CHAPTER 3

Network Security Patterns

Organizations typically focus on building applications and data-driven software to harvest value from thier data. An enterprise segmentation strategy helps technical teams create isolation across networks, applications, and identity-management systems.

The previous chapter explained how to set up Identity and Access Management (IAM) with Azure Active Directory (AAD).

This chapter covers the following topics:

- Software-defined networks (SDNs)
- Network topologies
- Segmenting subnets
- Controlling routing behavior
- Using gateways and firewalls

Software-Defined Networks (SDNs)

Software-defined networking is an architecture that's designed to centrally govern, manage, and configure virtual networking functionality with the help of software. Using SDNs, you can create cloud-based networks with routers, firewalls, and on-premises networks. See Figure 3-1.

S. Lad, *Azure Security For Critical Workloads*, https://doi.org/10.1007/978-1-4842-8936-5_3

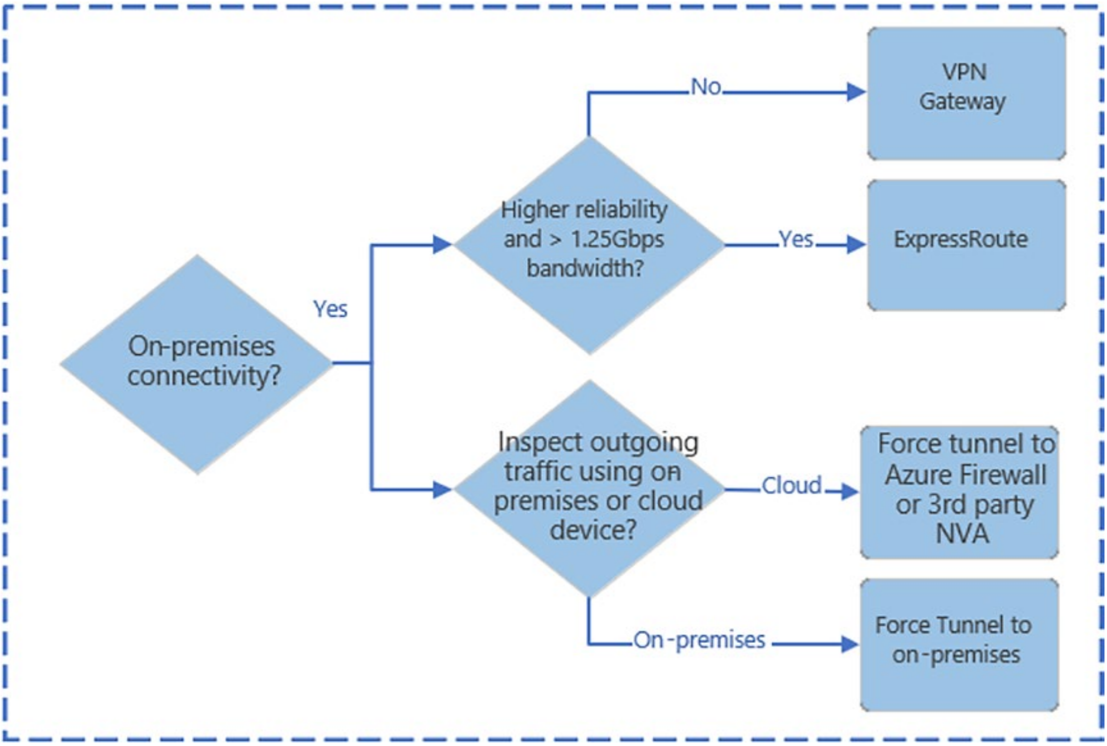

On-premises connectivity?
Yes
Higher reliability and > 1.25Gbps bandwidth?
No
VPN Gateway
Yes
ExpressRoute
Inspect outgoing traffic using on premises or cloud device?
Cloud
Force tunnel to Azure Firewall or 3rd party NVA
On-premises
Force Tunnel to on-premises

Figure 3-1. *Networking decision guide*

SDNs provide various options with differing prices and complexity. There are many ways to implement SDN technologies to create cloud-based virtual networks. Based on your governance requirements, you can structure the virtual networks for migration and interact with an existing IT infrastructure.

Types of virtual networking architectures:

- PaaS: All the PaaS products have limited built-in networking features. So, in most cases, you don't have to specify the software-defined network to support the workload requirements.

- Cloud-native: A cloud-native architecture supports cloud-based workloads using the virtual network that's built on top of the default software-defined networking capabilities. See Figure 3-2.

