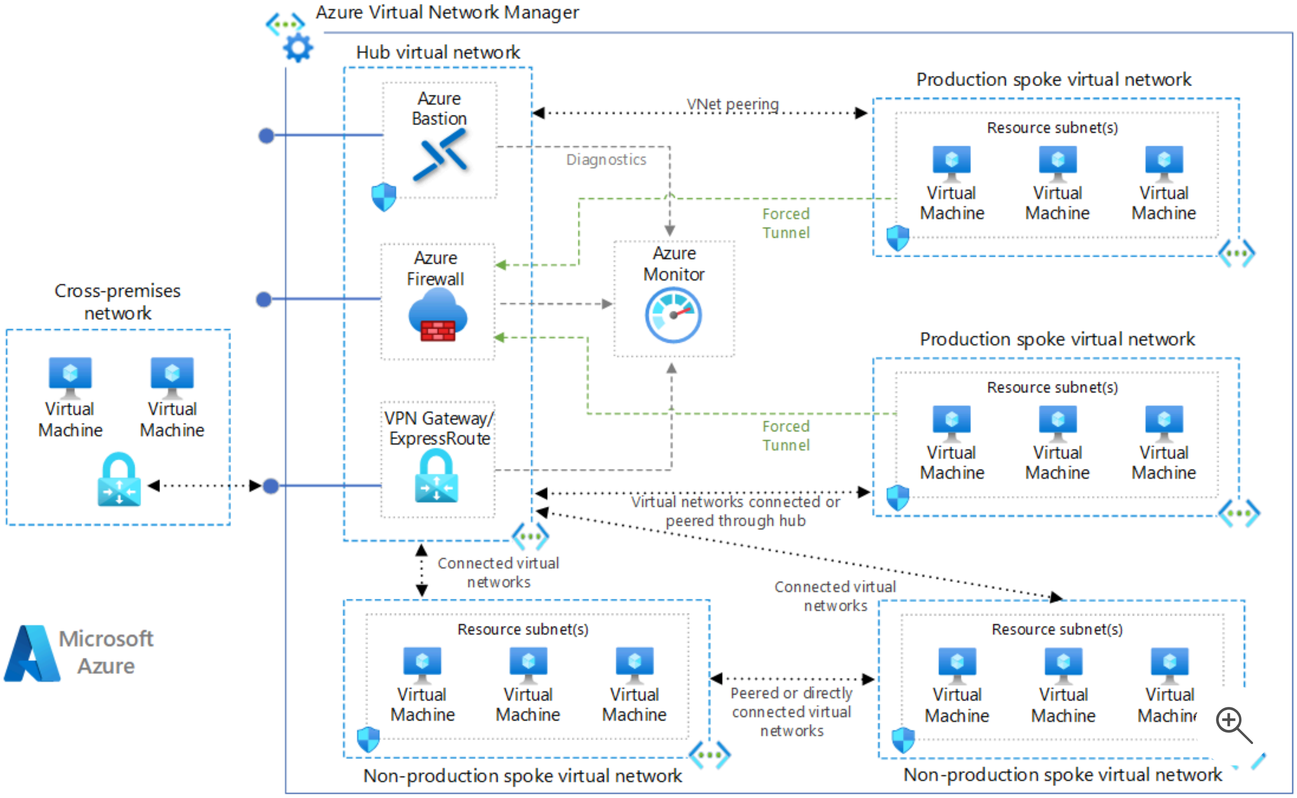
Hub-spoke network topology in Azure

Azure Bastion Azure Firewall Azure Network Watcher Azure Virtual Network Azure VPN Gateway

This reference architecture implements a hub-spoke network pattern with customer-managed hub infrastructure components. For a Microsoft-managed hub infrastructure solution, see Hub-spoke network topology with Azure Virtual WAN.

Hub-spoke is one of the network topologies recommended by the Cloud Adoption Framework. See, Define an Azure network topology to understand why this topology is considered a best practice for many organizations.

