# Azure Networking Strategy

Azure has its own physical network in and between data centers. Any network configuration done by an Azure user is purely software configuration of existing infrastructure and applications. It all ends up being entries in a database.

Networking services are split between 4 major categories:

* Connectivity
* Protection
* Delivery
* Monitoring

**Connectivity**

Azure Networking is built around **Virtual Networks (VN)**. These provide connectivity between services, inside and outside of Azure.

A VN is not required for some services, because it is provided as part of the serverless, managed service; these are usually Saas or PaaS offerings; for IaaS services, such as virtual machines, a VN is expected to be required.

A VN is assigned an adress space, which is a contiguous block of private IP addresses, which can be divided into **subnets**. A best practice recommendation is to have a few large spaces with many subnets rather than having many small VNs with small adress spaces. 5 IP addresses are reserved by Azure in every subnet. VNs in a single subscription cannot overlap.

A VN comes with a default subnet. Subnets can be configured with **Network Security Groups (NSGs)** to filter inbound and outbound traffic.

A best practice recommendation is to use subnets inside a VN to separate application layers and provide isolation and limit exposition.

Devices are added to a subnet using a **Network Interface Card (NIC)**. NICs can have their own NSGs to provide an additional layer of filtering, although it is not recommended to mix both levels, except in very specific situation (such as restricting VN traffic to a single machine inside a subnet). A device can have multiple NICs and be part of multiple subnets, but they must be part of the same VN. All devices on a VN must exist in the same region as the VN.

All devices on the same VN can talk to each other by default, and can reach the outside. Outside devices must be explicitly allowed to reached into the VN.

Resources from a different VN (including managed resources, such as storage accounts or SQL Databases) can be made part of a VN by creating a **Virtual Network Endpoint**, which will represent the resource inside the VN. Access to the resource can then be restricted to that VN through NSGs.

**VNet Peering**connects two VNs in the same region as if they were one. These VNs can be in different subscriptions. They must not have any address space overlap. When there are many different VNs that need to communicate, a Hub and Spoke pattern is recommended, in which when two Spokes need to communicate, they do so through a central VN (Hub). NSG rules are put in place to enforce this setup.

When the VNs are in different region, they can be linked through **Global VNet Peering**.

Azure services (called devices or appliances) can be added to a VN to provide additional features and benefits. Some are available for free in a basic form, but most have a cost, even if it’s only in their Premium edition.

**Azure Load Balancer (LB)**

A load balancer dispatches requests between (hopefully identical) servers able to handle the same types of requests. It applies the same rules to all traffic, and works at level 4 (Transport) of the OSI networking model.

It reduces traffic to servers by spreading it over multiple machine, allowing for horizontal scalability, which can be combined with auto-scale rules in Azure to add or remove server instances based on various conditions. The servers are automatically added or removed from the load balancer’s list of available servers. Rules can also be added to scale vertically, increasing or decreasing server resources (number of CPU, speed of CPU, amount of memory), but this quickly reaches physical limits, while horizontal scaling is virtually endless.

A load balancer can also detect unresponsive servers using health probes, and remove them from its list, spreading traffic over the remaining instances.

It can also serve the role of proxy, being the publicly exposed part of a system, while the actual servers are actually hidden inside a well-protected subnet that only the load balancer can reach.

The most common traffic/request distribution modes are:

* Round-robin: Each new request goes to the next available server in the list. A variation allows the load balancer to periodically check the load of each server and not send any traffic to servers already over a certain threshold.
* Sticky-sessions: The load balancer takes into account the affinity of a client to a server and directs all its requests to that specific server. This can become problematic when that server crashes, but some application’s design require this to function.

**Application Gateway**

An application gateway is a smarter LB, working at level 7 (Application) of the OSI networking model, and is thus aware of HTTP and traffic type, which can read the contents of HTTP requests and route traffic based on different criteria, such as contents of the URL or other conditions.

An application gateway has the option to provide a Web Application Firewall service, which will detect common attacks (such as cross-site scripting and SQL injections), following OWASP methods and risks. It can connect to Azure Monitor and Azure Security Center.

Both load balancer and application gateway must be in the same region as the servers they distribute traffic to. If the servers are in different regions, use Azure Traffic Manager or Azure Frontdoor.

**Virtual Private Network (VPN)**

A VPN is a seczre (encrypted) channel between networks, which can be built over the public Internet or private lines. It allows an enterprise network to be joined with an Azure VN. There are different categories:

* **Point-to-Site (P2S) VPN**: one computer is connected to a remote network, using a locally installed VPN software.
* **Site-to-Site (S2S) VPN**: two networks are connected remotely to each other, in this case an on-premises is extended to Azure (or the other way around). This requires the installation of a Network Gateway in the on-premises network that is used to route traffic into the Azure Virtual Network or receive traffic from Azure.

To be reached by VPN, an Azure VN must have a small subnet containing only the Azure VPN Gateway that will decrypt and encrypt traffic to/from the outside network, communicating with its corresponding service at the other end of the channel (either the VPN client for P2S or the VPN Gateway for S2S). Azure does not support all types of VPN Gateway.

The main categories of VPN setup are:

* Static: (old system) provides a fixed routing table.
* Dynamic: (new approach) making use of Border Gateway Protocol (BGP) so that each end of the channel can discover which address ranges the other side can handle.

Azure provides built-in reliability by setting up 2 connections between the on-premise VPN gateway and its Azure counterpart. Availability of the VPN link can be further improved by having multiple VPN gateways on premise (either active or inactive) and provisioning a failover Azure VPN gateway in the target VN, which can also be active or inactive, enabling 4 different configurations.

**ExpressRoute**

A high-speed, private (encrypted), fiber-optic connection between premises and Azure over private lines, usually provided by an Internet exchange provider (IXP).

ExpressRoute Direct is the next level of connection, connecting directly into the Azure Backbone in a data center, allowing for massive data ingestion and physical separation of traffic.

**Route Table**

A route table is a resource that provides routing for traffic to or from specific IP addresses. Rules are created to direct traffic to a VN Gateway, to a particular VN, to the Internet, or to a virtual appliance. A route table can also implement a rule to kill traffic (drop) to/from an IP address.

Once created, a route table can be associated with one or multiple VNs and subnets.

**Bastion**

Azure Bastion provides a server inside a VN that you have to connect to first (aka, jumpbox) before you can access anything else in the VN or its neighbors.

**Protection**

Protection of the applications and servers running in a VN can be implemented using:

**Firewalls**

A firewall is a network device (physical or logical) blocking traffic unless it matches specific rules (deny all — allow some, or whitelisting).

There are also third-party firewalls available on Azure.

**Network Security Groups (NSGs)**

An NSG is a subnet- (or NIC-) level filter for traffic, acting as a firewall, based on rules applied. Rules are evaluated in ascending order of priority, until a match is found. A rule has the following attributes:

* A name, to identify it in the interface, in the logs, and to programmatically manipulate it.
* A priority (1 to 65500), which determines its position in the evaluation process.
* A source and a destination IP port or port range.
* A source and a destination, which can be specified as “Any”, as “0.0.0.0/0” to allow all IP addresses, as a specific IP address, as a CIDR IP address block, as a service tag (Internet, AzureLoadBalancer, VirtualNetwork) or as an Application Service Group.
* A protocol, which can be one of TCP, UDP, ICMP, ESP, AH, or “Any” which combines TCP, UDP and ICMP.
* A direction, InBound or OutBound.
* An action, either Deny or Allow, which indicates what action must by taken on traffic when the rule is matched.

When a subnet is created, it contains 3 default InBound rules, which cannot be removed, but have a priority high enough to easily be overridden by user-defined rules.

* Name: AllowVirtualNetworkInBound, Priority: 65000, Source: VirtualNetwork, Destination: VirtualNetwork, Source Port: Any, Destination Port: Any, Protocol: Any, Direction: InBound, Action: Allow
* Name: AllowAzureLoadBalancerInBound, Priority: 65001, Source: AzureLoadBalancer, Destination: VirtualNetwor, Source Port: Any, Destination Port: Any, Protocol: Any, Direction: InBound, Action: Allow
* Name: DenyAllInBound, Priority: 65500, Source: Any, Destination: VirtualNetwork, Source Port: Any, Destination Port: Any, Protocol: Any, Direction: InBound, Action: Deny

**Application Security Groups (ASGs)**

An ASG is a logical container that can be used to configure NSG rules in a more fine-grained way. It is based on the IP addresses of resource, whose NICs are added to the ASG. Traffic to and from these resources can then be identified as such by NSG rules, and specific filtering performed.

**Distributed Denial of Service (DDoS) Protection**

This service detects DDoS traffic and stops it before it reaches the VN. A free version is automatically included, and a paid-for version adds more intelligence and functionalities.

**Web Application Firewall (WAF)**

Dedicated to Web servers, this type of firewall can be used through

* An Application Gateway
* The Azure Frontdoor service

**Azure Firewall**

A managed service provided by Azure in various editions to protect VNs and Azure resources.

**Delivery**

Azure networking service help improve delivery speed of data, most notably through the following offerings:

**Content Distribution Network (CDN)**

A CDN reduces traffic to front-end server through a constellation of servers placed around the globe, which can be used to host and replicate static files closer to the users.

Azure supports two external providers (Akamai and Verizon), as well as its own Azure CDN.

**Azure Traffic Manager (ATM)**

A service used to direct traffic at the DNS level to the nodes providing the request service around the globe, based on the user’s location. ATM acts as a DNS server for the domain of the server, and responds to DNS requests by returning the IP address of the instance closest to the requestor (by performing a reverse-lookup). It can also handle failover of the service when a region becomes unavailable.

**Azure Frontdoor**

Azure Frontdoor provides a secure and scalable entry point for global applications. It works at level 7 (Application) of the OSI networking model, and can distribute traffic based on rules (identifying URL parts and path, source location, …). It supports caching and can provide WAF and DDoS Protection.

**Azure DNS**

Azure provides a managed domain name service, which can be used to manage DNS records for a domain.

**Monitoring**

Azure provides different tools at various levels to monitor network activity and incidents.

**Network Watcher**

Attached to a VN, NW provides alerting and notifications, enables triggers to serverless apps (such as Azure Functions or LogicApps), and packet capture.

**ExpressRoute Monitor**

When using ExpressRoute to access Azure, a specific monitoring service is available to report on traffic.

**Azure Monitor**

Azure Monitor provides a centralized logging platform for applications and systems, with reporting and alerting capabilities.

**Pricing Considerations**

The information in this section might no longer be accurate due to the always shifting nature of cloud infrastructure and the competitive market. But the free/paid-for distinctions should remain relatively unchanged. Always consult Azure Pricing Calculator for the latest rates.

VNs are free. You can create up to 1000 VNs per subscription.  
Subnets are also free. You can create up to 3000 subnets per VN.

NSGs and ASGs are free.

Added devices come with their own costs, fixed (subscription or install fee) and/or running based on volume of traffic or requests.

Private IP addresses are free. Public or reserved IP addresses have a cost.

Data within a VN travels for free.  
Data between VNs in the same region (peering) are billed at the rate of $0.01 per GB, both on the inbound and the outbound sides of the connection.  
Data beween VNs in different region (global peering) are bill at different rates depending on the regions and whether they originate and end on the same continent or not, etc. Prices vary between $0.035 and $0.16 per GB.  
Inboud Internet traffic is free, but outbound traffic has a progressive price, between $0.08 and $0.18 per GB, with the first 100GB free each month.

ExpressRoute is priced depending on bandwidth, starting at $50 monthly for 50Mb/s + traffic cost, up to $50000 monthly for 10Gb/s. There is also an option for unlimited traffic, starting at $300 per month for 50Mb/s.

ExpressRoute Direct prices vary between $6000 and $8500 per month for a dual 10Gb/s connection, up to between $50000 to $80000 per month for a dual 100Gb/s connection.

A load balancer can be set up for free.  
An application gateway is billed based on traffic or at a fixed, time-based rate.  
Azure Traffic Manager is billed by request, at a cost of $0.5 per 1 million requests.  
Azure Fontdoor is billed based on the volume of inbound and outbound traffic as well as the number of rules defined, with a premium for the AWF option.

**Networking Strategy**

**Naming convention**

* Use names that make sense.
* Preferrably use a company-wide naming convention policy.
* A resource’s name should indicate the type of the resource and why it exists.
* Microsoft provides recommendations for naming.

**Tags**

Add metadata to resource for easier identification and reporting using tags.  
Use tags to indicate

* environment (dev, test, prod, …)
* project or application the resource is part of
* department responsible or to be billed
* …

**Regions**

* Determine how many regions the resources will be duplicated into.
* Create VNs in each region.
* Use subnets for layer separation.
* Leave room in the VNs for growth through new subnets, don’t use all available addresses from the start.
* Use few VNs in each region.

**Public IP**

* Determine if public IP addresses are required for some resources, or if Bastion or VPN access are enough.

**Peering**

* Determine if peering or global peering is required.
* Plan to avoid range overlaps when peering is required.

**Network Security Strategy**

* Keep It Simple, with a small number of VNs and reusable components.
* Use NSGs and plan to reuse them in different VNs.
* Use ASGs.
* Use Azure network protection services.
* Check out 3rd party security tools in Azure Marketplace.
* Reduce the attack surface size by exposing only ports and machines that really need it, and by disabling any code module that is not used.
* Disable SSH and RDP access, or ensure it can be used through Bastion or a VPN.
* Block Internet access if possible, both inbound and outbound.
* Limit the number of administrators, to improve consistency.
* Use subnets for security.
* Use Azure AD Conditional Access for administrator access.
* Use Just-In-Time Access for administrative operations.
* Use Azure AD Privileged Identity Management (AAD-PIM) to grant temporary permissions that are automatically removed.
* Use route tables to ensure VNs can only be accessed with a VPN.