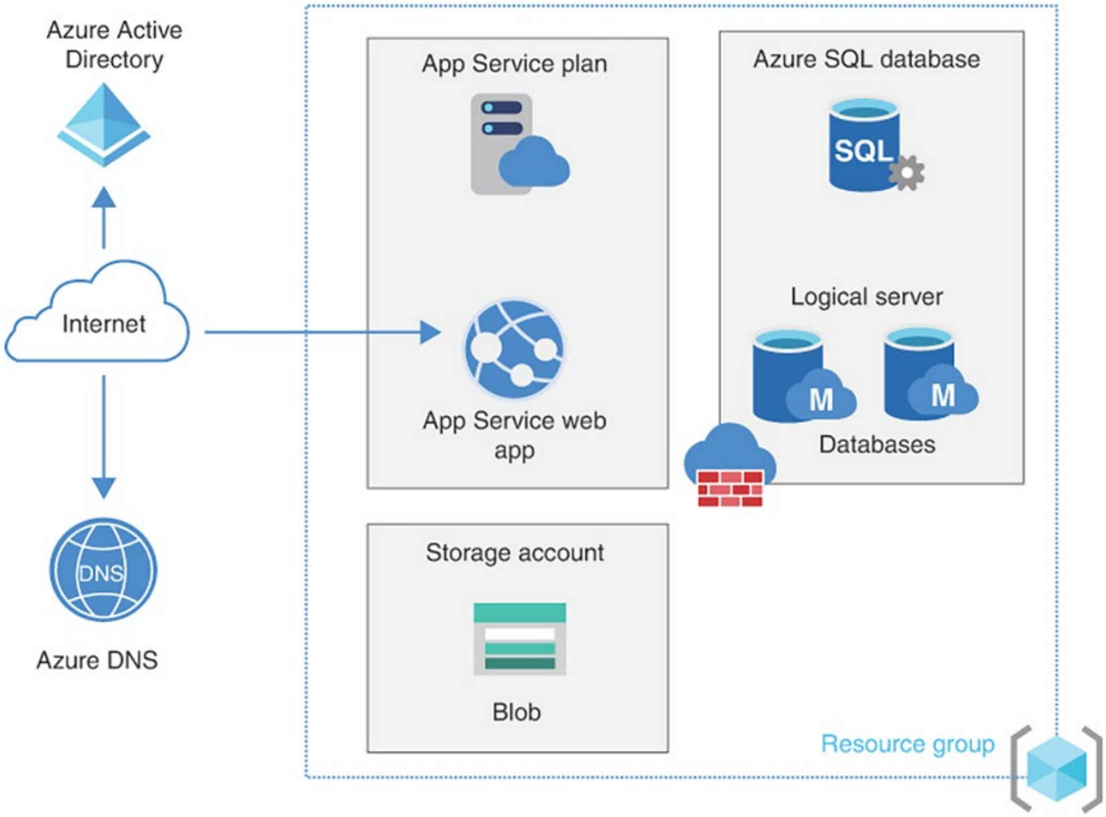


Figure 3-2. *Cloud-native architecture*

- Cloud Dematerialized Zone (DMZ): This cloud DMZ has limited connectivity between the on-premises and cloud networks, secured through a network implementation that controls the traffic between the environments. See Figure 3-3.

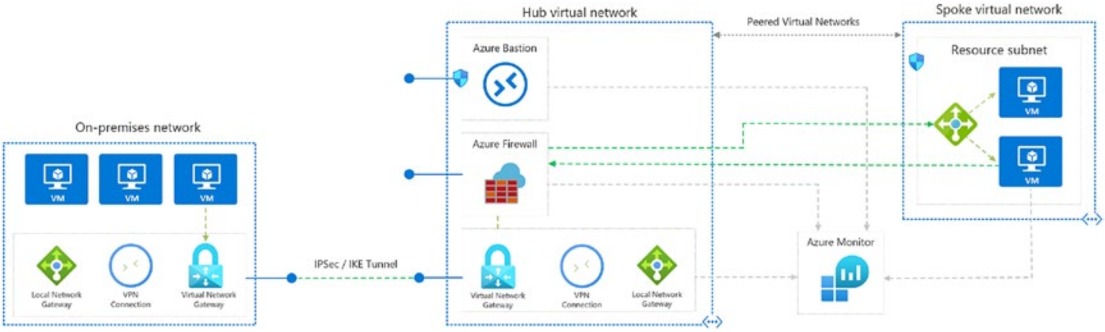


Figure 3-3. *Cloud DMZ*

- Hybrid: A hybrid cloud architecture allows virtual networks in the trusted cloud environments to access the on-premises resources as well as the cloud resources. See Figure 3-4.

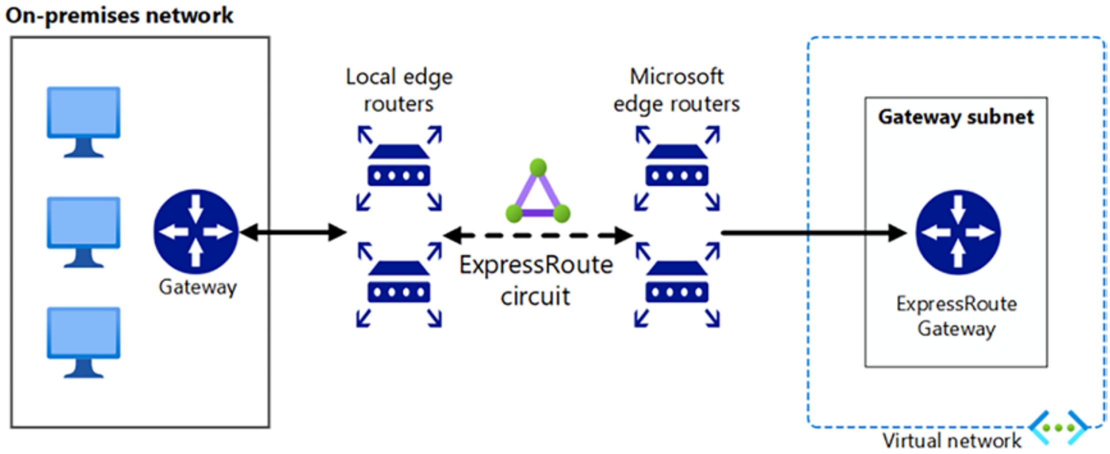


Figure 3-4. *Hybrid Virtual Network*

- Hub and spoke: This architecture centrally manages external connectivity and shared services to overcome potential subscription limits. See Figure 3-5.

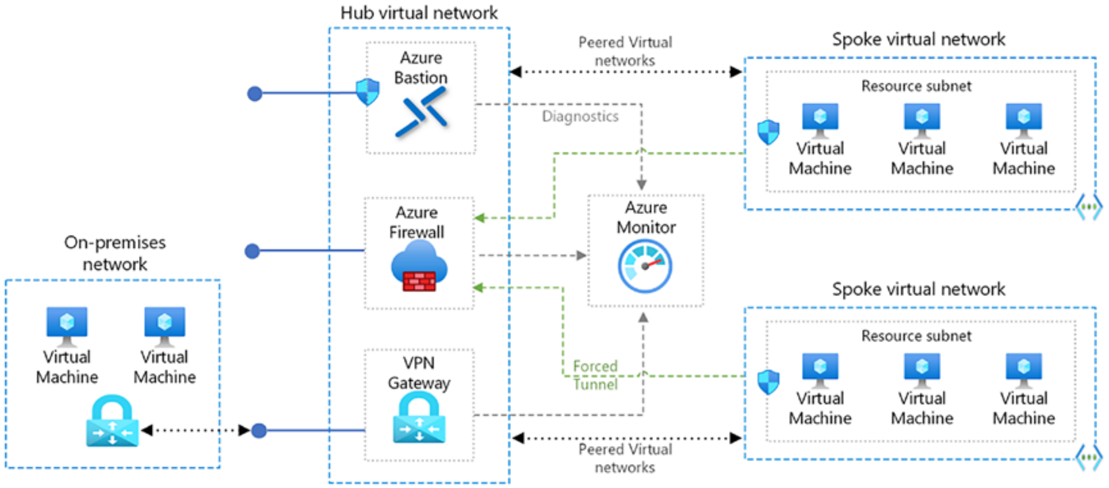


Figure 3-5. *Hub and spoke model*

- Hub and spoke organizes Azure-based cloud network infrastructure into multiple connected virtual networks. The hub is a virtual network that acts as a central location to manage external connectivity. The spokes are virtual networks that host the workloads and connect to the central hub using *virtual network peering.*

Network Topologies

Network topology is the arrangement of a network consisting of nodes and how they connect to the sender and receiver. Let's look at the various topologies in detail.

Mesh Topology

In a mesh topology, every device is connected to another device using a specific channel. Mesh topology protocols used are AHCP (Ad Hoc Configuration Protocols) and DHCP (Dynamic Host Configuration Protocol). See Figure 3-6.

