**Azure Networking Fundamentals**

What is a VNet?

A Virtual Network, or a VNet, is an isolated network within the Microsoft Azure cloud. A VNet in Azure provides a range of networking functions comparable to AWS Virtual Private Cloud (VPC). These functions include DNS, routing, enabling customization of DHCP blocks, access control, connectivity between virtual machines (VM) and virtual private networks (VPN).

An Azure VNet is a representation of a network in the cloud and is logical isolation of the Azure cloud dedicated to a subscription. In the background, it’s a software abstraction of a network that overlays Azure’s infrastructure to provide isolation from resources outside of the VNet, practically making it a private network. But that doesn’t mean the VNet can’t be connected. It can be linked with other VNets in Azure or connected on-premises infrastructure to create hybrid systems. Operationally, a VNet follows common IP routing principles to connection resources inside. So, it needs to have one or more address spaces associated with it (CIDR), which can be segmented into subnets, within which resources will reside.

VNets can be used to:

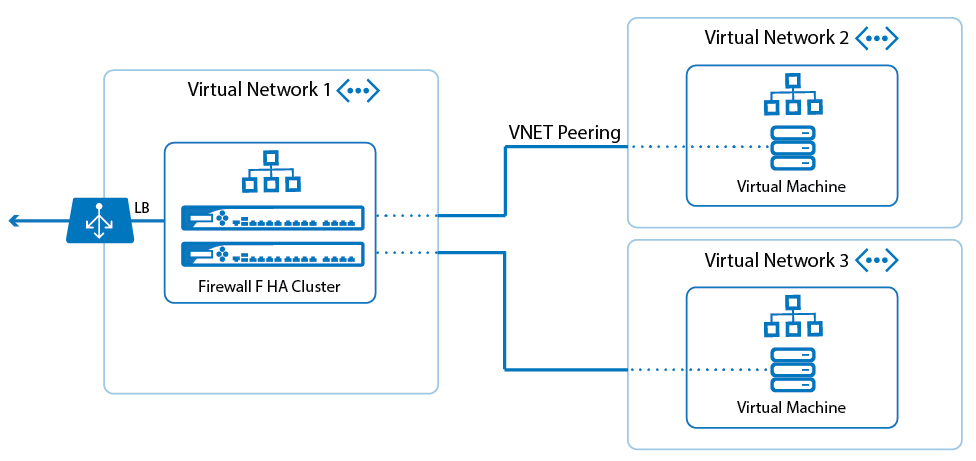
* Create a dedicated private cloud-only VNet to allow services and VMs within the VNet to communicate directly and securely in the cloud.
* Securely extend a data center, by building traditional site-to-site (S2S) VPNs, to securely scale capacity.
* Deploy hybrid clouds by securely connecting cloud-based applications to on-premises systems.

Key components of Azure VNets, include:

* **Subnets**: Divide a VNet into subnets or configure routing tables and Network Security Groups (NSG) to a subnet.
* **IP addresses**: Assign public or private IP addresses to an Azure VNet.
  + Use public IP address for public-facing communications. A dynamic IP will be assigned.
  + Use private IP address for connectivity within a VNet when using a VPN gateway or ExpressRoute. A dynamic IP assignment is a default, but a static IP can also be assigned.
* **Network Security Groups (NSG)**: Use to permit or deny traffic, via rules, to a subnet or network interface.
* **Firewall**: Azure offers a managed Firewall service that provides the ability to define L3-7 connectivity policies for granular control of what enters and leaves the network
* **Load balancing**: Three load balancing solutions offered by Azure include:
  + Azure Traffic Manager – comparable to Route53 in AWS
  + Azure Load Balancer
  + Azure Application Gateway
* **Routing tables**: As with general routing, anytime traffic needs to leave a subnet, it needs a routing function to forward packets to other subnets and networks. A router does this using a routing table, and that route table configuration is exposed in Azure for customized configuration. Route table can have rules that define where traffic should be sent to, i.e a virtual network, virtual network gateway or virtual machine. A User Defined Route, or UDR, can be used to forward traffic to a different VNet. This can be a powerful tool to build a connection between hubs.

Azure vNet Overview

Resources in the Azure cloud, such as VMs, still require some form of networking solution for communication with other resources. While you could have one giant network per a cloud customer, that would severely limit the flexibility of cloud use cases. There is a need for a logical construct to which resources are bound. Since everything still talks through a network, this is commonly done using a virtual network space in the cloud. for Azure, that’s called Azure Virtual Network or VNet. It allows many types of Azure resources to reside inside a VNet, such as Azure virtual machines (VMs). A VNet can be broken down to single or multiple subnets as well. It can then allow them to communicate securely with each other, with the Internet, and with local networks. The scope of a virtual network is a single region; however, several virtual networks of different regions can be connected together by virtual network peering as shown below:



Azure Virtual Network provides the following important functionalities:

##### **Isolation and segmentation**

You can deploy multiple virtual networks within each subscription and Azure region. Each virtual network is isolated from the other virtual networks by default.

* Specify a private IP address space through public and private addresses (RFC 1918). Azure assigns a private IP address to the resources of a virtual network from the address space that you assign.
* Segment the virtual network into one or more subnets and assign a part of the address space of the virtual network for each subnet.
* Use the name resolution provided by Azure or specify your own DNS server to be used by resources connected to a virtual network.

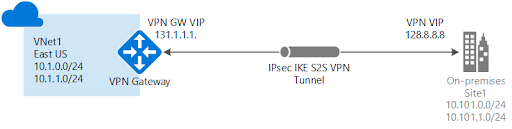
##### **Security and Traffic Control Policy**

You can filter network traffic between subnets using one or both of the following options:

* **Network Security Groups (NSG)**: Network security groups, NSG for short, is a container of the ruleset that contains one or more rulesets that dictates what type of traffic is allowed arriving and leaving the resources. Each individual rule can source, destination, protocol, and action. Source and destination can be IP address, VNet, or an Application Security Group.
* **Application Security Group (ASG)**: ASGs enable source/destination definition based on a label, rather than IP/network address. An ASG in and of itself is not actually a policy group, but rather an arbitrary definition that can be applied to resources, such as “AppServer”, “DataBase”, “myApp”, etc. This definition can later be used in rule inside an NSG. This is useful when a rule needs to be applied to resources based on their purpose, rather than their IP CIDR, which offers greater flexibility in policy application
* **Azure Managed Firewall**: Azure provides a managed firewall that controls traffic between the VNet and internet. This firewall is meant to protect internet facing conversation. It is important to note that this firewall requires in its own subnet, and forwards traffic to other resources using internal routing.
* **Virtual network Appliance**: Optional, for integration of 3rd party solutions, a virtual network appliance can be inserted into a VNet. This appliance is a virtual machine that executes a network function, such as a firewall, WAN optimization or other network function. To see a list of virtual network applications that can be deployed in a virtual network, see Azure Marketplace.

#### VPN with VNET

It is very common, if not ubiquitous, to need to have the cloud resources connect to On-Premises or other cloud resources. This is normally achieved by setting up a Virtual Private Network (VPN) between the two environments. As mentioned earlier, Azure VNet supports VPN connectivity as well. Such connectivity can be built between different VNets, or from a VNet to On-premises as shown in the picture below.



Source: Microsoft

Azure support various VPN modes, such as Site-Site, Point-Site, Policy-based and Route-based. This gives the cloud user flexibility to choose the best option for their tunnel according to their use cases and endpoint devices. There a couple of key components involved in the setup:

* **Virtual Network Gateway**: Virtual Network Gateway sits on the boundary of a VNet’s subnet and enables connectivity between that subnet and other networks or VPNs. This is where most of the VPN configuration resides.
* **Local Network Gateway**: Local Network Gateway is a representation of customers gateway on the other end of the tunnel. This simply holds configuration that tunnel needs to know about to build a VPN tunnel to the other end
* **Border Gateway Protocol (BGP)**: When setting up a hybrid cloud, we need to ensure that both ends of connection know about networks that reside on the other end. While static routing is an option, it normally isn’t the most suitable approach for a production network. In order to learn on-prem routes efficiently, there is a need for a routing protocol to communicate routes dynamically. BGP is the defacto choice of today, and Azure supports BGP over IPSec with route-based VPN options. With BGP running on top of you Azure VPN Gateway or ExpressRoute connection, you can propagate local BGP routes across your cloud and on-prem routers without the need for manual admin intervention. More information about the use of BGP with Azure VPN Gateway and ExpressRoute.