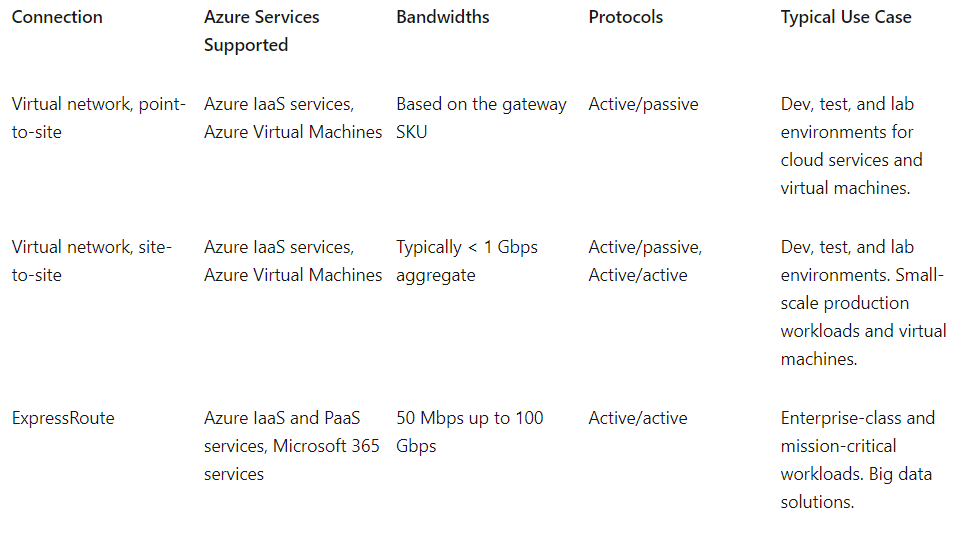
**VNet Peering** provides a low latency, high bandwidth connection useful in scenarios such as cross-region data replication and database failover scenarios. Since traffic is completely private and remains on the Microsoft backbone, customers with strict data policies prefer to use VNet Peering as public internet is not involved. Since there is no gateway in the path, there are no extra hops, ensuring low latency connections.

**VPN Gateways** provide a limited bandwidth connection and is useful in scenarios where encryption is needed, but bandwidth restrictions are tolerable. In these scenarios, customers are also not as latency-sensitive.

Use Azure ExpressRoute to create private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections. In some cases, using ExpressRoute connections to transfer data between on-premises systems and Azure can give you significant cost benefits.

ExpressRoute is a direct, private connection from your WAN (not over the public Internet) to Microsoft Services, including Azure. Site-to-Site VPN traffic travels encrypted over the public Internet. Being able to configure Site-to-Site VPN and ExpressRoute connections for the same virtual network has several advantages.





Point to site: single point to azure, resets if workstation is turned off.

Site to site: persistent connection between two networks (one on prem, one in azure). Connected via router so connection does not recent when computers are restarted.

Express route: For production, can carry larger workload. Probably more expensive…

**Azure Virtual WAN** is a networking service that provides optimized and automated branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to. You use the Azure backbone to connect branches and enjoy branch-to-VNet connectivity. There is a list of partners that support connectivity automation with Azure Virtual WAN VPN.

Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, User VPN (point-to-site), and ExpressRoute into a single operational interface. Connectivity to Azure VNets is established by using virtual network connections. The global transit network architecture based on a hub-and-spoke connectivity model. The cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.

Information about the **system routes** is recorded in a route table. A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network. Route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route table. Packets are matched to routes using the destination. The destination can be an IP address, a virtual network gateway, a virtual appliance, or the internet. If a matching route can't be found, then the packet is dropped.

A virtual network **service endpoint** provides the identity of your virtual network to the Azure service. Once service endpoints are enabled in your virtual network, you can secure Azure service resources to your virtual network by adding a virtual network rule to the resources.

Topics to know:

**Configure and Manage virtual networking (25-30%)**

Create and configure VNET peering

Configure private and public IP addresses, network routes, network interface, subnets, and virtual networks

Do not need a public IP address on a VM to manage it.

Public and Private IP addresses: All azure services are available on public IP addresses.

Consider public IP addresses for public ingress only.

All azure calls go through ARM rest API. You can send http requests, arm templates, terraform calls (Azure sdk), etc…

Service endpoints and private endpoints.

Service endpoints

Private endpoint: instead of create an exception for a provider, you provide an exception for a single resource.

Firewall needs to be in an empty subnet.