Architecture



Download a Visio file of this architecture.

Hub-spoke concepts

Hub-spoke network topologies typically include the many of following architectural concepts:

- **Hub virtual network** - The hub virtual network hosts shared Azure services. Workloads hosted in the spoke virtual networks can use these services. The hub virtual network is the central point of connectivity for cross-premises networks. The hub contains your primary point of egress and provides a mechanism to connect one spoke to another in situations where cross virtual network traffic is needed.

  A hub is a regional resource. Organizations that have their workloads in multiple regions, will should have multiple hubs, one per region.

  The hub enables the following concepts:

  - **Cross-premise gateway** - Cross-premise connectivity is the ability to connect and integrate different network environments to one another. This gateway is usually a VPN or an ExpressRoute circuit.

  - **Egress control** - The management and regulation of outbound traffic that originates in the peered spoke virtual networks.

  - **(optional) Ingress control** - The management and regulation of inbound traffic to endpoints that exist in peered spoke virtual networks.

  - **Remote access** - Remote access is how individual workloads in spoke networks are accessed from network location other than the spoke's own network. This could be for the workload's data or control plane.

  - **Remote spoke access for virtual machines** - The hub can be a convenient location to build out a cross-organization remote connectivity solution for RDP and SSH access to virtual machines distributed throughout spoke networks.

  - **Routing** - Manages and directs traffic between the hub and the connected spokes to enable secure and efficient communication.

- **Spoke virtual networks** - Spoke virtual networks isolate and manage workloads separately in each spoke. Each workload can include multiple tiers, with multiple subnets connected through Azure load balancers. Spokes can exist in different subscriptions and represent different environments, such as production and non-production. One workload could even spread across multiple spokes.

In most scenarios, a spoke should only be peered to a single hub network and that hub network should be in the same region as the spoke.

These spoke networks follow the rules for default outbound access. A core purpose of this the hub-spoke network topology is to generally direct outbound Internet traffic through the control mechanisms offered by the hub.

- **Virtual network cross-connectivity** - Virtual network connectivity is the path in which one isolated virtual network can communicate with another through a control mechanism. The control mechanism enforces permissions and allowed direction of communications between networks. A hub will provide an option to support select cross-network connections to flow through the centralized network.

- **DNS** - Hub-spoke solutions are often responsible for providing a DNS solution to be used by all peered spokes, especially for cross-premises routing and for private endpoint DNS records.

Components

- Azure Virtual Network is the fundamental building block for private networks in Azure. Virtual Network enables many Azure resources, such as Azure VMs, to securely communicate with each other, cross-premises networks, and the internet.

  This architecture connects virtual networks to the hub by using peering connections which are non-transitive, low-latency connections between virtual networks. Peered virtual networks can exchange traffic over the Azure backbone without needing a router. In a hub-spoke architecture, directly peering virtual networks to each other is minimal and reserved for special case scenarios.

- Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to VMs without exposing their public IP addresses. In this architecture, Azure Bastion is used as a managed offering to support direct VM access across connected spokes.

- Azure Firewall is a managed cloud-based network security service that protects Virtual Network resources. This stateful firewall service has built-in high availability and unrestricted cloud scalability to help you create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

  In this architecture, Azure Firewall has multiple potential roles. The firewall is the primary egress point for Internet-destined traffic from the peered spoke virtual networks. The firewall can also be used to inspect inbound traffic, using IDPS rules. And finally, the Firewall can also be used as a DNS proxy server to support FQDN traffic rules.

- VPN Gateway is a specific type of virtual network gateway that sends encrypted traffic between a virtual network on Azure and different network over the public internet. You can also use VPN Gateway to send encrypted traffic between other hubs virtual networks over the Microsoft network.

  In this architecture, this would be one option to connect some or all of the spokes to the remote network. Spokes would typically not deploy their own VPN Gateway, and instead use the centralized solution offered by the hub. You need to establish routing configuration to manage this connectivity.

