**Azure Virtual Network**

* A Vnet is the fundamental building block for a private network in Azure. Vnets allow azure

resources like VMs to communicate securely to each other, to the internet and on-premises networks. A Vnet is the representation of our own network in the cloud. We can logically isolate resources within our Vnet.

**Benefits of Vnet**

1. Isolation – As discussed, the components of a Vnet are isolated. We can connect to other Vnets or On Premises with Vnet Peering or VPN or Express route
2. Access to the public network
3. Access to VMs within the Vnet
4. Name resolution – We can resolve to other components in the Vnet and address them
5. Security – We can secure the components at various levels in the Vnet
6. Connectivity

Components of Vnets

* IP addresses
  + Public and private IP addresses
    - The Vnets are configured with a range of IP addresses. The Notation is in CIDR.
    - By default, Private IP addresses are assigned to the resources with which communication takes place between the resources
    - Optionally, Public IP address can be assigned to the resources
    - Please note that we will pay for Public IPs if they are not assigned. This is to conserve Public Ips
* Subnets
  + A Subnet is a subcomponent of Vnet. All resources must exist in a subnet.
  + A default subnet is created when a Vnet is created.
  + Access can be restricted at a subnet level also
  + Let's say we have 2 tiers in an application called Front end and Back end. We can create 2 subnets and configure access in such a way that internet traffic will flow to the front end subnet and from there to the back end subnet.
* NIC - Network interface card
  + A NIC is the networking component which allows traffic flow. A single NIC will contain the public and private address.
* NSG - Network security group
  + These are the rules that are assigned to allow traffic to flow. The NSG can be assigned at a NIC level or a subnet level. It is recommended to apply at any one level only.
  + If there is no NSG, then traffic will be allowed in and out
  + We set inbound and outbound rules
  + Priority – All rules are assigned a priority and the lowest number is taken first. If rule 100 says allow and 101 says deny, then the result is allow.
  + Default Security rules – There are 6 default rules that can neither be removed or modified.

FAQs

1. What is Vnet Peering?

* Vnet Peering allows two Vnets either in the same region (Default Vnet Peering) or Globally (Global Vnet Peering)

2) What are the pre-checks for Vnet Peering?

a. Peering is non-transitive. If Vnet A is peered with Vnet B and Vnet B with peered with Vnet C then it does not mean that Vnet A and Vnet C are connected

b. The Address ranges cannot overlap between the Vnets

c. When peered, adding or deleting address range is disabled. If we need to add address range, we need to delete the peering and add the address range and then add peering again.

**Azure DNS**

What is DNS?

Think of the phone directory that is used at home. It is difficult to remember a string of numbers and hence the phone directory will list the phone numbers with names of persons/businesses.

* Coming back to the IT world, computers communicate with IP addresses. The DNS (Domain naming system) is a friendly name given to the computer.
* For example, a web server has an IP address of 53.102.94.86. Instead of using the IP Address, we assign a host name as web1. In a domain, the FQDN (Fully qualified domain name) will be web1.whizlabs.com.
* This is facilitated by DNS Servers which are setup in a hierarchy. At the top most level, we have the ROOT and under the root, we have the top level domains (TLD). examples of which are .ORG, .COM, .NET, .IN etc.,
* In addition to this, we have domain registrars where we purchase a domain name.
* Examples are Godaddy, Namecheap and Amazon too via Route53. When a user tries to connect to a server whizlabs.com, the DNS resolves this to the IP address by going to the ROOT and then to the .COM server.
* DNS works with a concept of Zones. We can set up Private or Public zones. Public zones are used when we want the internet to be able to resolve our names.
* However when we want to enable internal communication, we create private zones.
* Please note that zones can also be configured with a “Split-horizon” view which allows a private and public DNS zone to share a name.

FAQ

1. What is IP 168.63.129.16?

* This is actually called a Wire Server and has an IP address of 168.63.129.16. and it facilitates communication between Azure resources. It also serves as a DNS and DHCP server by default. Please ensure that this IP is not blocked.