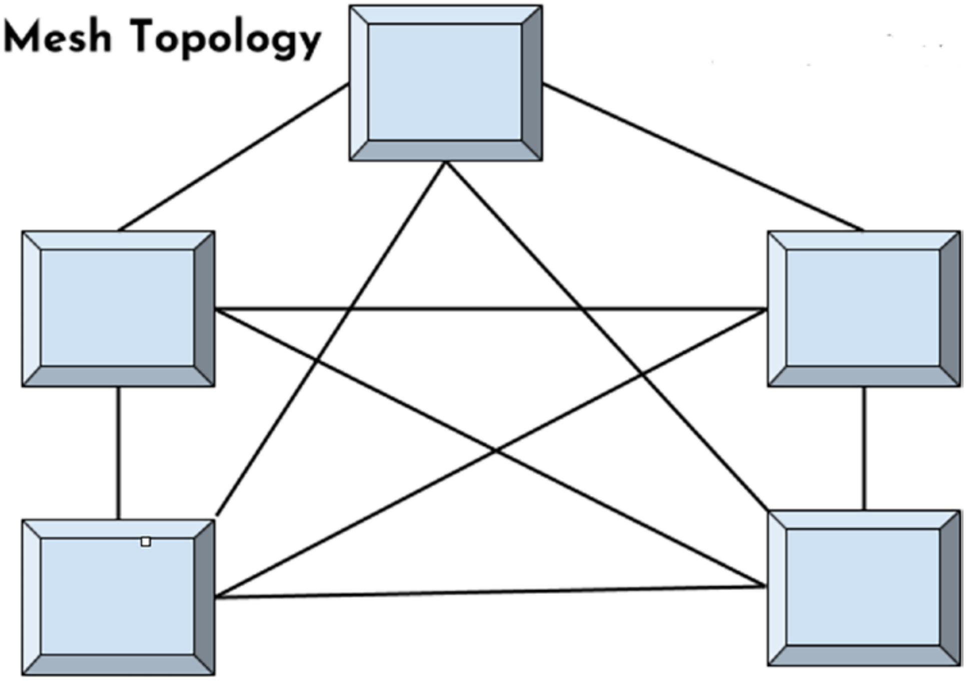


Figure 3-6. *Mesh topology*

Star Topology

In a star topology, all the devices are connected to a single hub using the cable. This hub is a central node and all other nodes are connected to it. Various popular protocols used in the star topology are as follows:

- Collision Detection (CD)
- Carrier Sense Multiple Access (CSMA)

One major problem with the star topology is that if the concentrator or connector fails, the whole system will crash. The cost of installing the star topology is also very high. The overall performance of the star topology is based on that single concentrator. See Figure 3-7.

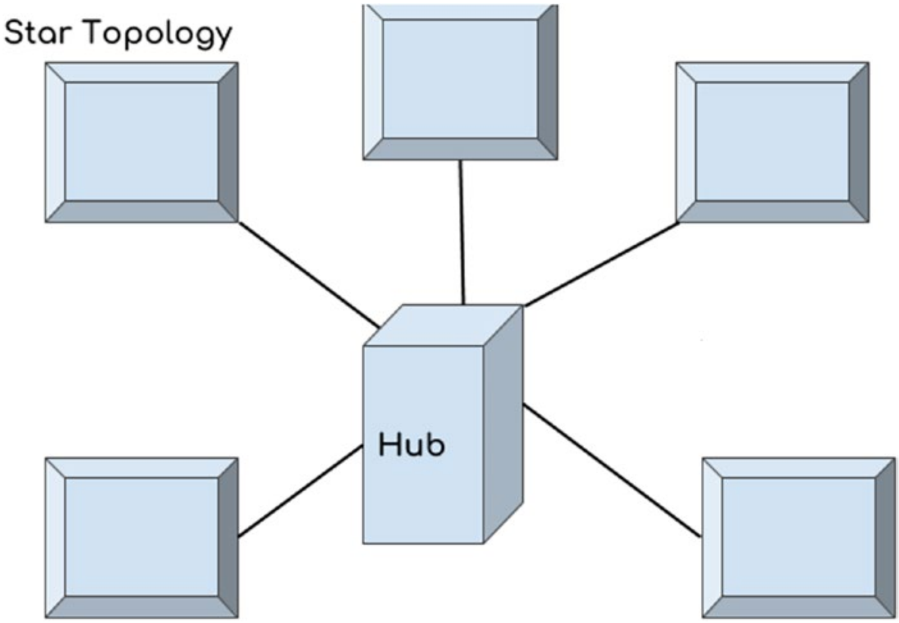


Figure 3-7. *Star topology*

Bus Topology

A bus topology is a type of network in which every computer and network device is connected to a single cable. A bus topology transmits data from one end to the other end in a single direction. See Figure 3-8.

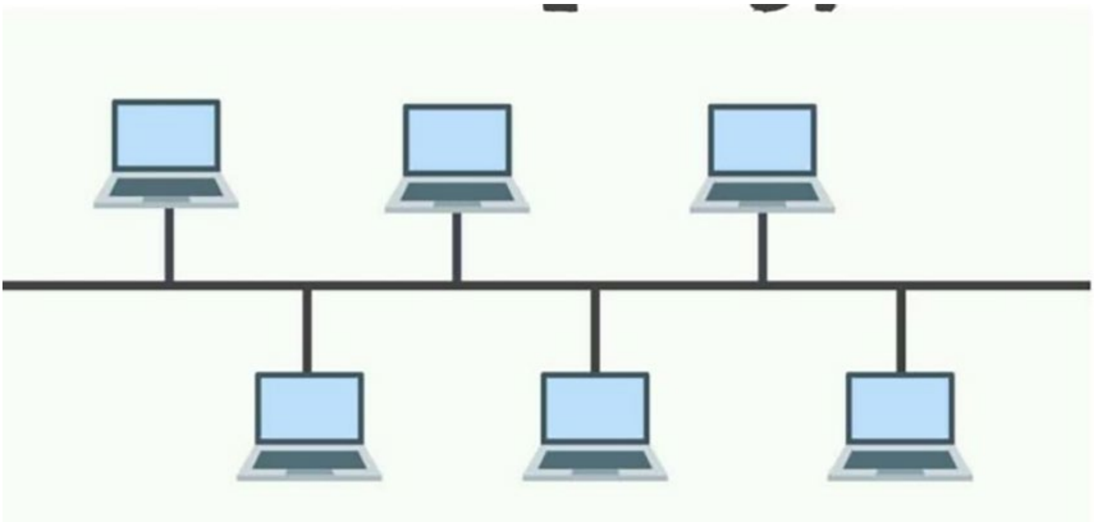


Figure 3-8. *Bus topology*

Ring Topology

This topology forms a ring by connecting a device to its two neighboring devices. In this topology, a number of repeaters are used with a large number of nodes. This is because, for example, if data has to be sent to 100 nodes, it has to pass through 99 nodes. This data transmission is unidirectional. See Figure 3-9.

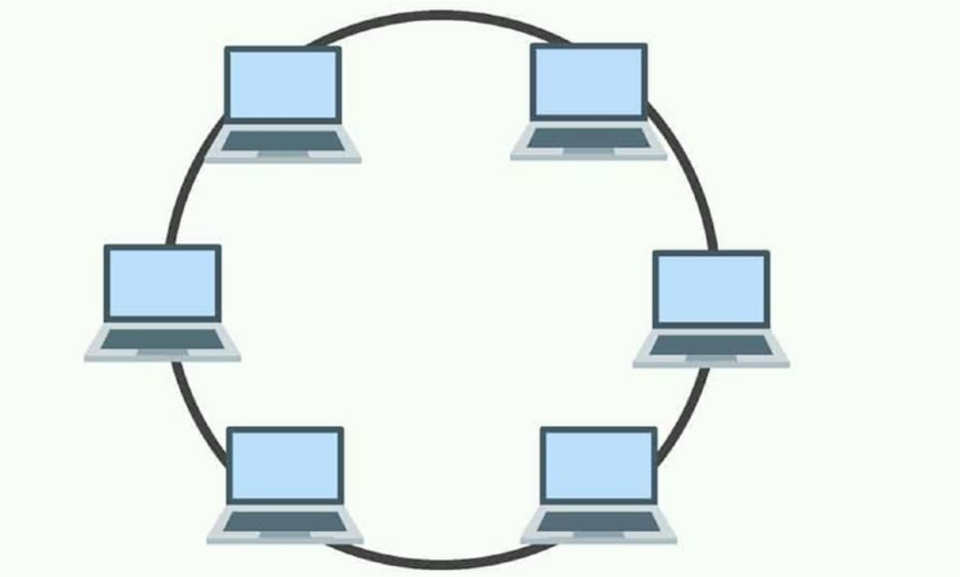


Figure 3-9. *Ring topology*

Tree Topology

Tree topology is a variation of star topology that has a hierarchical flow of data. This topology uses SAC (standard automatic configuration) protocols like DHCP. One major problem with the tree topology is that, if the central hub fails, the entire system fails and its cost is very high because of the cabling. It allows more devices to be attached to a single central hub. This way it decreases the distance travelled by the signal. See Figure 3-10.

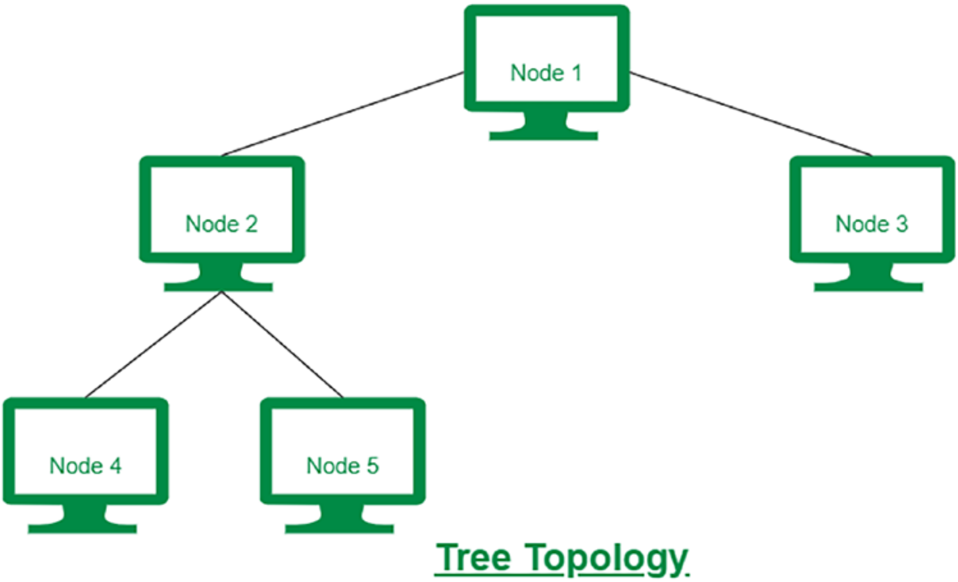


Figure 3-10. *Tree topology*

Hybrid Topology

A hybrid topology is a combination of various types of topologies. It is mainly used when the nodes are free to take any form. In a hybrid topology, each individual topology uses its specific protocol to get the work done. See Figure 3-11.

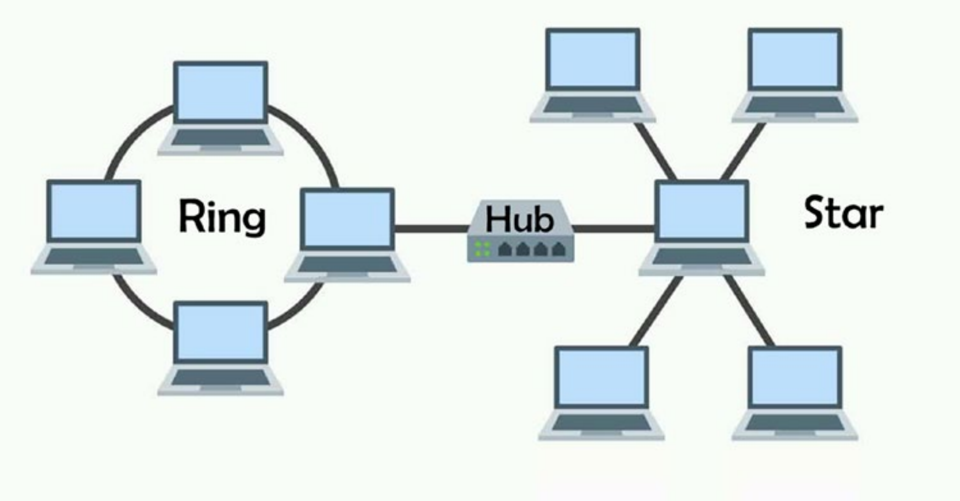


Figure 3-11. *Hybrid topology*

Segmenting Subnets

Enterprises need to create a strategy to consistently segment access to the application and data using the network, applications, and data and access controls. The main reasons for segmenting are as follows (see Figure 3-12):

- Group together similar assets that are part of the workload or application development
- Separate resources to improve security
- Set up and comply with governance policy as per the organization's standards