- Azure ExpressRoute gateway exchanges IP routes and routes network traffic between your on-premises network and your Azure virtual network. In this architecture, ExpressRoute would alternative option to a VPN Gateway to connect some or all of the spokes to a remote network. Spokes would not deploy their own ExpressRoute, and instead those spokes would use the centralized solution offered by the hub. Like with a VPN Gateway, you need to establish routing configuration to manage this connectivity.

- Azure Monitor can collect, analyze, and act on telemetry data from cross-premises environments, including Azure and on-premises. Azure Monitor helps you maximize the performance and availability of your applications and proactively identify problems in seconds. In this architecture, Azure Monitor is the log and metric sink for the hub resources and for network metrics. Azure Monitor might be used as a logging sink for resources in spoke networks as well, but that's a decision for the various connected workloads and is not mandated by this architecture.

Alternatives

This architecture involves the creation, configuration, and maintenance of several Azure resource primitives, namely: `virtualNetworkPeerings`, `routeTables`, and `subnets`. Azure Virtual Network Manager is a management service that helps you group, configure, deploy, and manage virtual networks at scale across Azure subscriptions, regions, and Microsoft Entra directories. With Virtual Network Manager, you can define network groups to identify and logically segment your virtual networks. You can use connected groups that allow virtual networks within a group to communicate with each other as if they were manually connected. This layer adds a layer of abstraction over those primitives to focus on describing the networking topology vs working about the implementation of that topology.

It's recommended that you evaluate using Virtual Network Manager as a way to optimize your time spending with network management operations. Evaluate the cost of the service against your calculated value/savings to determine if Virtual Network Manger is a net benefit for your network's size and complexity.

Scenario details

This reference architecture implements a hub-spoke network pattern where the hub virtual network acts as a central point of connectivity to many spoke virtual networks. The spoke virtual networks connect with the hub and can be used to isolate workloads. You can also enable cross-premises scenarios by using the hub to connect to on-premises networks.

This architecture describes a network pattern with customer-managed hub infrastructure components. For a Microsoft-managed hub infrastructure solution, see Hub-spoke network topology with Azure Virtual WAN.

The benefits of using a customer-managed hub and spoke configuration include:

- Cost savings
- Overcoming subscription limits
- Workload isolation
- Flexibility
  - More control over how network virtual appliances (NVAs) are deployed, such as number of NICs, number of instances, or the compute size.
  - Use of NVAs that aren't supported by Virtual WAN

For more information, see Hub-and-spoke network topology.

Potential use cases

Typical uses for a hub and spoke architecture include workloads that:

- Have several environments that require shared services. For example, a workload might have development, testing, and production environments. Shared services might include DNS IDs, Network Time Protocol (NTP), or Active Directory Domain Services (AD DS). Shared services are placed in the hub virtual network, and each environment deploys to a different spoke to maintain isolation.
- Don't require connectivity to each other, but require access to shared services.
- Require central control over security, like a perimeter network (also known as DMZ) firewall in the hub with segregated workload management in each spoke.

- Require central control over connectivity, such as selective connectivity or isolation between spokes of certain environments or workloads.

Recommendations

The following recommendations apply to most scenarios. Follow these recommendations unless you have specific requirements that override them.

Resource groups, subscriptions, and regions

This example solution uses a single Azure resource group. You can also implement the hub and each spoke in different resource groups and subscriptions.

When you peer virtual networks in different subscriptions, you can associate the subscriptions to the same or different Microsoft Entra tenants. This flexibility allows for decentralized management of each workload while maintaining shared services in the hub. See Create a virtual network peering - Resource Manager, different subscriptions, and Microsoft Entra tenants.

Azure landing zones

The Azure landing zone architecture is based on the hub-spoke topology. In that architecture, the hub's shared resources and network is managed by a centralized platform team, while spokes share a co-ownership model with the platform team and the workload team that is using the spoke network. All hubs reside in a "Connectivity" subscription for centralized management, while spoke virtual networks exist across many individual workload subscriptions, called application landing zone subscriptions.