Configuring subnets:

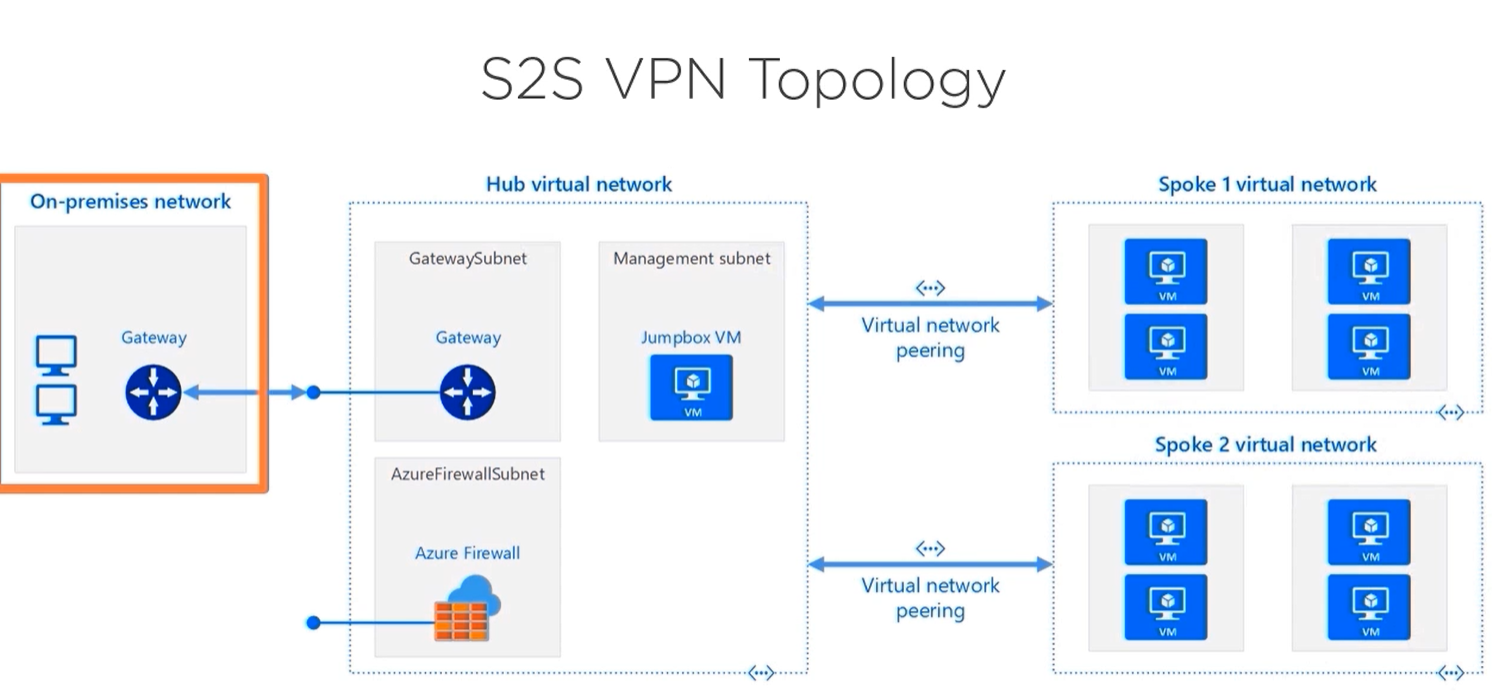
Delegation of a subnet is allowed, and sometimes required. AzureFirewallSubnet is a reserved subnet delegation. If you want to restrict network traffic for a particular resource, you can add a Service Endpoint inside a subnet pointing toward a resource. This limits access to that subnet. Resource is still “accessible” over public internet, but azure redirects traffic. Private Endpoint does the same thing but only for a specific resource!

We can say that a Network Security Group is a firewall, but a very basic one. It is a Microsoft provided solution to filter traffic at the network layer. On the other hand, Azure Firewall is a robust service with tons of features to ensure maximum protection of your resources and regulate traffic depending upon its authenticity. Azure Firewall is a fully managed firewall that can analyze and filter L3 and L4 traffic, as well as L7 application traffic. Azure Firewall offers the same capabilities as of an NSG, and many more in addition. Azure Firewall supports application FQDN tags, whereas NSG lacks this feature. Another major difference between an NSG and Azure Firewall is that Azure Firewall allows you to mask the source and destination network addresses while NSG doesn’t. Also, there is no threat-intelligence-based filtering option in NSG, whereas this feature is present in Azure Firewall.

**Configuring an Azure Virtual Private Network**

VPN is a secure encrypted over an unsecure communications medium (internet).

2 types in Azure: Site to site, S2S VPN, lways on encrypted tunnel. Policy and route based. Policy is kind of outdated. Route based is generally what you want wherever possible. Active/Active, Active/Passive.



Point to site VPN: What you use with Allscripts VPN. Single workstation connects to a remote network.

Runs on private carrier network (Comcast or AT&T maybe…)

Azure virtual wan: Microsoft managed hub and spoke architecture. Roll up of services: VNet peering, Azure VPN types, ExpressRoute, Azure Firewall, User-defined routing.

Configure High availability

Azure WAN contains Hubs