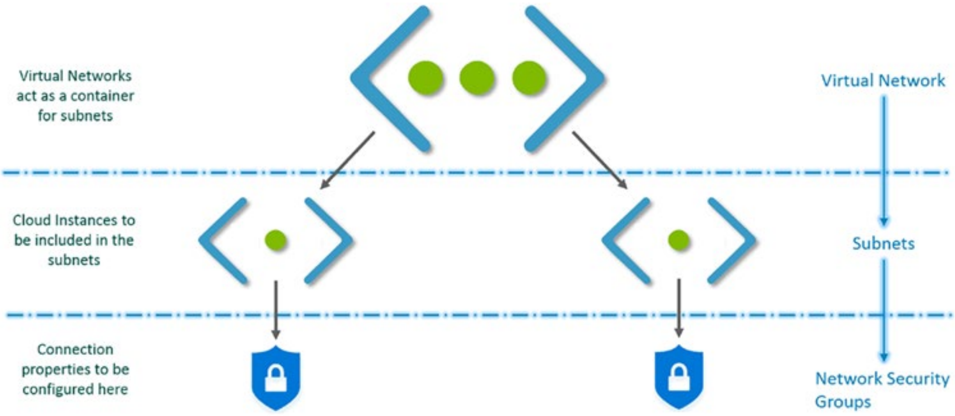

Virtual Networks act as a container for subnets
Virtual Network
Cloud Instances to be included in the subnets
Subnets
Connection properties to be configured here
Network Security Groups

Figure 3-12. *Network segmentation*

With segmentation, you can create software-defined perimeters using various Azure services and features. When an application is placed in a separate segment, traffic between the segments will be controlled to secure the communication paths. The main advantage of segmentation is that, even if the segmentation is compromised, it will not affect the rest of the network.

When working with Azure, there are various segmentation options available:

- Azure subscription: Creates logical boundaries between the large teams/organizations within the company. This ensures that communication between the resources is provisioned explicitly. See Figure 3-13.

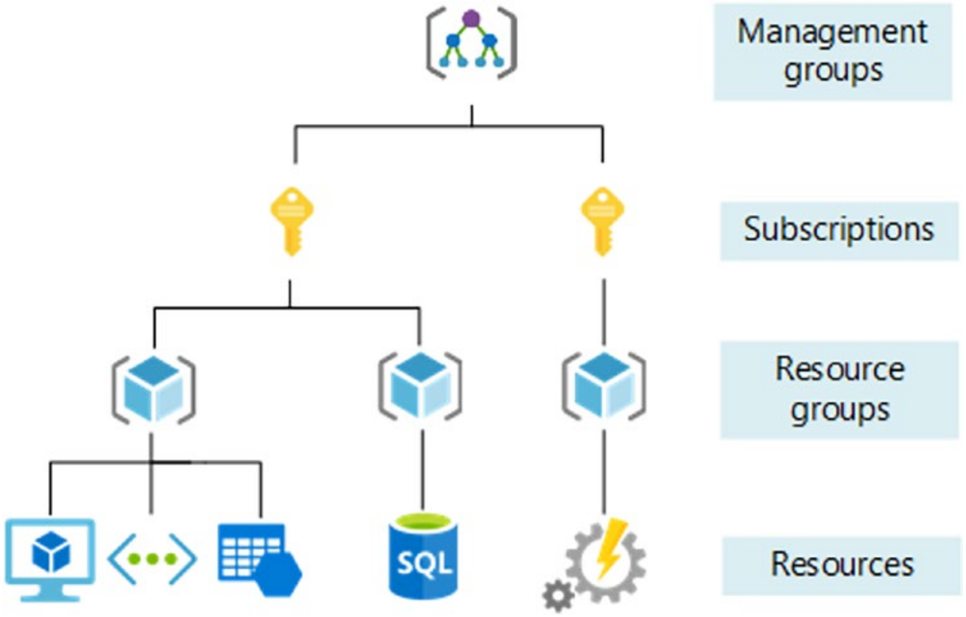


Figure 3-13. *Azure subscriptions*

- Virtual Network: Azure Virtual Network is a fundamental building block that creates a private network within the Azure environment. With VNET, you can enable many types of resources, such as Azure Virtual Machines, to securely communicate between the on-premises resources and any Internet resources. See Figure 3-14.

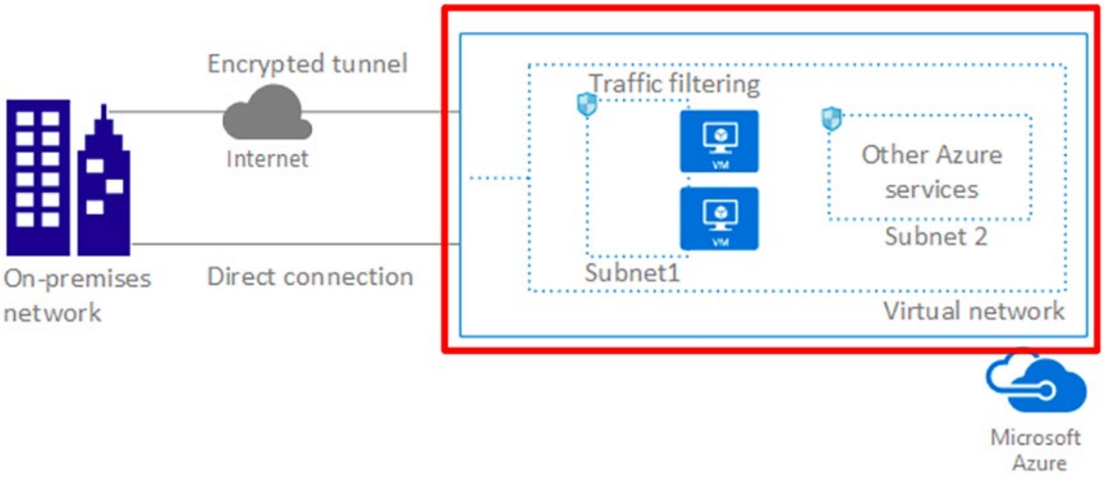


Figure 3-14. *Azure Virtual Network*

- Network Security Group(NSG): With NSGs, you can control traffic between resources within and outside the virtual network. You can also maintain granular access control by creating a separate logical environment for subnets, VMs, or group of VMs. See Figure 3-15.

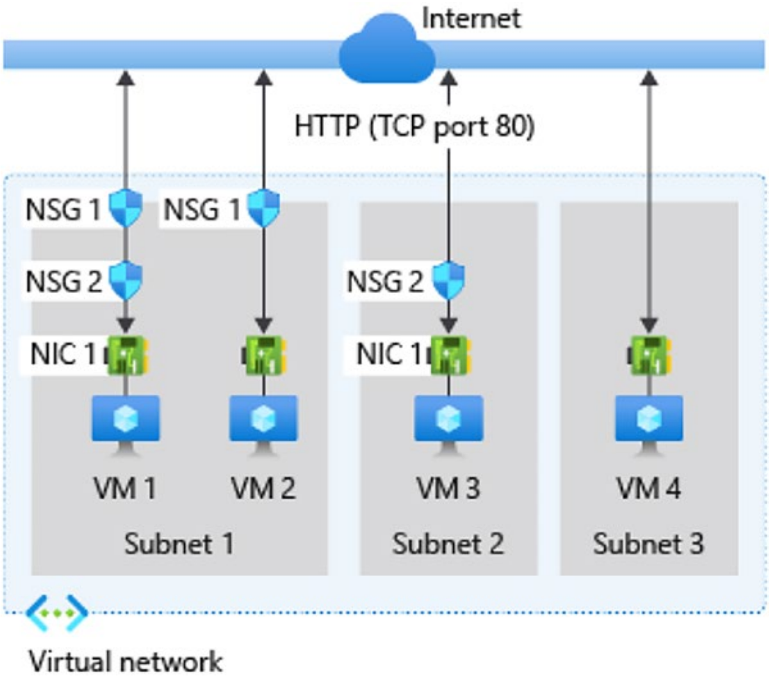
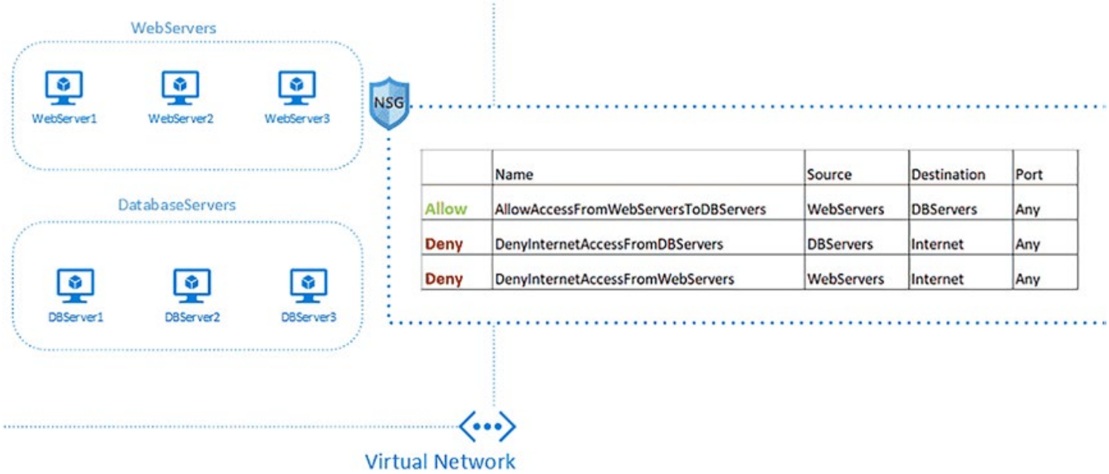


Figure 3-15. *Network security group*

- Application Security Group (ASG): Application Security Groups are the same as Network Security Groups, but they are referenced with respect to the application context. This allows groups of VMs under the application tag and defines the rules for each underlying VM. See Figure 3-16.



	Name	Source	Destination	Port
Allow	AllowAccessFromWebServersToDBServers	WebServers	DBServers	Any
Deny	DenyInternetAccessFromDBServers	DBServers	Internet	Any
Deny	DenyInternetAccessFromWebServers	WebServers	Internet	Any

Figure 3-16. *Application security group*

- Azure Firewall: Azure has a cloud-native firewall that can be deployed to a virtual network or an Azure virtual WAN. It filters the traffic between the cloud resources, the Internet, and the on-premises server/resources. With Azure Firewall, you can create rules and policies and specify allow/deny traffic rules using layer 3 to layer 7 controls. You can also filter the traffic. See Figure 3-17.

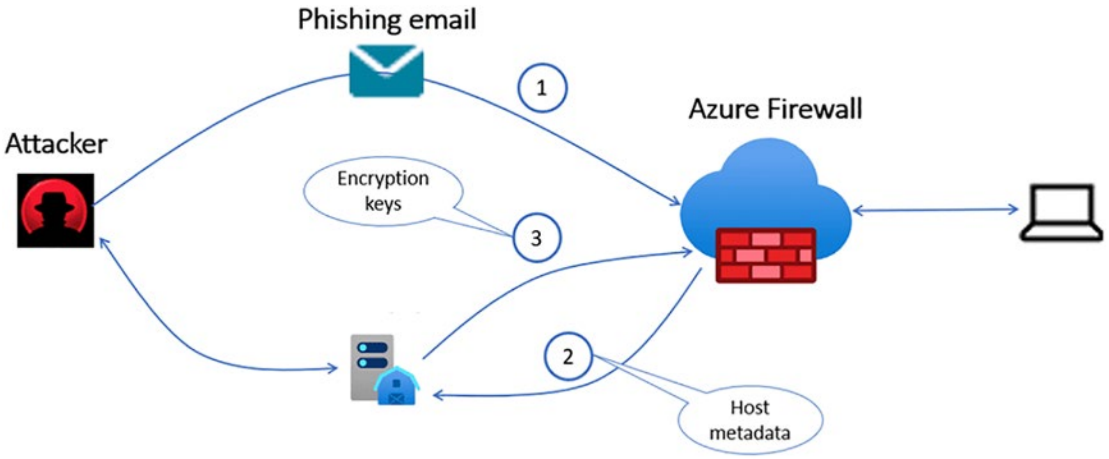


Figure 3-17. *Azure Firewall*

There are various standard segmentation patterns that isolate and secure workloads in Azure from a networking point of view. Let's explore these various standard patterns in detail and discuss which one is best from an organizational point of view.

- Single VNET: With a single VNET, all the application components reside in a single virtual network. When you are working in a single region and VNET can't span across multiple regions, you can use the single VNET approach. See Figure 3-18.

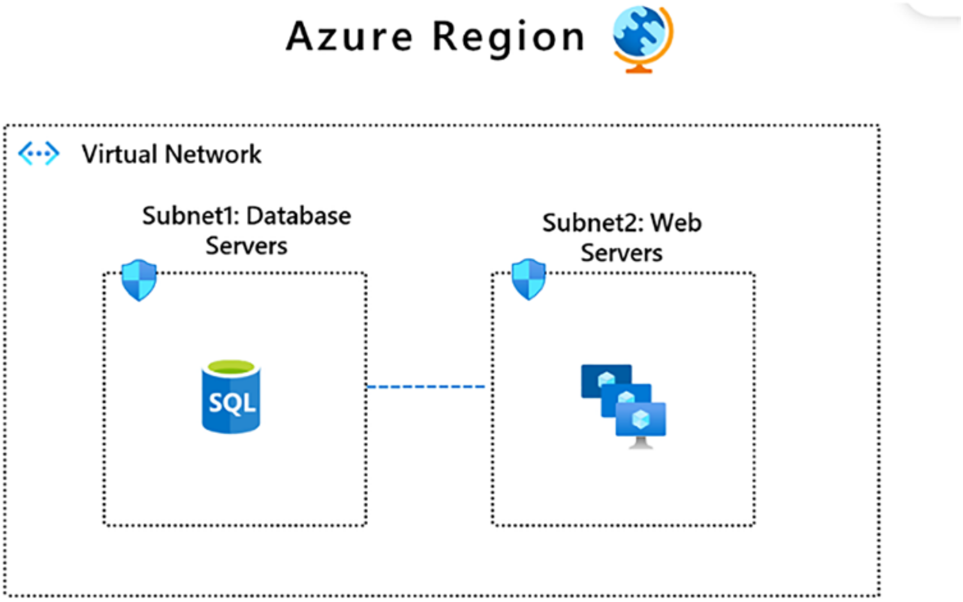


Figure 3-18. *Single VNET*

- Common ways to segment subnets or application groups include using the Network Security Groups and Application Security Groups. In Figure 3-18, Subnet 1 uses a SQL database and Subnet 2 uses Azure VMs. You can configure NSG to allow the communication between Subnet 1 and Subnet 2.

- Multiple VNET with VNET peering: Using the multiple VNET approach, you can spread resources across multiple VNETs. You can enable communication across the VNETs using VNET peering. VNET peering is recommended when you need to group applications in separate VNETs. When you use VNET peering, connecting between VNETs is not transitive. See Figure 3-19.

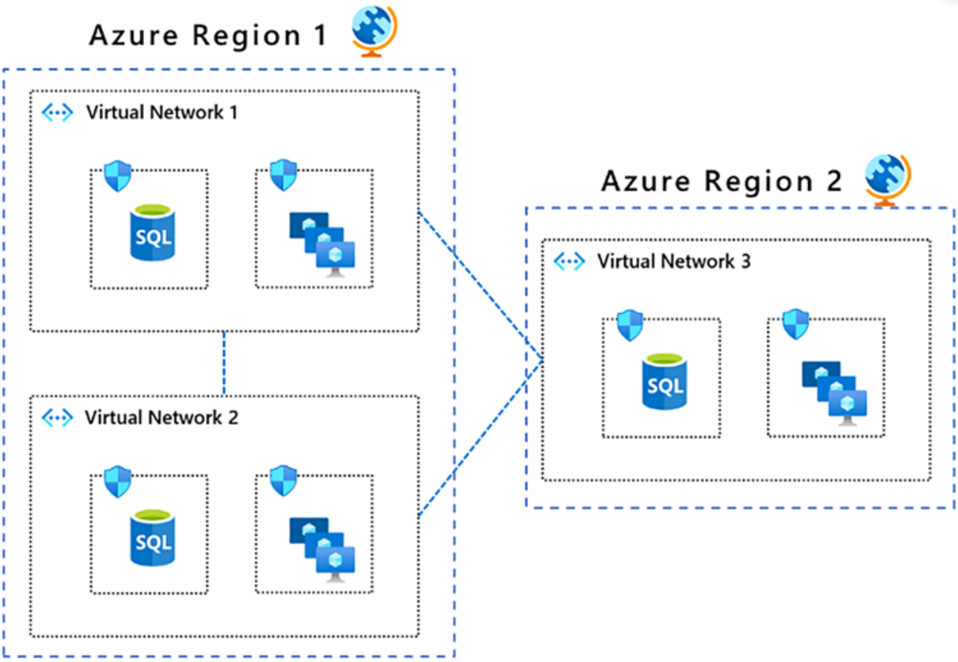


Figure 3-19. *Multiple VNETs with peering*

Controlling Routing Behavior

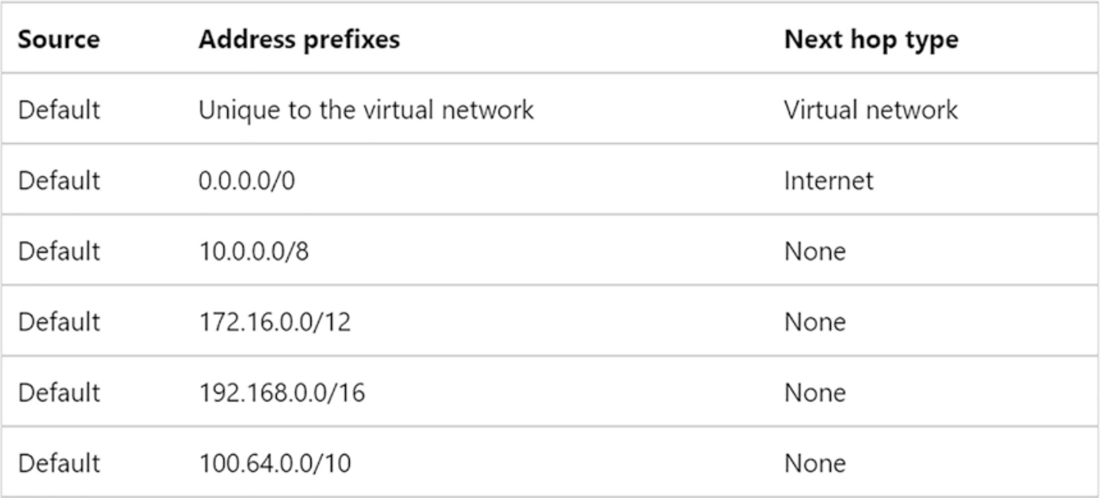
When you set up a virtual network for an application, you can determine the traffic between the services and within the virtual network by controlling the routing behavior. When you create a virtual network, you have default routes that will be enabled to allow that communication. In many cases, these default routes are sufficient to control the traffic within the VNET. If customization is required, you can customize the networking routes

Let's look at the concepts of routing the network traffic:

- System routes: Azure automatically creates a system route and assigns the routes to each subnet within a virtual network. Since these system routes are created by default, you can't create them and you don't have permission to remove them. But you can change or override the existing system routes using the custom routes. Azure creates default system routes for each subnet and it adds optional default routes to specific subnets using the Azure capabilities.