Virtual network subnets

The following recommendations outline how to configure the subnets on the virtual network.

GatewaySubnet

The virtual network gateway requires this subnet. You can also use a hub-spoke topology without a gateway if you don't need cross-premises network connectivity.

Create a subnet named *GatewaySubnet* with an address range of at least 26. The `/26` address range gives the subnet enough scalability configuration options to prevent reaching the gateway size limitations in the future and to accommodate for a higher number of ExpressRoute circuits. For more information about setting up the gateway, see Hybrid network using a VPN gateway.

AzureFirewallSubnet

Create a subnet named *AzureFirewallSubnet* with an address range of at least `/26`. Regardless of scale, the `/26` address range is the recommended size and covers any future size limitations. This subnet doesn't support network security groups (NSGs).

Azure Firewall requires this subnet. If you use a partner network virtual appliance (NVA), follow its network requirements.

Spoke network connectivity

Virtual network peering or connected groups are non-transitive relationships between virtual networks. If you need spoke virtual networks to connect to each other, add a peering connection between those spokes or place them in the same network group.

Spoke connections through Azure Firewall or NVA

The number of virtual network peerings per virtual network is limited. If you have many spokes that need to connect with each other, you could run out of peering connections. Connected groups also have limitations. For more information, see Networking limits and Connected groups limits.

In this scenario, consider using user-defined routes (UDRs) to force spoke traffic to be sent to Azure Firewall or another NVA that acts as a router at the hub. This change allows the spokes to connect to each other. To support this configuration, you must implement Azure Firewall with forced tunnel configuration enabled. For more information, see Azure Firewall forced tunneling.

The topology in this architectural design facilitates egress flows. While Azure Firewall is primarily for egress security, it can also be an ingress point. For more considerations about hub NVA ingress routing, see Firewall and Application Gateway for virtual networks.

Spoke connections to remote networks through a hub gateway

To configure spokes to communicate with remote networks through a hub gateway, you can use virtual network peerings or connected network groups.

To use virtual network peerings, in the virtual network **Peering** setup:

- Configure the peering connection in the hub to **Allow** gateway transit.
- Configure the peering connection in each spoke to **Use the remote virtual network's gateway**.
- Configure all peering connections to **Allow** forwarded traffic.

For more information, see Create a virtual network peering.

To use connected network groups:

1. In Virtual Network Manager, create a network group and add member virtual networks.
2. Create a hub and spoke connectivity configuration.
3. For the **Spoke network groups**, select **Hub as gateway**.

For more information, see Create a hub and spoke topology with Azure Virtual Network Manager.

Spoke network communications

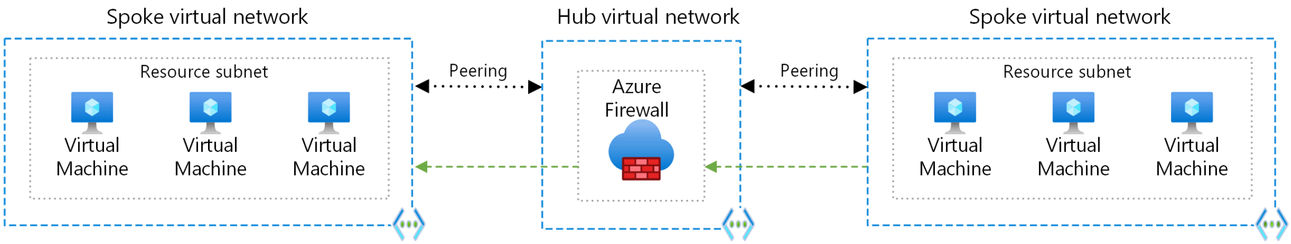
There are two main ways to allow spoke virtual networks to communicate with each other:

- Communication via an NVA like a firewall and router. This method incurs a hop between the two spokes.
- Communication by using virtual network peering or Virtual Network Manager direct connectivity between spokes. This approach doesn't cause a hop between the two spokes and is recommended for minimizing latency.
- Private Link could be used to selectively expose individual resources to other virtual networks. For example, exposing an internal load balancer to a different virtual network, without needing to form or maintain peering or routing relationships.

For more information on spoke-to-spoke networking patterns, see Spoke-to-spoke networking.

Communication through an NVA

If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.



You can also use a VPN gateway to route traffic between spokes, although this choice affects latency and throughput. For configuration details, see Configure VPN gateway transit for virtual network peering.

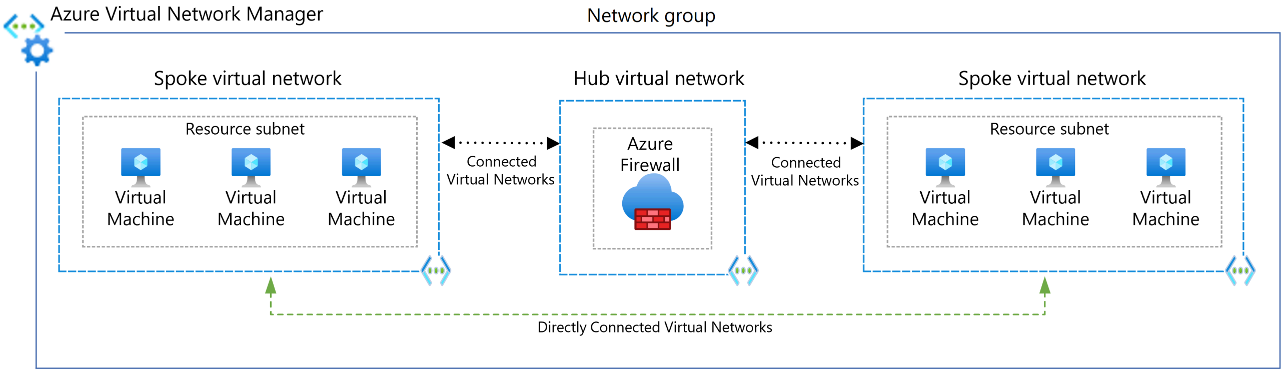
Evaluate the services you share in the hub to ensure that the hub scales for a larger number of spokes. For instance, if your hub provides firewall services, consider your firewall solution's bandwidth limits when you add multiple spokes. You can move some of these shared services to a second level of hubs.

Direct communication between spoke networks

To connect directly between spoke virtual networks without traversing the hub virtual network, you can create peering connections between spokes or enable direct connectivity for the network group. It's best to limit peering or direct connectivity to spoke virtual networks that are part of the same environment and workload.

When you use Virtual Network Manager, you can add spoke virtual networks to network groups manually, or add networks automatically based on conditions you define.

The following diagram illustrates using Virtual Network Manager for direct connectivity between spokes.



Considerations

These considerations implement the pillars of the Azure Well-Architected Framework, which is a set of guiding tenets that can be used to improve the quality of a workload. For more information, see Microsoft Azure Well-Architected Framework.

Reliability

Reliability ensures your application can meet the commitments you make to your customers. For more information, see Overview of the reliability pillar.

Use Availability zones for Azure services in the hub that support them.

As a general rule, it's best to have at least one hub per region and only connect spokes to those hubs from the same region. This configuration helps bulkhead regions to avoid a failure in one region's hub causing widespread network routing failures in unrelated regions.

For higher availability, you can use ExpressRoute plus a VPN for failover. See Connect an on-premises network to Azure using ExpressRoute with VPN failover and follow the guidance to design and architect Azure ExpressRoute for resiliency.

Due to how Azure Firewall implements FQDN application rules, ensure that all resources that are egressing through the firewall is using the same DNS provider as the firewall itself. Without this, Azure Firewall might block legitimate traffic because the firewall's IP resolution of the FQDN differs from the traffic originator's IP resolution of the same FQDN. Incorporating Azure Firewall proxy as part of spoke DNS resolution is one solution to ensure FQDNs are in sync with both the traffic originator and Azure Firewall.

Security

Security provides assurances against deliberate attacks and the abuse of your valuable data and systems. For more information, see Design review checklist for Security.

To protect against DDoS attacks, enable Azure DDOS Protection on any perimeter virtual network. Any resource that has a public IP is susceptible to a DDoS attack. Even if your workloads aren't exposed publicly, you still have public IPs that need to be protected, such as:

- Azure Firewall's public IPs
- The VPN gateway's public IPs
- ExpressRoute's control plane public IP

To minimize the risk of unauthorized access and to enforce strict security policies, always set explicit deny rules in network security groups (NSGs).

Use the Azure Firewall Premium version to enable TLS inspection, network intrusion detection and prevention system (IDPS), and URL filtering.

Virtual Network Manager security

To ensure a baseline set of security rules, make sure to associate security admin rules with virtual networks in network groups. Security admin rules take precedence over and are evaluated before NSG rules. Like NSG rules, security admin rules support prioritization, service tags, and L3-L4 protocols. For more information, see Security admin rules in Virtual Network Manager.

Use Virtual Network Manager deployments to facilitate controlled rollout of potentially breaking changes to network group security rules.

Cost Optimization

Cost Optimization is about ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see Design review checklist for Cost Optimization.

Consider the following cost-related factors when you deploy and manage hub and spoke networks. For more information, see Virtual network pricing .

Azure Firewall costs

This architecture deploys an Azure Firewall instance in the hub network. Using an Azure Firewall deployment as a shared solution consumed by multiple workloads can significantly save cloud costs compared to other NVAs. For more information, see Azure Firewall vs. network virtual appliances .

To use all deployed resources effectively, choose the right Azure Firewall size. Decide what features you need and which tier best suits your current set of workloads. To learn about the available Azure Firewall SKUs, see What is Azure Firewall?

Direct peering

Selective use of direct peering or other non-hub routed communication between spokes can avoid the cost of Azure Firewall processing. Savings can be significant for networks that have workloads with high-throughput, low-risk communication between spokes, such as database synchronization or large file copy operations.

Operational Excellence

Operational Excellence covers the operations processes that deploy an application and keep it running in production. For more information, see Design review checklist for Operational Excellence.

Enable diagnostic settings for all services, such as Azure Bastion, Azure Firewall, and your cross-premesis gateway. Determine which settings are meaningful to your operations. Turn off settings that aren't meaningful to avoid undue costs. Resources such as Azure Firewall can be verbose with logging and you can incur high monitoring costs.

Use Connection monitor for end-to-end monitoring to detect anomalies and to identify and troubleshoot network issues.

Use Azure Network Watcher to monitor and troubleshoot network components, including using Traffic Analytics to show you the systems in your virtual networks that generate the most traffic. You can visually identify bottlenecks before they become problems.

If you're using ExpressRoute, use ExpressRoute Traffic Collector where you can analyze flow logs for the network flows sent over your ExpressRoute circuits. ExpressRoute Traffic Collector gives you visibility into traffic flowing over Microsoft enterprise edge routers.

Use FQDN-based rules in Azure Firewall for protocols other than HTTP(s) or when configuring SQL Server. Using FQDNs lowers the management burden over managing individual IP addresses.

Plan for IP addressing based on your peering requirements, and make sure the address space doesn't overlap across cross-premises locations and Azure locations.

Automation with Azure Virtual Network Manager

To centrally manage connectivity and security controls, use Azure Virtual Network Manager to create new hub and spoke virtual network topologies or onboard existing topologies. Using Virtual Network Manager ensures that your hub and spoke network topologies are prepared for large-scale future growth across multiple subscriptions, management groups, and regions.

