

AZ-500

Tag 2

Microsoft Azure Security Technologies

Guten Morgen!



Agenda

1 Manage identity and access ✓

2 Secure networking VNet ✓

3 Secure compute, storage, and databases

4 Manage security operations



Entra ID

Managed ID

Lab

(ServiceEP)

PrivateEP



Lab

Azure FW

App GW

Front Door

LB

Learning path: Secure Networking

Plan and implement security for virtual networks

Plan and implement security for private access to Azure resources

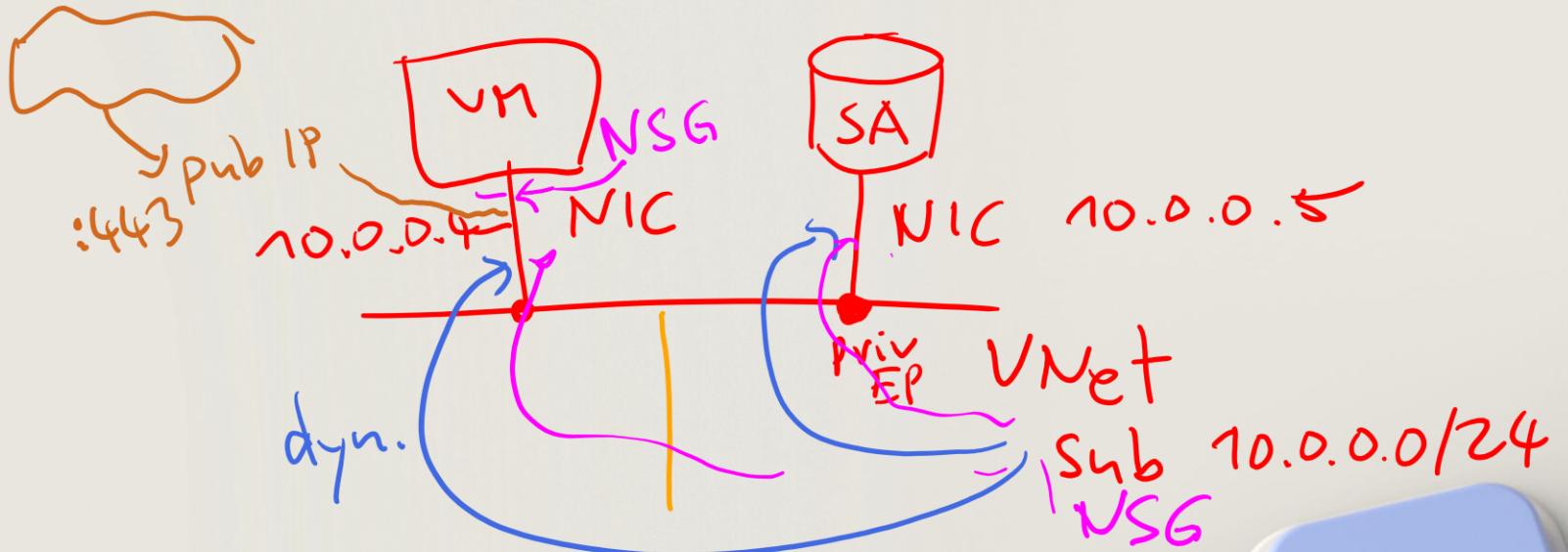
Plan and implement security for public access to Azure resources

Module Labs

Learning Objectives

After completing this learning path, you will be able to:

- 1** Plan and implement security measures for virtual networks, encompassing NSGs, ASGs, UDRs, VNET peering, VPN gateways, Virtual WAN, and network monitoring using Network Watcher.
- 2** Establish private access to Azure resources using Service Endpoints, **Private Endpoints**, Private Link services, and secure configurations for App Service, Azure Functions, and Azure SQL Managed Instance.
- 3** Implement security for public Azure access, including TLS application integration, Azure Firewall, Application Gateway, Front Door, WAF, and recommendations for Azure DDoS Protection.



Plan and implement security for virtual networks

peering

VNet2
Sub 10.1.0.0/24

Plan and implement security for virtual networks

- 1 Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
 - 2 Plan and implement user-defined routes (UDRs)
 - 3 Plan and implement VNET peering or VPN gateway
 - 4 Plan and implement Virtual WAN, including secured virtual hub
 - 5 Secure VPN connectivity, including point-to-site and site-to-site
 - 6 Implement encryption over ExpressRoute
 - 7 Configure firewall settings on PaaS resources
 - 8 Monitor network security by using Network Watcher, including NSG flow logging
- Label "Web-Server"*

Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)



Firewall

Network Security Groups

- An NSG can contain any number of rules within Azure subscription limits.
- For each security rule, you can specify source, destination, port, and protocol.
- Rules are evaluated and applied based on the five-tuple (source, source port, destination, destination port, and protocol) information.
- Modifying NSG rules will only impact the new connections that are formed.
- Use augmented security rules to simplify security definition for virtual networks.



Label

Application Security Groups

- ASGs enable you to reuse your security policy at scale without manual maintenance of explicit IP addresses.
- The rules that specify an ASG as the source or destination are only applied to the network interfaces that are members of the ASG.
- ASGs have some limitations, such as:
 - All network interfaces assigned to an ASG must exist in the same virtual network that the first network interface assigned to the ASG is in.

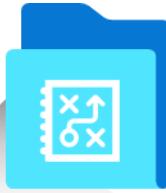
Network Virtual Appliance (NVA)

Plan and implement User-Defined Routes (UDRs)



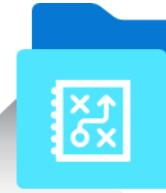
You can create a route table and associate it to zero or more virtual network subnets.

Each subnet can have zero or one route table associated to it.



By default, the table's routes are combined with the subnet's default routes.

In case of conflicting route assignments, user-defined routes override the default routes.



You can specify the following next hop types when creating a user-defined route:

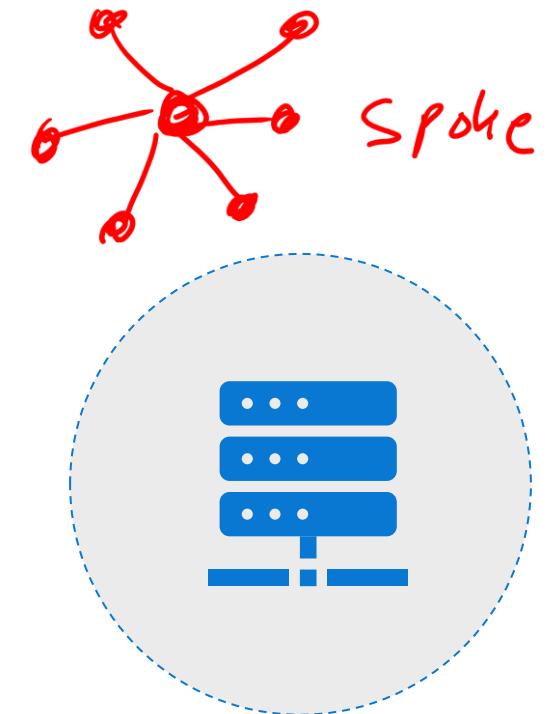
- Virtual appliance
- Virtual network gateway
- None
- Virtual network
- Internet



You can't specify VNet peering or VirtualNetworkService Endpoint as the next hop type in user-defined routes.

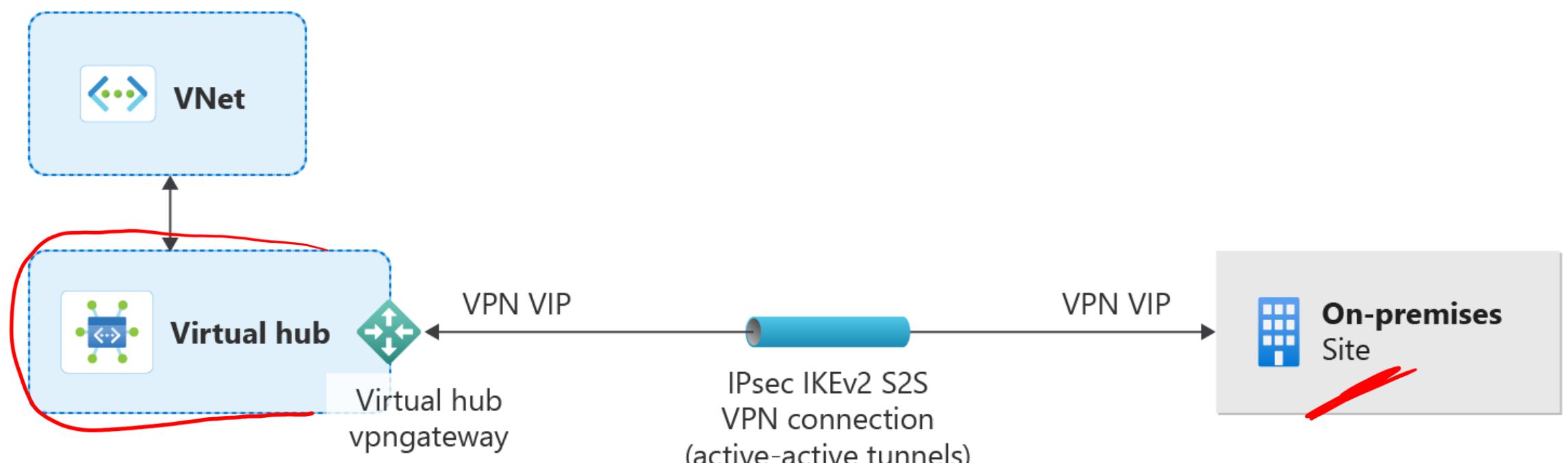
Plan and implement Virtual Network (VNET) peering or VPN gateway

- Azure supports two types of peering:
 - **Virtual network peering**
 - **Global virtual network peering** (have some limitations)
- For peered virtual networks, resources in either virtual network can directly connect with resources in the peered virtual network.
- You can resize the address space of Azure virtual networks that are peered without incurring any downtime on the currently peered address space.
- Use service chaining to direct traffic from one virtual network to a virtual appliance or VPN gateway in a peered network through user-defined routes.
- Both virtual network peering and global virtual network peering support gateway transit.



Plan and implement Virtual WAN, including secured virtual hub

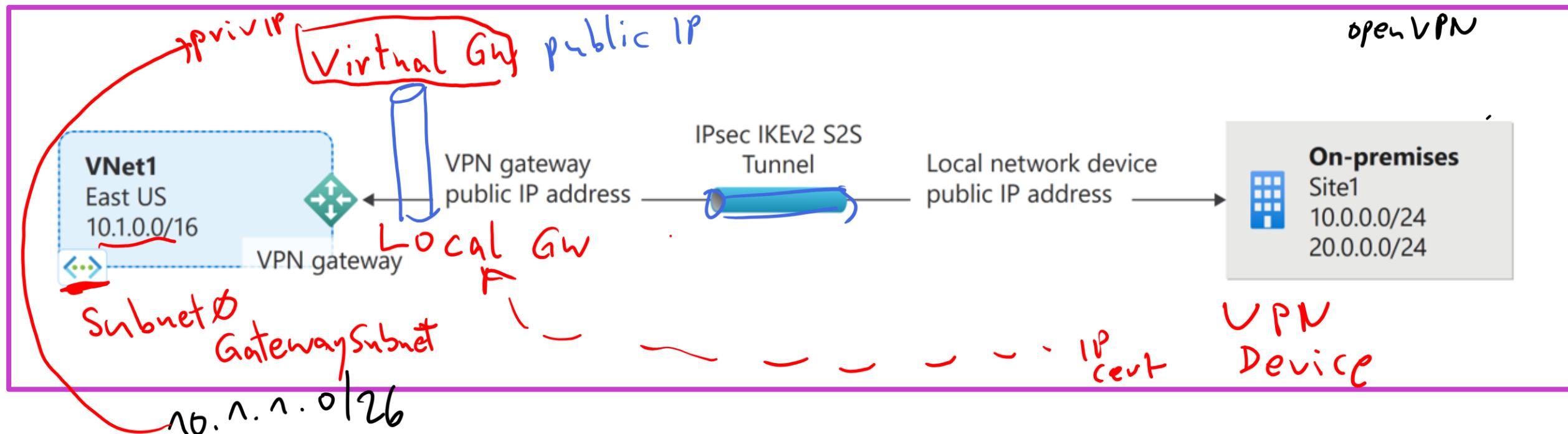
A Virtual WAN uses an IPsec/IKE VPN to connect Azure resources, requiring an on-premises VPN device with a public IP.



Secure VPN connectivity, including site-to-site and point-to-site

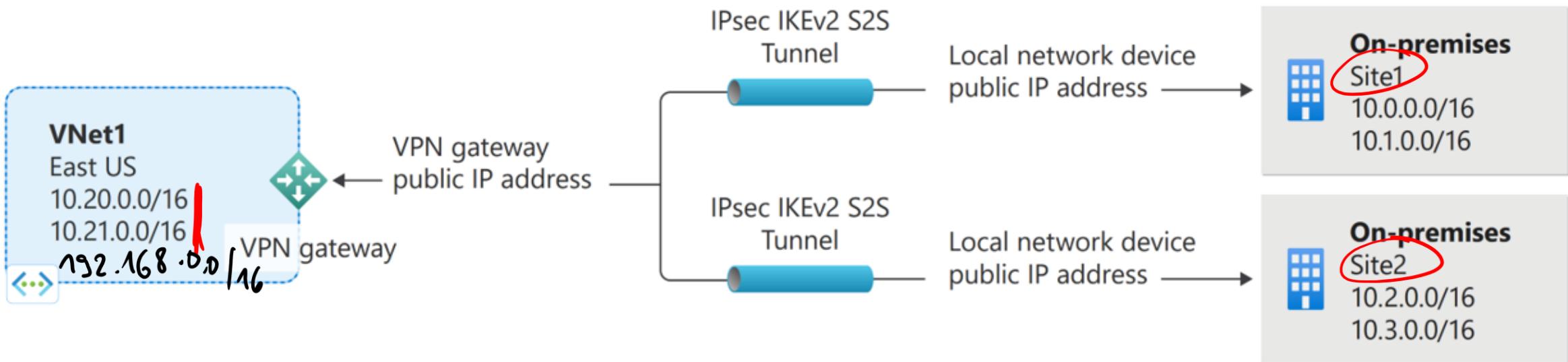
Site-to-site VPN

Point-to-site
IKEv2
SSL



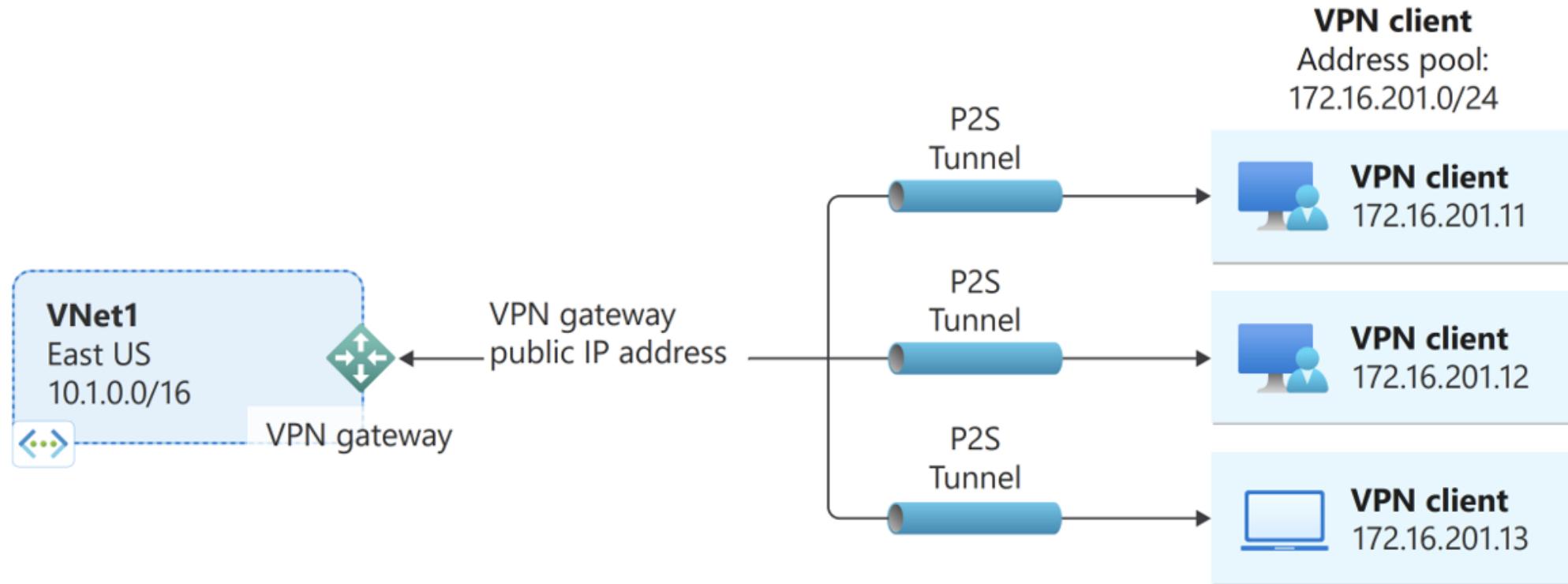
Secure VPN connectivity, including a site-to-site VPN with two IPsec IKEv2 tunnels

Site-to-site VPN (Two IPsec IKEv2 S2S Tunnels)



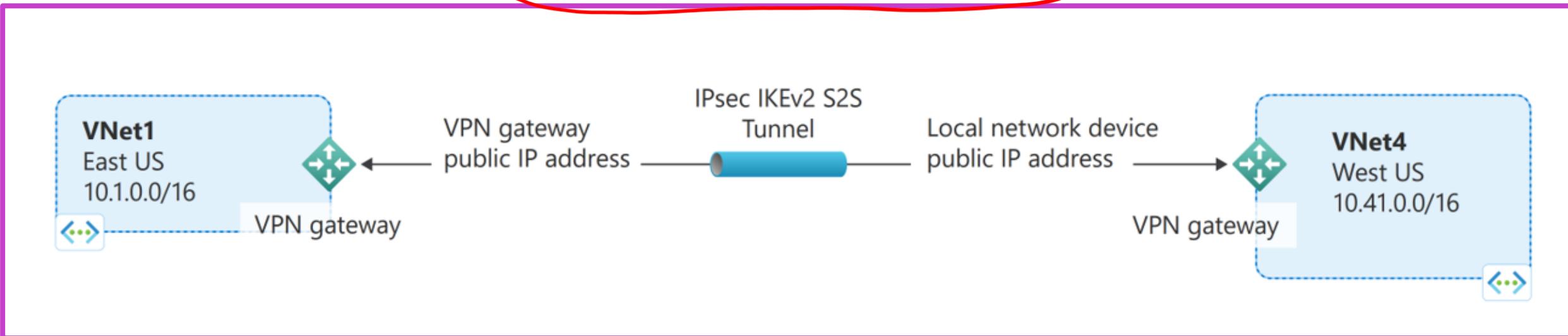
Point-to-site Virtual Private Network

Point-to-site (P2S) VPN gateway connection



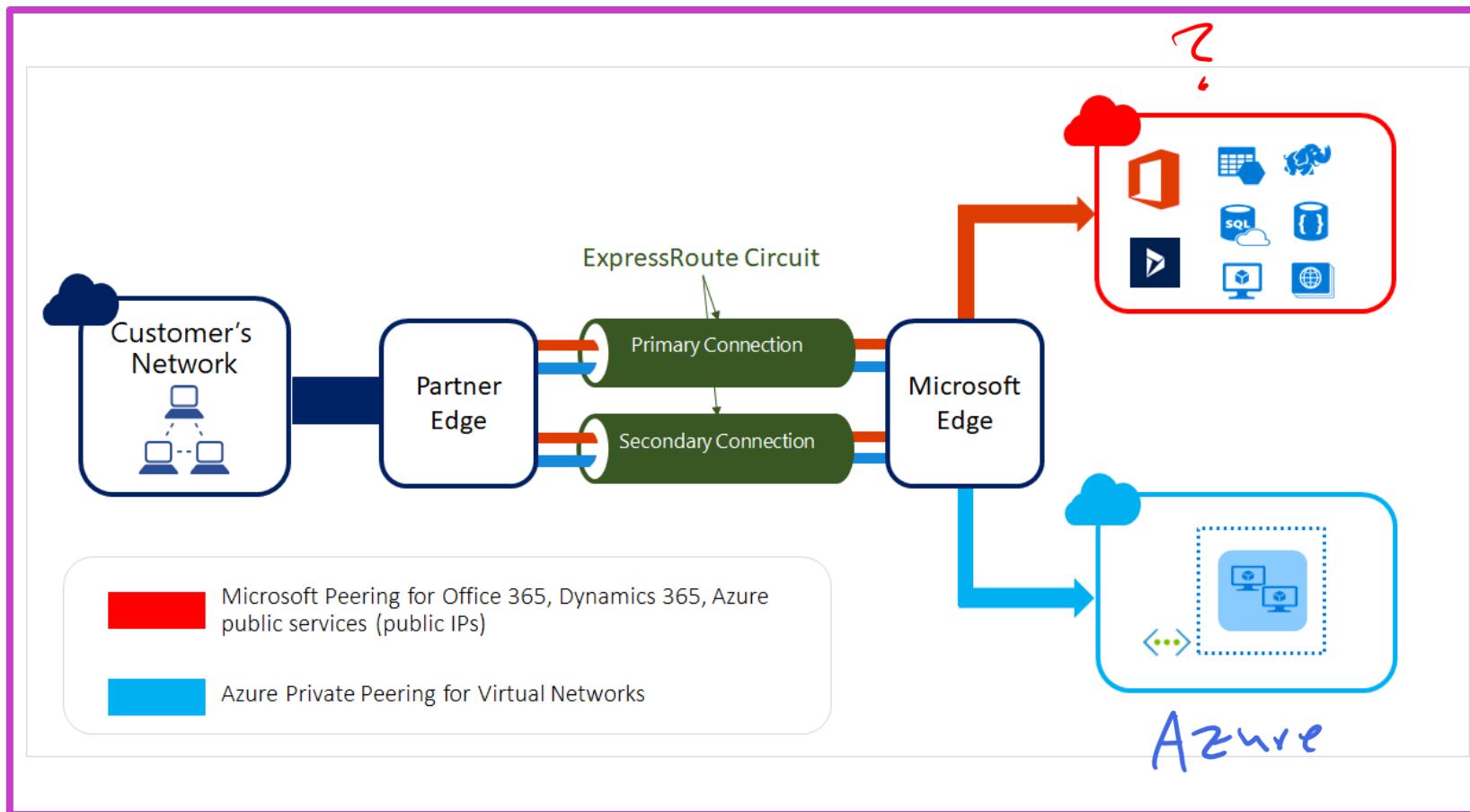
VNet-to-VNet connections (Internet Protocol Secure/Internet Key Exchange Virtual Private Network Tunnel)

statt peering

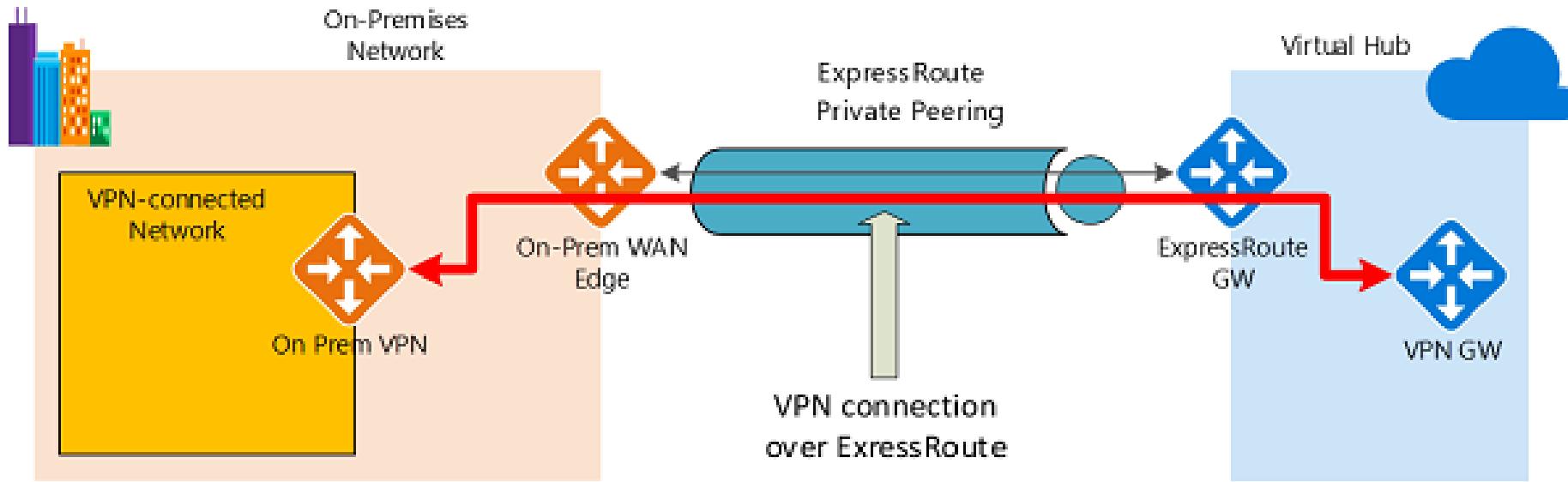


Azure ExpressRoute

- ExpressRoute provides **private connections** between **on-premises networks** and **Microsoft cloud services**, offering higher security, speed, and reliability than the internet.
- Supports various connectivity models including **IP VPN**, **point-to-point Ethernet**, and **colocation facility cross-connections**, with benefits like global reach and dynamic routing.
- Features include **Layer 3 connectivity via BGP**, built-in redundancy for reliability, access to Azure and Microsoft 365, and bandwidth options ranging from 50 Mbps to 10 Gbps.



Azure ExpressRoute Encryption



Azure Virtual WAN Connection

- Azure Virtual WAN offers encrypted IPsec/Internet Key Exchange (IKE) VPN connections via ExpressRoute, avoiding public internet.

Traffic Paths to Azure

- Two routes exist from on-premises to Azure - one encrypted IPsec-protected path and one direct ExpressRoute path. For encryption, the VPN route should be prioritized over ExpressRoute.

Azure to On-Premises Traffic

- Ensure encrypted IPsec path preference either by advertising more specific prefixes on the VPN Border Gateway Protocol (BGP) session or using disjoint prefixes for VPN and ExpressRoute.

Configure firewall settings on PaaS resources

To configure firewall settings, choose from the following options:



Azure native controls: Azure Firewall and the web application firewall in Application Gateway offer basic security. It is simple to set up and configure.



Third-party offerings: This option includes next-generation firewall (NGFW) and other third-party offerings, and its configuration might be more complex.

The location of ExpressRoute connection can affect how the firewall works. You have these options to terminate ExpressRoute in existing (on-premises) networks:



Terminate outside the firewall (the perimeter network paradigm)

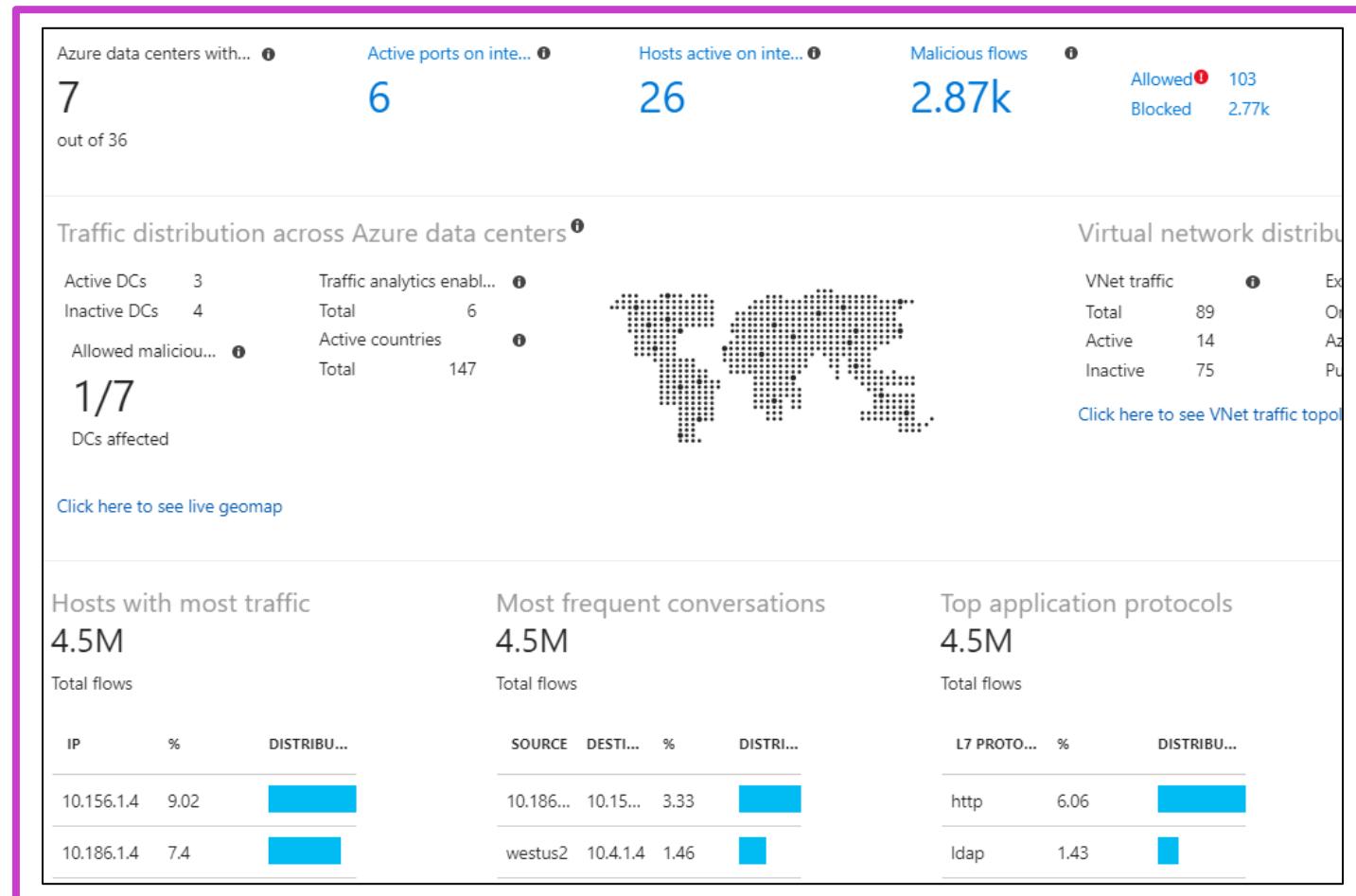


Terminate inside the firewall (the network extension paradigm) [default recommendation]

Monitor network security by using Network Watcher, including NSG flow logging

- Utilize Network Watcher's connection monitor to regularly assess VM-endpoint communication for reachability, latency, and network topology changes.
- Apply network performance monitor to oversee performance across different network infrastructure points and use topology capability for understanding virtual network resource relationships.
- Examine NSG flow logs with tools like Power Business Intelligence for network monitoring, usage optimization, and compliance purposes.

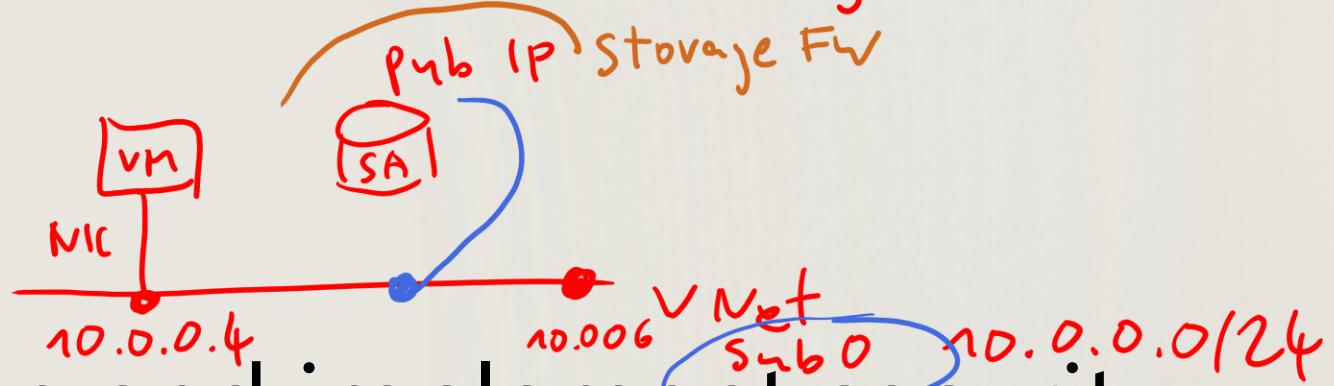
Example of analytics from NSG flow log data



Demonstrations: Network connectivity

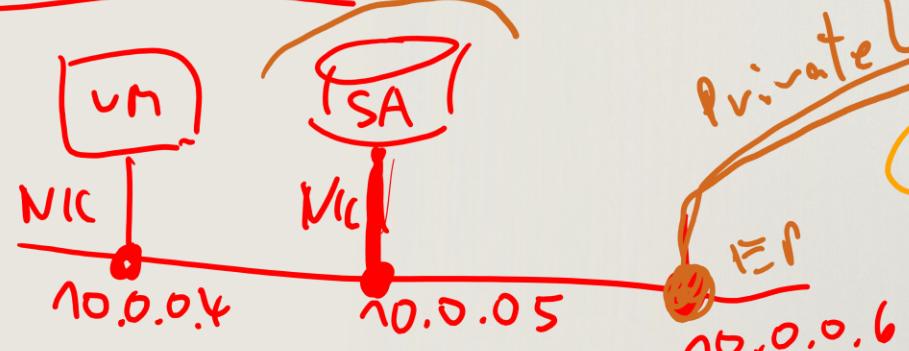
- 1 Network Security Groups
- 2 Application Security Groups

a) Service EP (Routing)



Plan and implement security
for private access to Azure
resources

b) Private EP (NIC Interface)



Plan and implement security for private access to Azure resources

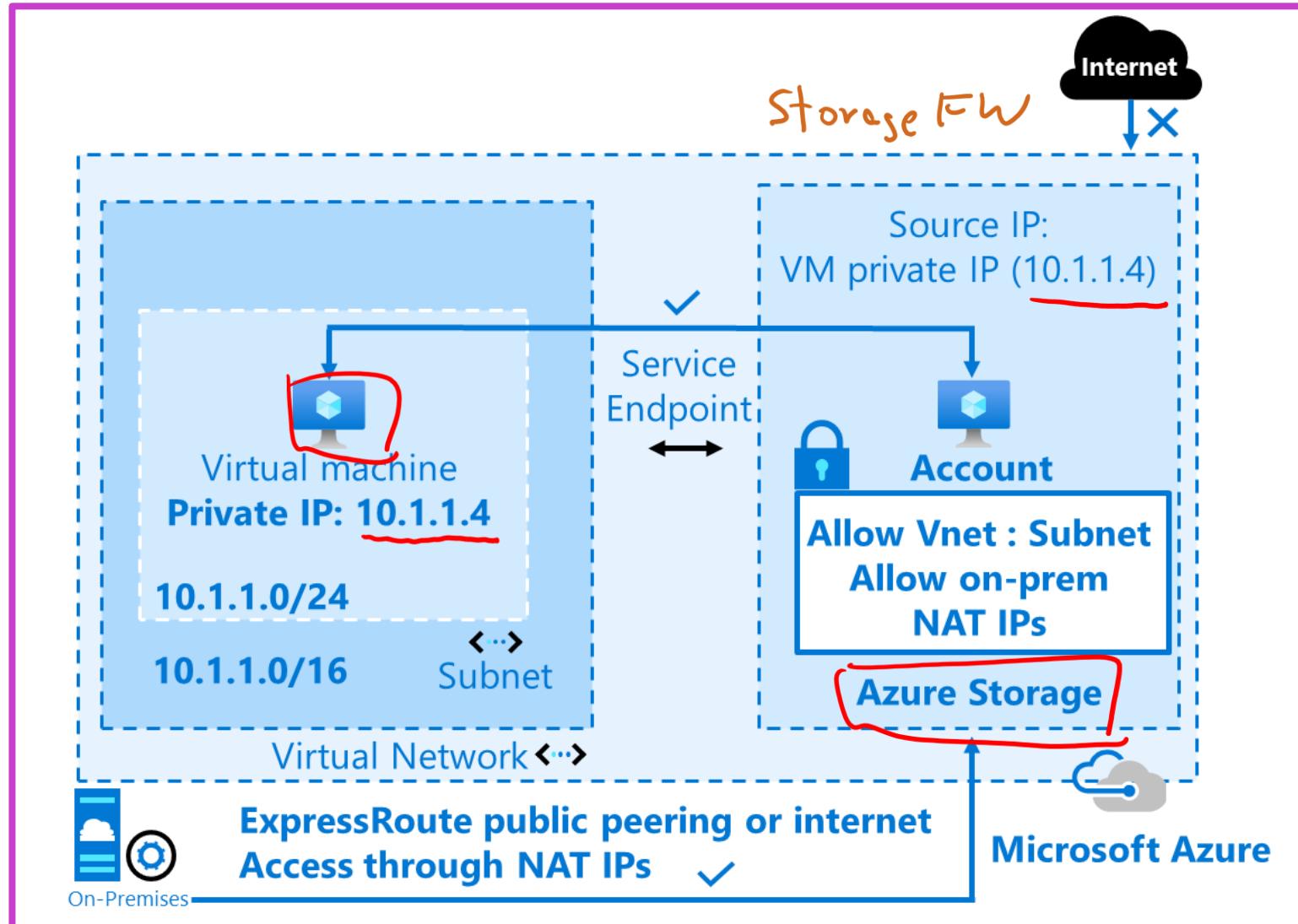
- 1** Plan and implement virtual network Service Endpoints
- 2** Plan and implement Private Endpoints
- 3** Plan and implement Private Link services
- 4** Plan and implement network integration for Azure App Service and Azure Functions
- 5** Plan and implement network security configurations for an App Service Environment (ASE)
- 6** Plan and implement network security configurations for an Azure SQL Managed Instance

Lab

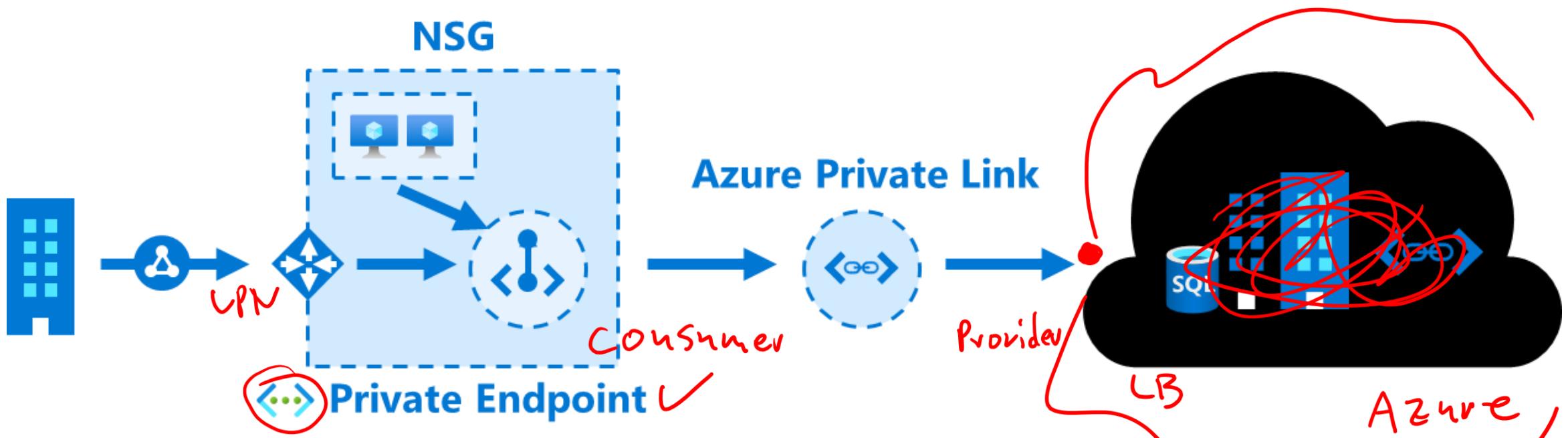
Plan and implement virtual network Service Endpoints

- Endpoints limit network access to specific subnets and IP addresses
- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Endpoints use the Microsoft Azure backbone network
- Simple to set up with less management overhead

Cost ?



Plan and implement Private Endpoints



Private connectivity to services on Azure

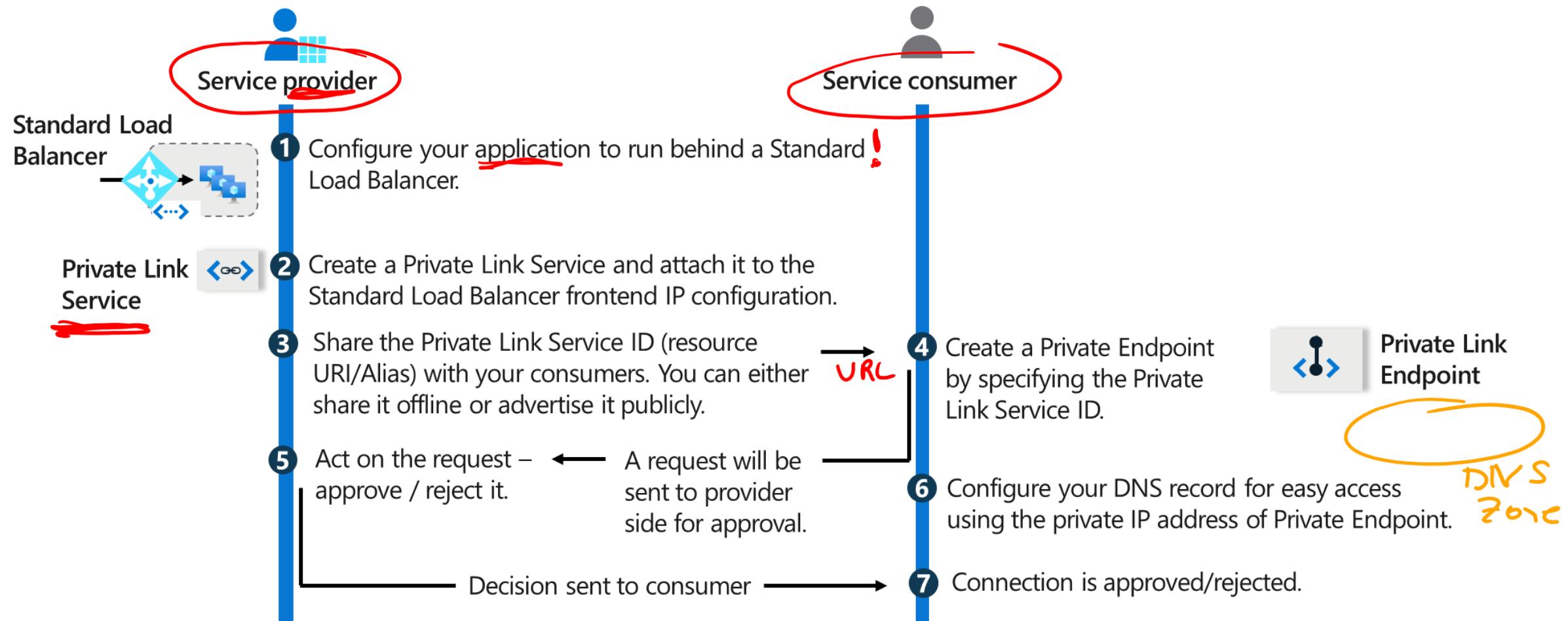
Integration with on-premises and peered networks

Traffic remains on the Microsoft network, with no public internet access

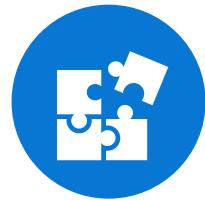
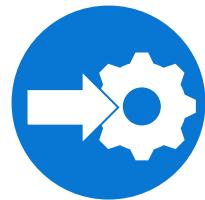
During a security incident within your network, only the mapped resource would be accessible

Plan and implement Private Link services

Remember the following key aspects while planning and implementing Private Link services:



Plan and implement network integration for Azure App Service and Azure Functions



Integration features	Network integration for Azure App Service and Azure Functions
Gateway-required virtual network integration	For network integration of Azure App Service and Azure Functions, you can connect directly to a virtual network in other regions or to a classic virtual network in the same region.
Regional virtual network integration	For network integration of Azure App Service and Azure Functions, you can connect to virtual networks in the same region by having a dedicated subnet in the virtual network you're integrating with.

Plan and implement network security configurations for an App Service Environment (ASE)

Remember these key considerations while you plan and implement network security configurations for an ASE:



Implement Virtual Network Integration



Optimize Network Security Groups (NSGs)



Enhance Security with Azure Private Link



Limit Public Network Exposure



Integrate DDoS Protection



Implement and Fine-Tune the Web Application Firewall (WAF)

Plan and implement network security configurations for an Azure SQL Managed Instance

While planning and implementing network security configurations, follow this baseline:



Private Virtual Network Deployment



Leverage Network Security Groups (NSGs)



Incorporate Azure Private Link



Disable Public Network Access



Monitoring with Microsoft Defender for Cloud



Enforce Azure Policies

Plan and implement security for public access to Azure resources

Plan and implement security for public access to Azure resources

- 1** Plan and implement TLS to applications, including Azure App Service and API Management
- 2** Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies
- 3** Plan and implement an Azure Application Gateway
- 4** Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- 5** