Network Architecture Guidance for Azure

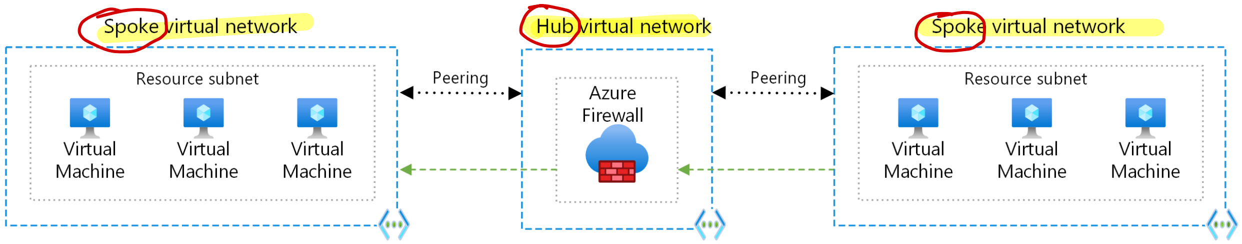
The following are some best practices when setting up and working with network resources in Azure Cloud environments.

> **Note:** When working in an existing cloud environment, it is important to understand any current patterns, and how they are used, before making a change to them. You should also work with the relevant stakeholders to make sure that any new patterns you introduce provide enough value to make the change.

Provide
- Network Security
- Monitory
- Connectivity on premise/ other cloud Env^n

Networking and VNet Setup

Hub-and-Spoke Topology



A hub-and-spoke network topology is a common architecture pattern used in Azure for organizing and managing network resources. It is based on the concept of a central hub that connects to various spoke networks. This model is particularly useful for organizing resources, maintaining security, and simplifying network management.

The hub-and-spoke model is implemented using Azure Virtual Networks (VNet) and VNet peering.

- The hub: The central VNet acts as a hub, providing shared services such as network security, monitoring, and connectivity to on-premises or other cloud environments. Common components in the hub include Network Virtual Appliances (NVAs), Azure Firewall, VPN Gateway, and ExpressRoute Gateway.

- The spokes: The spoke VNets represent separate units or applications within an organization, each with its own set of resources and services. They connect to the hub through VNet peering, which allows for communication between the hub and spoke VNets.

Implementing a hub-and-spoke model in Azure offers several benefits:

- Isolation and segmentation: By dividing resources into separate spoke VNets, you can isolate and segment workloads, preventing any potential issues or security risks from affecting other parts of the network.
- Centralized management: The hub VNet acts as a single point of management for shared services, making it easier to maintain, monitor, and enforce policies across the network.
- Simplified connectivity: VNet peering enables seamless communication between the hub and spoke VNets without the need for complex routing or additional gateways, reducing latency and management overhead.
- Scalability: The hub-and-spoke model can easily scale to accommodate additional spokes as the organization grows or as new applications and services are introduced.
- Cost savings: By centralizing shared services in the hub, organizations can reduce the costs associated with deploying and managing multiple instances of the same services across different VNets.

Read more about hub-and-spoke topology

When deploying hub/spoke, it is recommended that you do so in connection with landing zones. This ensures consistency across all environments as well as guardrails to ensure a high level of security while giving developers freedom within development environments.

Firewall and Security

When using a hub-and-spoke topology it is possible to deploy a centralized firewall in the Hub that all outgoing traffic or traffic to/from certain VNets, this allows for centralized threat protection while minimizing costs.

DNS

The best practices for handling DNS in Azure, and in cloud environments in general, include using managed DNS services. Some of the benefits of using managed DNS services is that the resources are designed to be secure, easy to deploy and configure.

- **DNS forwarding:** Set up DNS forwarding between your on-premises DNS servers and Azure DNS servers for name resolution across environments.
- **Use Azure Private DNS zones for Azure resources:** Configure Azure Private DNS zones for your Azure resources to ensure name resolution is kept within the virtual network.

Read more about Hybrid/Multi-Cloud DNS infrastructure and Azure DNS infrastructure

IP Allocation

When allocating IP address spaces to Azure Virtual Networks (VNets), it's essential to follow best practices for proper management, and scalability.

Here are some recommendations for IP allocation to VNets:

- **Reserve IP addresses:** Reserve IP addresses in your address space for critical resources or services.
- **Public IP allocation:** Minimize the use of public IP addresses and use Azure Private Link when possible to access services over a private connection.
- **IP address management (IPAM):** Use IPAM solutions to manage and track IP address allocation across your hybrid environment.
- **Plan your address space:** Choose an appropriate private address space (from RFC 1918) for your VNets that is large enough to accommodate future growth. Avoid overlapping with on-premises or other cloud networks.
- **Use CIDR notation:** Use Classless Inter-Domain Routing (CIDR) notation to define the VNet address space, which allows more efficient allocation and prevents wasting IP addresses.
- **Use subnets:** Divide your VNets into smaller subnets based on security, application, or environment requirements. This allows for better network management and security.
- **Consider leaving a buffer between VNets:** While it's not strictly necessary, leaving a buffer between VNets can be beneficial in some cases, especially when you anticipate future growth or when you might need to merge VNets. This can help avoid re-addressing conflicts when expanding or merging networks.
- **Reserve IP addresses:** Reserve a range of IP addresses within your VNet address space for critical resources or services. This ensures that they

have a static IP address, which is essential for specific services or applications.
- **Plan for hybrid scenarios:** If you're working in a hybrid environment with on-premises or multi-cloud networks, ensure that you plan for IP address allocation across all environments. This includes avoiding overlapping address spaces and reserving IP addresses for specific resources like VPN gateways or ExpressRoute circuits.

Read more at azure-best-practices/plan-for-ip-addressing

Resource Allocation

For resource allocation the best practices from Cloud Resource Design Guidance should be followed.

Last update: August 26, 2024