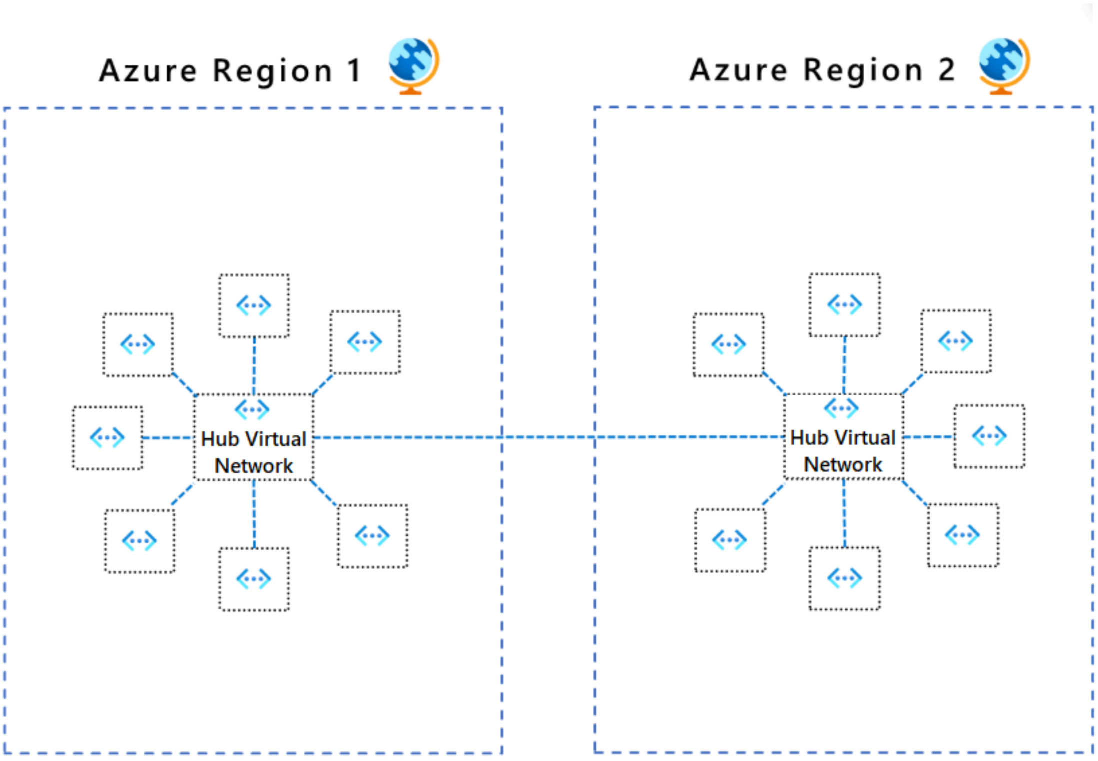
Example Virtual Network Manager use case scenarios include:

- Democratization of spoke virtual network management to groups such as business units or application teams. Democratization can result in large numbers of virtual network-to-virtual network connectivity and network security rules requirements.
- Standardization of multiple replica architectures in multiple Azure regions to ensure a global footprint for applications.

To ensure uniform connectivity and network security rules, you can use network groups to group virtual networks in any subscription, management group, or region under the same Microsoft Entra tenant. You can automatically or manually onboard virtual networks to network groups through dynamic or static membership assignments.

You define discoverability of the virtual networks that Virtual Network Manager manages by using Scopes. This feature provides flexibility for a desired number of network manager instances, which allows further management democratization for virtual network groups.

To connect spoke virtual networks in the same network group to each other, use Virtual Network Manager to implement virtual network peering or direct connectivity. Use the global mesh option to extend mesh direct connectivity to spoke networks in different regions. The following diagram shows global mesh connectivity between regions.



You can associate virtual networks within a network group to a baseline set of security admin rules. Network group security admin rules prevent spoke virtual network owners from overwriting baseline security rules, while letting them independently add their own sets of security rules and NSGs. For an example of using security admin rules in hub and spoke topologies, see Tutorial: Create a secured hub and spoke network.

To facilitate a controlled rollout of network groups, connectivity, and security rules, Virtual Network Manager configuration deployments help you safely release potentially breaking configuration changes to hub and spoke environments. For more information, see Configuration deployments in Azure Virtual Network Manager.

To simplify and streamline the process of creating and maintaining route configurations, you can use automated management of user-defined routes (UDRs) in Azure Virtual Network Manager.

To simplify and centralize the management of IP addresses, you can use IP address management (IPAM) in Azure Virtual Network Manager. IPAM prevents IP address space conflicts across on-premises and cloud virtual networks.

To get started with Virtual Network Manager, see Create a hub and spoke topology with Azure Virtual Network Manager.

Performance Efficiency

Performance efficiency is the ability of your workload to scale to meet the demands placed on it by users in an efficient manner. For more information, see Performance Efficiency pillar overview.

For workloads that communicate from on-premises to virtual machines in an Azure virtual network that require low latency and high bandwidth, consider using ExpressRoute FastPath. FastPath allows you to send traffic directly to virtual machines in your virtual network from on-premises, bypassing the ExpressRoute virtual network gateway, increasing performance.

For spoke-to-spoke communications that require low-latency, consider configuring spoke-to-spoke networking.

Choose the appropriate gateway SKU that meet your requirements, such as number of point-to-site or site-to-site connections, required packets-per-second, bandwidth requirements, and TCP flows.

For latency-sensitive flows, such as SAP or access to storage, consider bypassing Azure Firewall or even routing through the hub at all. You can test latency introduced by Azure Firewall to help inform your decision. You can use features such as VNet peering that connects two or more networks or Azure Private Link that enables you to connect to a service over a private endpoint in your virtual network.

Understand that enabling certain features in Azure Firewall, such as intrusion detection and prevention system (IDPS), reduces your throughput. For more information, see Azure Firewall performance.

Deploy this scenario

This deployment includes one hub virtual network and two connected spokes, and also deploys an Azure Firewall instance and Azure Bastion host. Optionally, the deployment can include VMs in the first spoke network and a VPN gateway. You can choose between virtual network peering or Virtual Network Manager connected groups to create the network connections. Each method has several deployment options.

- Hub-and-spoke with virtual network peering deployment
- Hub-and-spoke with Virtual Network Manager connected groups deployment

Contributors

This article is maintained by Microsoft. It was originally written by the following contributors.

Principal authors:

- Alejandra Palacios | Senior Customer Engineer
- Jose Moreno | Principal Engineer
- Adam Torkar | Azure Networking Global Blackbelt at Microsoft

Other contributors:

- Matthew Bratschun | Customer Engineer
- Jay Li | Senior Product Manager
- Telmo Sampaio | Principal Service Engineering Manager

To see non-public LinkedIn profiles, sign in to LinkedIn.

Next steps

- To learn about secured virtual hubs and the associated security and routing policies that Azure Firewall Manager configures, see What is a secured virtual hub?

Advanced scenarios

Your architecture may differ from this simple hub-spoke architecture. The following is a list of guidance for some advanced scenarios:

- **Add more regions and fully-mesh the hubs to each other** - Spoke-to-spoke networking for multi-region connectivity patterns and Multi-region networking with Azure Route Server

- **Replace Azure Firewall with a custom network virtual appliance (NVA)** - Deploy highly available NVAs

- **Replace Azure Virtual Network Gateway with custom SDWAN NVA** - SDWAN integration with Azure hub-and-spoke network topologies

- **Use Azure Route Server to provide transitivity between your ExpressRoute and VPN or SDWAN, or to customize prefixes advertised over BGP on Azure virtual network gateways** - Azure Route Server support for ExpressRoute and Azure VPN

- **Add Private resolver or DNS servers** - Private resolver architecture

Related resources

Explore the following related architectures:

- Azure firewall architecture guide
- Firewall and Application Gateway for virtual networks
- Troubleshoot a hybrid VPN connection
- Spoke-to-spoke networking
- Baseline architecture for an Azure Kubernetes Service (AKS) cluster

Feedback

Was this page helpful? 👍 Yes 👎 No