Connection-specific

DNS

Suffix

.

lhlv032okq5e3g5zezobyk5bwf.bx.internal.cloudapp.net

Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter #2

Physical Address. . . . . . . . . : 00-0D-3A-8E-15-4C

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::7dbd:c33b:1ab:8e7f%7(Preferred)

IPv4 Address. . . . . . . . . . . : 10.0.1.4(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Lease Obtained. . . . . . . . . . : Saturday, March 13, 2021 7:06:42 PM

Lease Expires . . . . . . . . . . : Wednesday, April 20, 2157 9:38:31 AM

Default Gateway . . . . . . . . . : 10.0.1.1

DHCP Server . . . . . . . . . . . : 168.63.129.16

DHCPv6 IAID . . . . . . . . . . . : 117443898

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-DE-C5-9A-00-15-5D-00-04-01

DNS Servers . . . . . . . . . . . : 168.63.129.16

NetBIOS over Tcpip. . . . . . . . : Enabled

2) Can I buy my domain from Azure?

* No, Azure is not a domain registrar. You need to buy from a domain registrar and you can create a zone in azure and add the records for DNS resolution.

3) How do we configure VMs to use private zones?

* We can configure auto registration and for Vnet that we link with the Virtual Network Link on the DNS Zone, the DNS registration will be done automatically when the VM is created.

4) How do I use my custom website?

* We need to create a public zone and add an alias record. Once verified with the registrar, we can start using our custom name.

**Azure Firewall**

What is a Firewall?

* A Firewall is a security device for the network that monitors both incoming and outgoing traffic. Based on a set of security rules, it will either allow or deny the traffic. It acts as a barrier between our network and traffic from external sources like the internet. The objective is to block malicious traffic which include hackers and viruses.

**Azure Firewall**

● Azure Firewall is a network virtual appliance (NVA) which is a managed network security device on the cloud.

● The function is to protect our network resources on the cloud. There are two types of firewalls and they are classified as either Stateful or Stateless. Let’s say that you allow a certain incoming traffic (say port 80).

● When the same traffic returns, it is automatically allowed if it is stateless. On the other hand, Stateful traffic will need a specific rule for the outgoing traffic also, else the traffic will be blocked.

● Azure Firewall is a fully stateful firewall. So, we need to allow both incoming as well as outgoing traffic.

● Azure Firewall has built-in high availability and is highly scalable. We can create, enforce, and log application and network connectivity policies across subscriptions and virtual networks from a central location called Firewall Manager.

We need to set up a static public IP address for the virtual network resources

allowing outside firewalls to identify traffic originating from the virtual network. It is

fully integrated with Azure Monitor for logging and analytics.

● A typical setup for the firewall is done via a hub and spoke model where the Vnet

which hosts the firewall will act as a hub and the other Vnets will act as a spoke.

● The On premises and Internet is also connected to Azure Firewall. In this way, all

traffic will enter via the firewall and the rules setup via the policies will then allow or

deny the traffic.

● Please note the subnet that hosts the firewall must be named as Azurefirewallsubnet

else it will not function

Please see below the subnet created for the Azure firewall named as

AzureFirewallSubnet.

As discussed, the rules are set up in a central location using the Firewall Manager.

You can see the pol1 being assigned to fwvnet1 Virtual Networks. We can assign the

same policy to other networks and it is easier to manage centrally.

A Policy consists of rule collections which in turn contains individual rules. Here we

specify if the rule is to allow or deny.

We assign a priority from 0 to 65535 and the lowest number takes the priority while

processing the rules.

● We could place the rule collection within a group called the rule collection group.

Also, the rule is available as a tab called Network rules on the main panel.

● We specify the source type as either an IP address or IP Group. We can give a range

of IP addresses for Source and Destination. We can give \* to indicate all.

● We can specify Protocol and Port numbers. In the example below, we have given

Google a DNS server with IP of 8.8.8.8 and port of 53 which will allow DNS

resolution.

We can optionally enable intelligence-based filtering called Threat Intelligence and

the mode can be set to OFF/Alert only or Alert and deny. Microsoft threat

intelligence feed provides a list of IP addresses and domains and these recorded are

included as rules to allow or deny

This is the Network Rule tab which lists the rules.

We can also set up DNS servers for DNS resolution on the DNS tab.

Finally, we can see the topology of the Vnet and the firewall subnet on the Network watcher

blade under the Topology tab.

Azure Load Balancer

● Azure provides load balancing at Layer 7 which is the application layer via Azure

Application Gateway. This is typically http traffic.

Azure also provides load balancing at Layer 4 which is a transport layer consisting of

TCP and UDP protocols. This is the Azure Load Balancer.

● We could use the Azure Load balancer for both public facing as well as internal

application. The load balancer is set up with a backend pool which distributes traffic

to a set of VMs or VM Scale sets.

Here are the steps to create a load balancer:

Step 1: Create Load Balancer

We create a load balancer with the following options:

● Name for the load balancer

Internal or Public load balancing

● SKU type could be Standard or Basic. Since Basic does not have an SLA,

Standard SKU type is recommended for Production workload which has SLA

of 99.99%. Standard SKU comes with many more additional / better features

than Basic SKU like https.

● Regional or Global – This is a new feature and is available for Public Load

balancers

Step 2: Create Backend pool

● We create a backend pool where we attach VMs or VMSS

● VMs/ VMSS have to be in the same location.

● We could add multiple backend pools

Step 3: Add Health Probe

●

●

●

●

We need to add a health probe

We can configure TCP/HTTP/HTTPS as protocol

We add a port number

We add an interval and unhealthy threshold which is the interval for checking

where the probe passes a health check. The unhealthy threshold is the

number of times a probe is allowed to fail consecutively after which the

instance will be marked as unhealthy and traffic routing will be stopped.

Step 4: Add Load Balancing rule

● We create a load balancing rule

● We specify frontend IP address and Protocol (TCP or UDP) and Port

● We specify the Backend port and pool

We specify health probe

● We can also specify session persistence. If this option is enabled, the traffic

will be routed to the same VM.

Azure Load Balancer can also be configured to use as follows to map traffic to the available

servers:

● 2 tuple (Source IP, Destination IP)

● 3 tuple (Source IP, Destination IP, Protocol)

● 5 tuple (Source IP, Source Port, Destination IP, Destination Port, Protocol)

Please see how the traffic is routed based on the 5 tuples.

Azure Application Gateway

One of the main benefits of the Cloud is elasticity on-demand.

In a traditional datacenter, if there is a peak load requirement of 100 cores from 10-11 am

when users login, the machines will always need to have the capacity of 100 cores.

However, in the cloud environment, we will have a single VM with 50 cores at all times and

add another VM with 50 cores between 10-11 AM alone. This has reduced consumption by

almost 50%.

But how do we now distribute the load between the two VMs?

The solution is Load Balancing.

Load balancing can be done at 2 layers in the OSI model. One is at Layer 4 where we will use

the Azure load balancer. Here a combination of source and target ip and TCP/UDP Protocol

will be used to achieve routing.

The other routing type is at Layer 7, which is the Azure Application gateway. Here the

application gateway uses a front-end IP address which is resolved from FQDN via DNS. It has

an optional WAF (Web application firewall).

OSI LAYER and the load balancing options within Azure

How does the Application gateway work?

Step 1: User sends a request to a website with FQDN (fully qualified domain name) – for

example, https://whizlabs.com/videos. The query will be sent to a DNS server, and it will

return the IP address.

Step 2: The application gateway will be configured with a listener, a logical entity checking

for connection requests. The listener is configured with a front-end IP address, protocol, and

port number for connection requests.

Step 3: The application gateway also has a backend Pool/s. The backend pools could be VMs

or VMSS (VM Scale Sets) or external servers, or Azure App servers. Based on routing rules

set up, the traffic will be routed to the appropriate backend servers.

In the above example, you can see the routing rules being processed with url based routing.

So when the users type the url https://whizlabs.com/videos, the gateway sees the videos in

the url and sends the traffic to the Video Serving Pool.

Application Gateway with WAF

There is an optional feature WAF that can be additionally added to the application gateway.

WAF is based on Core Rule Set (CRS).

We need to set up a WAF Policy that has rules. There are two types of rules. One is Managed

rule sets which Azure preconfigures. The other is custom rules. Some of the features of WAF

are

● Some of the features that WAF provides are preventing SQL injection/ XSS/ http

protocol violations.

● It also protects against crawlers and scanners. We also can allow or block traffic

coming in from certain countries/regions in preview, and it is called Geo-filter traffic.

● WAF can be set up in two modes which are Detection or Prevention.

● When WAF is added, the traffic will be evaluated before Step 3 above against the

WAF rules.

● If violating traffic is found in Detection mode, the warning will be issued, and traffic

continues to flow. In Prevention mode, the traffic will be blocked.

Azure Traffic Manager

Azure provides the following services for Delivery.

● CDN

● Front Door

● Traffic Manager

● Application Gateway

● Load Balancer

While Load Balancers and Application Gateways operate at Layer 4 and 7, Traffic Manager

operates at a DNS level.

This service will distribute traffic to public-facing azure services at a global level. The public

endpoints provided are having high availability and quick response.

We can use Traffic Manager to route traffic to regional application gateways at a global level,

which could have a load balancer setup for multiple VMs at a database tier utilizing all the

services.

Here are some more scenarios:

Application Gateway - to load balance between your servers in a region at the application

layer.

Front Door - optimize the global routing of your web traffic and optimize top-tier end-user

performance and reliability through quick global failover.

Load Balancer - Network Layer Load Balancing

How does a Traffic Manager work?

The Traffic Manager uses DNS for resolution. It uses this to find the name server. Then it

locates the endpoints (which are not disabled) and routes the traffic based on the routing

methods specified.

Routing Methods:

Here are the routing methods which we can configure:

Check in the PDF

FAQs

1. What is the name of the website that will be created when we configure Traffic

Manager?

Azure will always use azurewebsites.net as a suffix. We cannot change it

2. So how do we use our website like whizlabs.com?

You need to create an alias in your DNS zone and point to the Traffic Manager.

Azure Express Route

Connectivity to Azure

● There are several ways to connect to Azure. Broadly classifying them, we could either

use the internet or have a direct connection.

● While connecting via the internet, we need to use a VPN to connect our

infrastructure on premises with the cloud using a VPN gateway which encrypts our

traffic by creating a tunnel.

● We could choose either a client-to-site VPN which is only one client system

connected to the cloud or site-to-site VPN where we connect two sites.

● This setup depends on the public internet and we must secure and could have

reliability issues.

● Hence it is better to use a dedicated connection between our infrastructure and the

cloud with an Express Route connectivity.

● We need to locate a connectivity provider. There are several choices available based

on location.

● For example, in India, we have BSNL/AIRTEL/SIFY and in the USA, we have AT&T/

SPRINT/ VERIZON and many more.

Express Route connectivity allows us to connect to 2 Microsoft cloud services –

Microsoft Azure Services as well as Microsoft 365 services.

● Also, we can see from the above diagram that there is an active-active redundant

pair of cross connections setup for high availability. We can add further redundancy

by adding up to 16 Express route connections.

Express route has the following bandwidths to choose from based on our

requirements:

● 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps

● If we have multiple subscriptions, we can connect all of them to a single Express

route connection.

● You can have upto 10 Vnet connections on a standard Express route connection and

upto 100 for Premium connection. However please note that all connections will

share the same bandwidth.

We could even have a site-to-site VPN for adding redundancy. If there were issues with the

Express route, we can failover to the S-2-S VPN.

FAQs

1) If I have a 100 Mbps circuit, what is ingress and egress capacity?

You will have an incoming capacity of 100 Mbps and outgoing capacity of 100 Mbps.

What is the routing protocol?

Express route uses BGP (Border gateway protocol)

2) What happens if there is any maintenance?

There won’t be any impact. Express route uses an active-active setup and only the

circuit will be maintained at a given time.

3) So where does the connection land on the Azure cloud?

We connect to one of the Vnets in a subscription. We can connect upto 10 Vnets in

each of the 10 subscriptions max. We need to go for Premium if we would like to add

more.

How do we plan for Disaster recovery?

Microsoft recommends 2 Express connectivity to avoid a single point of failure. We

could also set up a Site-to-site VPN instead of a second circuit.

Azure VPN Gateway

This is one of the methods that allows inter-site connectivity. Express route is the preferred

connection as it has higher bandwidth and is in active-active mode. Smaller enterprises can

choose VPN gateways or one could use VPN Gateway as a backup to Express route

connectivity.

The VPN gateways are set up over the Public internet. Hence the traffic needs to be

encrypted. IPSEC is used as the tunnelling protocol which creates a secure tunnel through

which the data travels. Even if the traffic is intercepted, it cannot be decrypted.

VPN Gateways types

● Site-to-Site VPN Gateways

o Here the On-premises will be a site and Azure VPN will be another site. We

can connect multiple VNets.

● Point to Site VPN gateways

o Here we connect a single client machine from on-premises to the Azure VNet.

o We can use the same connection on multiple clients by exporting the

configuration from the existing client.

● Internal Gateway between Azure networks

o This is a special use case where we want to encrypt traffic between Azure

Vnets.

Steps to establish VPN Gateway

1. GatewaySubnet

a. We need to create a subnet with the name “gatewaysubnet” for the setup

b. If we are creating a Vnet, this subnet gets created automatically.

Please see the diagram below which shows the gateway subnet. This was created implicitly

when the wlvnet1 was created as part of the Vnet gateway creation.

Local Network Gateway

a. We need to obtain a Public IP address from the on-premises admin team and

use that as the endpoint.

b. See the IP address given as 53.24.54.23. This is the ip address of the router

on-premises

Virtual Network Gateway

a. We need to create the virtual network gateway with the following inputs

i. Gateway type – in our case, we are going to use VPN

ii. Vpn type – could be either Route-based or Policy-based. Please note

that we cannot change the type once it is created.

We need to delete the gateway and recreate it to make the change.

Policy based is the most common type

iii. SKU – There are several SKUs. Please note that Basic is considered

legacy and not recommended.

iv. Subnet – As mentioned, the name should be GatewaySubnet.

4. Connection

a. Once the prerequisites are fulfilled with the creation of Gateway Subnet,

Local Network Gateway and the Virtual Network Gateway, we can create

connection as follows

i. Connection type – the options are Vnet-to-Vnet, Express Route or

Site-to-Site. In our case, we choose Site-to-site which uses the IPsec

tunnelling protocol by default.

ii. Bidirectional Connectivity – Connections are usually unidirectional.

We can select bidirectional to choose 2-way communication

iii. Shared Key(PSK) - We need to create a password here and need to

share this with the on-premises admin to configure from their side.

5. On-premises setup

a. Once the setup is complete, we can download the configuration to be shared

to the on-premises admin.

b. We need to get the router model and select the same from the dropdown list

and download the configuration and share with the admin along with the

shared key.

Topology

We can check for the topology from the network watcher – topology blade.

What is a CDN?

CDN stands for Content Delivery network. It is an architecture of distributed network of

servers that can efficiently deliver web content to users.

CDNs will cache the content on edge servers in the POP (point of presence) locations

keeping the content closer to the users thereby minimizing latency. This is made possible by

using the existing network infrastructure of the CDN provider.

Let's say that a company Whizlabs has a headquarters in NY, USA and branches in CA, USA

and Bangalore, India.

The Servers are located in NY and we have a user logging in from Bangalore, India. The data

needs to traverse the network and this will cause latency.

The solution here is to use CDN and use the Bangalore location to cache the data. Now, the

user will be able to retrieve the data from Bangalore.

Please note that the data is not stored permanently on the edge location. This is to ensure

that data does not go stale and it is current.

So we may set a cache interval of 24 hours and every day, the data will be retrieved from the

Origin Server (NY, USA) and cached on the edge locations.

Also, if the data is not available (first time accessing) or if the cache has been marked as

invalid, the data will be fetched from Server and sent to the user and cached on the edge location

The next time, the request will be fulfilled by the edge server. This also reduces the load on

the Origin server.

FAQs:

1) How long is the data cached on the edge Server?

The TTL (time to live) by default is 7 days. This can be configured as per the

application requirements. Once TTL expires, the cache will be marked as invalid.

2) What type of azure servers can serve as Origin Servers to get source data?

Azure Web App, Azure Cloud Service, Azure Storage account, or any public web

server.

3) What are the CDN products available?

Azure has its own product. Besides that, it has tied up with Akamai and Verizon.

Here are the offerings:

a. Azure CDN Standard from Microsoft

b. Azure CDN Standard from Akamai

c. Azure CDN Standard from Verizon

d. Azure CDN Premium from Verizon.

Please note that not all products might be available at all locations. You will need to check

the product availability for your location.

4) What are some of the additional features?

a. Dynamic site acceleration(DSA)

b. Video streaming optimization

c. Customizable, rules based content delivery engine

d. HTTPS support with CDN endpoint

e. Compression encodings

Who are the market leaders for CDN? - PFB