- Default routes: Each default route contains an address prefix and the next hop type. Whenever a virtual network is created, Azure automatically creates the default system routes listed in Table 3-1.

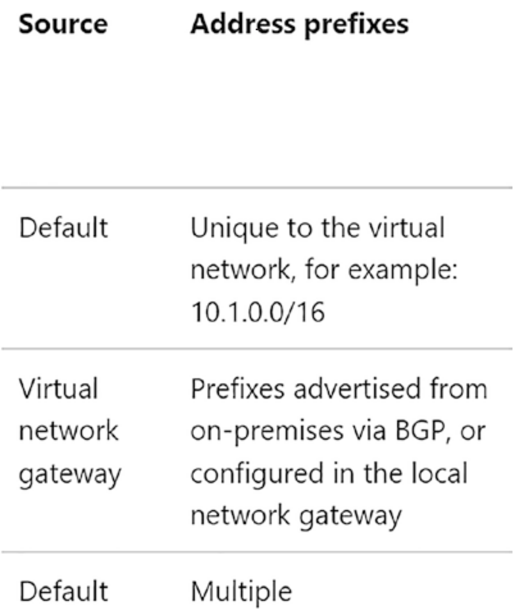
Table 3-1. *Default Routing Rules*



Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	172.16.0.0/12	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

- Apart from the default routes, there are various other optional routes that can be configured. Depending on the capability, Azure adds optional default routes to specific subnets or to all subnets in the virtual network. See Table 3-2.

Table 3-2. Optional Default Routes



Source	Address prefixes
Default	Unique to the virtual network, for example: 10.1.0.0/16
Virtual network gateway	Prefixes advertised from on-premises via BGP, or configured in the local network gateway
Default	Multiple

- Custom routes: You can create custom routes either by creating user-defined routes or by exchanging the Border Gateway Protocol (BGP) between the on-premises network gateway and the Azure network gateway.
- User-defined routes: You can create user-defined routes in Azure to override Azure's default system routes or add more routes to the subnet's route table. You can create a route table and an associate route table to zero or more virtual network subnets.
- Border Gateway Protocol (BGP): On-premises network gateway can exchange routes with the cloud Azure network gateway using the Border Gateway Protocol. Using BGP with an Azure virtual network depends on the type of gateway. When you exchange routes with Azure using BGP, a separate route is added to the route table of all the subnets in the virtual network. See Figure 3-20.

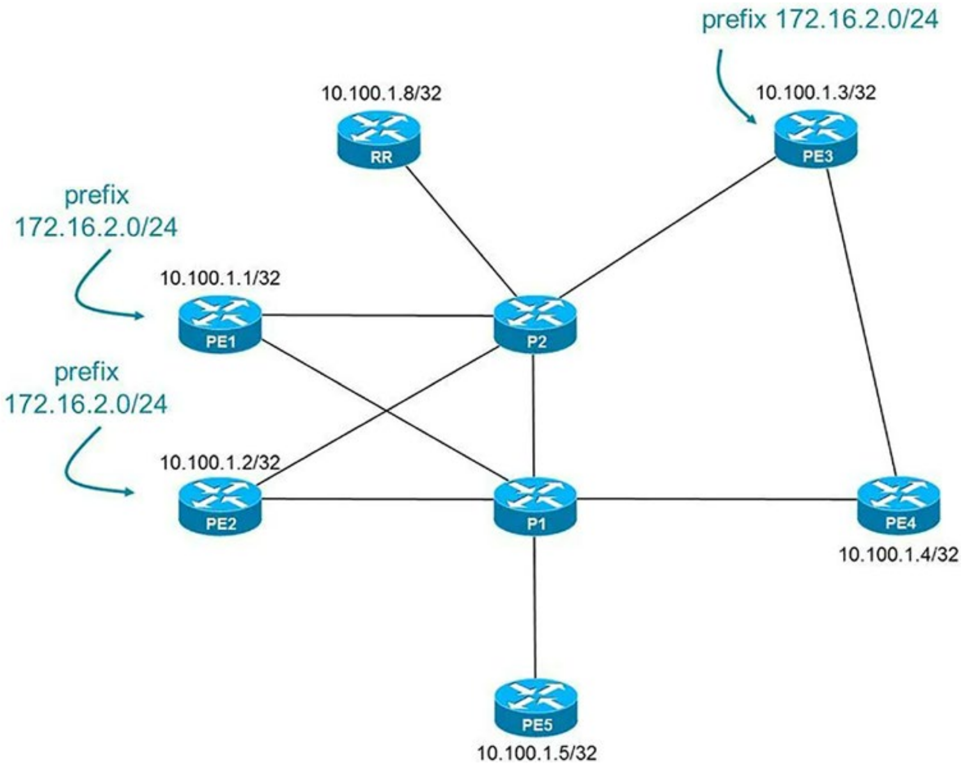


Figure 3-20. *Border Gateway Protocol*

VPN Gateway route propagation can be disabled on a subnet using the route table. Connectivity with VPN connection is achieved using the custom routes with the Virtual Network Gateway.

Using Gateways and Firewalls

In order to secure your Azure application workload, you have to make sure that all security measures—including authentication, authorization, and encryption—are properly in place. You can add security layers to the virtual machine where the application is hosted and deployed. These layers protect inbound flow from the users.

Azure Firewall is a next-generation firewall that provides network address translation. It is an intelligent firewall security and it provides the best of threat protection for the workload running in the cloud.

Azure Firewall standard provides L3-L7 filtering and threat intelligence directly from Microsoft Cyber Security. Azure Firewall Premium has advanced capabilities compared to Azure Firewall. These advanced capabilities include byte sequence in network traffic or attacks done by the antivirus or malware software.

You can properly govern and manage Azure Firewall across multiple subscriptions using the Azure Firewall Manager. With the Firewall Manager, you can apply the firewall policy to apply common network rules in the Azure AD Tenant. The Firewall Manager can support firewalls in both VNET and Virtual WANs. Azure Firewall is based on the five pillars of the architectural excellence:

- Reliability
- Security
- Cost optimization
- Operational excellence
- Performance excellence

Azure Application Gateway is a load balancer that helps you control and manage the traffic of web applications. With the application gateway, you can make routing decisions based on the HTTP requests.

With Azure Application Gateway, you can perform URL-based routing. You can enable Secure Socket Layer (SSL)/Transport Layer Security (TLS) gateways, auto-scaling, zone redundancy, static VIPs, and web application firewalls by enabling the application gateway.

Conclusion

This chapter explored in detail the software-defined networks and the approach to be followed by an enterprise organization. You also learned about various network topologies and how to use subnets in the virtual network to isolate the network traffic. You also learned that you can control and route traffic using the NSG rules and ASG.