Contents

[Analysis 1](#_Toc162009094)

[ExpressRoute 1](#_Toc162009095)

[NAT Gateway 1](#_Toc162009096)

[ExpressRoute 1](#_Toc162009097)

[NAT Gateway 8](#_Toc162009098)

[private access to Azure Services 10](#_Toc162009099)

[Az-700 Simplier 14](#_Toc162009100)

[Azure Firewall 14](#_Toc162009101)

[load balancer 22](#_Toc162009102)

[Icons image for memorising 24](#_Toc162009103)

# Analysis

## ExpressRoute

* Design and implement ExpressRoute
* Design and implement ExpressRoute Global Reach
* Design and implement ExpressRoute FastPath
* Troubleshoot ExpressRoute connection issues

1. Pricing
2. Options
3. How should you configure
4. Minimum number of Express Route circuits
5. Order / how do you connect sth with sth using ExpressRoute
6. Diffirence : ExpressRoute -vs- etc etc
7. Comble needs : link sth to sth / how

## NAT Gateway

* Describe the Azure NAT Gateway service.
* Recognize scenarios where Azure NAT Gateway is applicable.
* Perform basic deployment of the Azure NAT Gateway service.

1. Choose best tool for specyfic needs
2. What is supported

|  |  |
| --- | --- |
| ExpressRoute **ExpressRoute is a type of GateWay** | ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a   * private connection * to Microsoft Azure * to Microsoft 365. * from an any-to-any (IP VPN) network, * from a point-to-point Ethernet network, * from a virtual cross-connection through a connectivity provider at a colocation facility. * As no public offer more reliability, faster speeds, consistent latencies, and higher security. |
| Options   * ExpressRoute FastPath * ExpressRoute Global Reach * ExpressRoute Direct * ExpressRoute Local   Provide reliable and secure connectivity to Azure services.-vs-Connect your network to the public internet. |  |
| SKU  PRICING  Site-to-site vs point-to-site | P2S –   * Other site is the client computer (laptop) * requires public facing IP   P2P – traditional VPN protocol [considered legacy]  S2S – connect corporate site   * On-premise + Azure Virtual Network |
| ExpressRoute gateway |  |
| ExpressRoute circuit |  |
| peering for an ExpressRoute |  |
| ExpressRoute circuit to a virtual network |  |
| ExpressRoute circuit to a virtual network |  |
| Improve data path performance between networks with ExpressRoute FastPath |  |
| connection issues   * properties |  |
|  |  |

A diagram of a cloud service

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated A diagram of a connection between a vpn and a vpn

Description automatically generated

A diagram of a computer

Description automatically generated A diagram of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated A diagram of a computer

Description automatically generated A diagram of a company

Description automatically generated A diagram of a company

Description automatically generated

S2S

Secure con to Azure cloud infrastructure

* Manage Azure Vm localy
* Manage local server on Azure

A screenshot of a computer

Description automatically generatedA close-up of a white background

Description automatically generatedA diagram of a cloud computing network

Description automatically generated

|  |  |
| --- | --- |
| NAT Gateway | Network Address Translation  used for decades for mapping local IP addresses to public addresses. |
| Problem solves | resolving connectivity problems |
| Can’t | can’t use Azure NAT Gateway to configure inbound connections handling. |
| Can |  |

A computer screen shot of a diagram

Description automatically generated A diagram of a network

Description automatically generated A diagram of a network

Description automatically generated A diagram of a network

Description automatically generated A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| private access to Azure Services |  |
| 1. Azure Private Link, and 2. virtual network service endpoints.   Private Endpoint | Solve problem  replaces the resource's public endpoint. |
|  | |
| * Understand the difference between private link and private endpoints * Design and configure Private Endpoints * Integrate a Private Link with DNS and on-premises clients * Create, configure, and provide access to Service Endpoints |  |
|  | Adding service endpoints doesn't remove the public endpoint. It simply provides a redirection of traffic.  To enable a Service Endpoint, you must do the following two things:   * Turn off public access to the service. * Add the Service Endpoint to a virtual network. |
| **Private Links are dependent on Private Endpoints.**  **A Service Endpoints connects to external resources. A Private Endpoint enable a private and secure connection between your virtual network and Azure.** | |

A diagram of a server

Description automatically generated

A diagram of a server

Description automatically generatedA screenshot of a computer

Description automatically generated

A diagram of a computer network

Description automatically generated

## Az-700 Simplier

Vnet – is for a Virtual network, which is like a virtual Space, for connecting.   
it encapsulate the content like on-premise or azure services. And keep it isolated letting to configure all kind of input output tools.

The problems solved by Vnet are :

* Isolation
* Control
* Connectivity

For connections

The alternatives exist provided by AWS, Google, Third parties, Container oriented technologies, and hybrid oriented focusing more on app layer

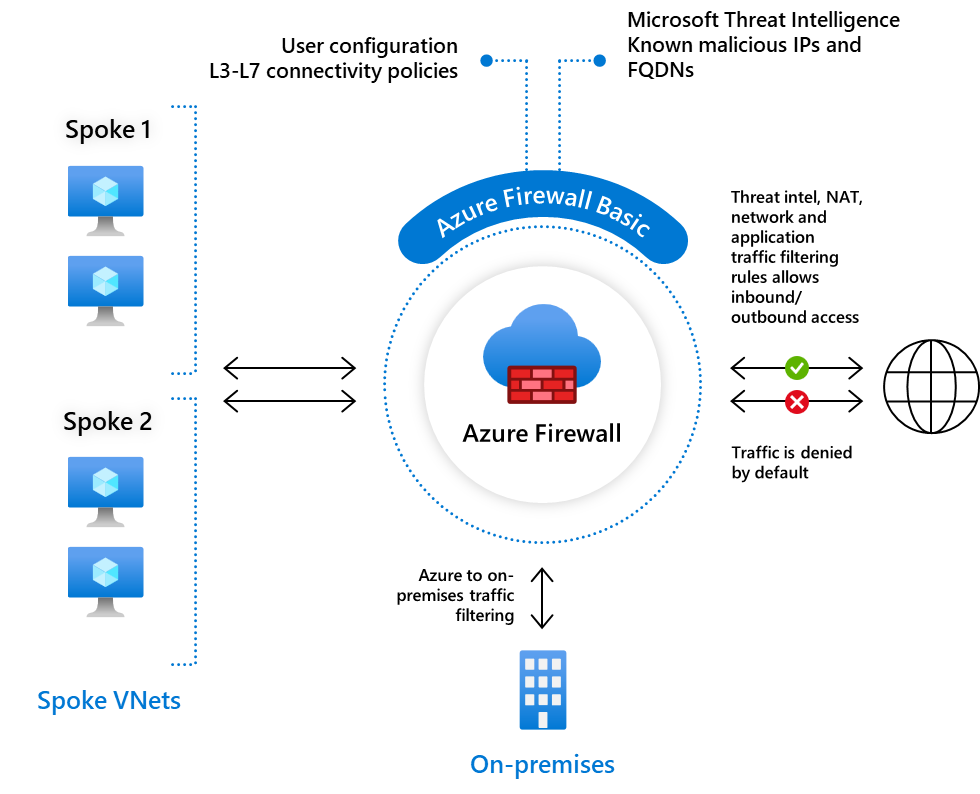
More fined tools

* Bastion
* NSGs
* Application Gateway
* Azure Firewall

|  |  |
| --- | --- |
| Azure Firewall | Control monitor access |
| * Firewall Manager * Evaluate whether Azure Firewall is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic. * Firewall Premium * Evaluate whether Azure Firewall Manager is the right solution for deploying policies across multiple firewalls. * Identify and describe use cases for Azure Firewall and Azure Firewall Manager.   [**Start**](https://learn.microsoft.com/en-us/training/modules/introduction-azure-firewall/1-introduction/)Add | Set several FW, ex. create policies for several FW  TLS Inspection – decrypt, process, encrypt than send  IDPS – intrusion detection and prevention system,  URL Filtering – extends FQDN  Web categories – control over |
| **FireWall -**  firewall are only about ip, leting in and out control,  but handling this in more inteligent and automatic way require more tuned tools  Azure Front Door  For global audience, need for optimize by region  Azure Application GateWay  Internal trafic management :  - url based routing , multi site hosting, session affinity,  Web Application Firewall (WAF) Setup: Implementing geographic restrictions using WAF is relatively straightforward in both Azure Front Door and Azure Application Gateway. The complexity doesn't lie much in setting up the firewall itself but rather in choosing the service that best fits your application's needs.  **NAT Gateway** vs. **Application Gateway**  NAT Gateway and Application Gateway are different services within Azure, serving distinct purposes:  **NAT Gateway** is a network service that provides Network Address Translation (NAT) capabilities for virtual networks in Azure. Its primary function is to enable resources within a private virtual network to access the internet or other public networks while maintaining the private IP address of the resources. NAT Gateway is about outbound internet connectivity and IP address masquerading for virtual networks.  **Application Gateway**, on the other hand, is a web traffic load balancer and application-level router. It is designed to manage incoming web traffic, distribute it across multiple servers or services, and offer various application-level routing features (such as URL-based routing, SSL termination, and session affinity), along with the integrated Web Application Firewall (WAF) for security. | |

A diagram of a cloud computing system

Description automatically generated A diagram of a firewall

Description automatically generated 

Network service endpoints

* Direct connection to azure service, not accessible to the internetroute A diagram of a server

  Description automatically generated

Route table : is about global connectivity, it is about describing all connectivity possible for given context.

* Source: it is about how it was created
* Next Hop Type : where it goes, where it is connected into

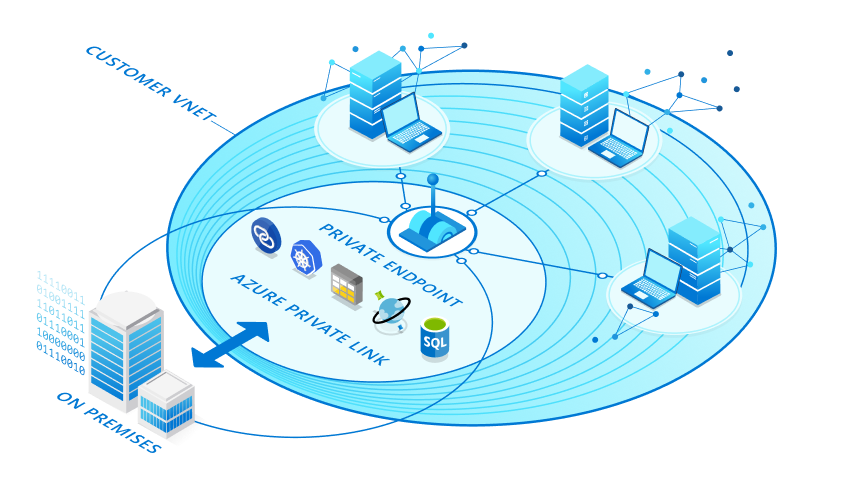
A diagram of a server

Description automatically generated

A screenshot of a computer

Description automatically generated

Private Link – remove public part from the connection



* Private Endpoints are part of Private Link,
* Private link can contain more than one private endpoints
* Private link is a higher level service, and is encapsulating endpoints

Azure DNS Private Resolver – is like a smart number on the phone, which provides kind of names for the ip, so I know what computer I am connecting to

Private DNS Resolver - it is like the old style telephone operator connecting the call with the correct destination

DNS Zone is like the phone book, may be resolved by resolver or the vnet itself when inside vnet where no need for operator becouse direct connection

Certyfication a totall BS

A screenshot of a computer

Description automatically generated

In real-world Azure configurations, such details are crucial for the correct setup and functionality of networking and DNS resolution services. Misalignments between the VNet of a resolver's endpoint and the VNet to which DNS zones are linked could indeed lead to misconceptions about how these components interact within Azure's networking architecture.

* The Azure Private DNS Resolver is indeed like an operator, but its association with a subnet (e.g., being placed in Subnet4) doesn't limit it to a specific "phone book" (DNS Zone). Instead, this placement determines where within the virtual network (VNet) the resolver's endpoint exists. This is important for routing and security within the network infrastructure, dictating where the resolver listens for DNS queries.
* The resolver's ability to access DNS zones isn't limited by its subnet placement but by the virtual network links and DNS zone configurations. So, even if the resolver's inbound endpoint is in a subnet within VNet1, it can resolve DNS queries for any zone that VNet1 has access to, according to the virtual network links to DNS zones.

In the scenario you mentioned, since the resolver (Private1) is associated with VNet1, it primarily resolves names from DNS zones linked to VNet1. The fact that it has an "inbound endpoint on Subnet4" seems to be a misconfiguration or a typo since Subnet4 is part of VNet2, not VNet1. For clarification, a resolver's capability to resolve DNS zones is based on its associated VNet and the links that VNet has to DNS zones, not the specific subnet the resolver's endpoint is placed in.

|  |
| --- |
| for him being in vnet1 it is not possible to resolve zone2 ?  ChatGPT  **ChatGPT**  Correct, if the Azure Private DNS Resolver is configured within VNet1, it would not natively resolve DNS queries for Zone2.com if Zone2.com is linked exclusively to VNet2, under normal circumstances. This is because the DNS zones are linked to specific virtual networks, and the resolver's ability to resolve names within a DNS zone depends on that zone being linked to the virtual network where the resolver is deployed.  In the given scenario, since the resolver (Private1) is associated with VNet1, it's primarily set up to resolve DNS queries for DNS zones linked to VNet1. Therefore, it wouldn't directly resolve queries for Zone2.com unless there's some form of interconnection or configuration allowing VNet1 to access DNS information for Zone2.com, such as:   * **VNet Peering** between VNet1 and VNet2, with appropriate DNS forwarding configurations, could potentially allow for DNS resolution across VNets, depending on the specific setup and permissions. * **Custom DNS Forwarding** setup on the DNS Resolver could also potentially route queries for Zone2.com through VNet1, assuming there's a way to handle these queries appropriately (like forwarding them to a resolver that can access Zone2.com).   However, without such configurations explicitly designed to bridge these networks and their respective DNS zones, a resolver in VNet1 would not resolve names in Zone2.com by default. |

When I will use p2s (peer-to-peer) – two comp connected together

And when S2S – Site-to-Site is connecting over internet in secure way

* Connect data centers
* Is encrypted -
* Merge two distant network into a single unified network

# load balancer

Basic SKU - single availability zone.

Standard SKU - supports integration with services across peered virtual networks, which the Basic SKU does not support.

**Public Load Balancer** - ability to provide a single public IP address-to access-multiple virtual machines

**Internal Load Balancer**: is-distributing network traffic within a private network, does not provide public IP addresses or direct access from the internet to the virtual machines

* it necessitates an IP address within the subnet for its operation.
* is assigned to-him a private IP address from within the subnet it is configured to operate in. which serves as the front-end to the load balancer

|  |  |
| --- | --- |
| Traffic -vs- layers |  |
| Layer 7 | **Azure Application Gateway**: Primarily operates at Layer 7 (HTTP, HTTPS), offering application-level routing and load balancing, such as URL-based routing and SSL termination. While it can provide high availability for web applications, it's not designed for generic network traffic inspection tasks that NVAs are typically used for.  **Azure Front Door**: Similar to Azure Application Gateway, Azure Front Door is a global, scalable entry-point that works at Layer 7. It's primarily designed for managing, securing, and delivering web content and applications at a global scale, not for internal network traffic inspection. |
| DNS | **Azure Traffic Manager**: Operates at the DNS level to route traffic between global Azure regions or external endpoints. It's NOT suitable for intra-Azure virtual network traffic routing or for scenarios requiring inspection of all virtual network traffic. |
|  |  |

A blue and grey rectangular boxes

Description automatically generated

Adress spaces

Vnets not between regions

# Ddos - Distributed Denial of Service

Services running on Azure are inherently protected by the default infrastructure-level DDoS protection.

* helps secure layers 3 and 4
* provides application (layer 7) protection with Azure Web Application Firewall, which is included with Azure Gateway.
* (OPTIONAL) Azure DDoS IP Protection as pay-per-protected IP model.

*Each Azure application has its own traffic pattern, which is unique like a human fingerprint.*

# Icons image for memorising

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A computer screen with a blue cube on it  Description automatically generated | A computer screen with a blue cube on it  Description automatically generated | A computer screen with a blue cube on it  Description automatically generated | A computer screen with a blue cube on it  Description automatically generated | A computer screen with a blue cube on it  Description automatically generated |
| A blue and white logo  Description automatically generated with medium confidence | A blue and white logo  Description automatically generated with medium confidence | A blue and white logo  Description automatically generated with medium confidence | A blue and white logo  Description automatically generated with medium confidence | A blue and white logo  Description automatically generated with medium confidence |
| A logo with purple cubes  Description automatically generated | A logo with purple cubes  Description automatically generated | A logo with purple cubes  Description automatically generated | A logo with purple cubes  Description automatically generated | A logo with purple cubes  Description automatically generated |
| A blue and white sign with arrows  Description automatically generated | A blue and white sign with arrows  Description automatically generated | A blue and white sign with arrows  Description automatically generated | A blue and white sign with arrows  Description automatically generated | A blue and white sign with arrows  Description automatically generated |
| A cloud with a brick wall  Description automatically generated | A cloud with a brick wall  Description automatically generated | A cloud with a brick wall  Description automatically generated | A cloud with a brick wall  Description automatically generated | A cloud with a brick wall  Description automatically generated |
| A blue and green arrows with a green dot  Description automatically generated |  |  |  |  |
| A yellow key with white text  Description automatically generated  Azure Subscription |  |  |  |  |
| A blue line drawing of a server  Description automatically generated  On-premise |  |  |  |  |
| A logo of a company  Description automatically generated  Active Directory Domain Services (AD DS) |  |  |  |  |

# Abreviation

BFD - Bidirectional Forwarding Detection

DDoS - Distributed Denial of Service

VPN GateWay == virtual Network gateway (they’re the same thing)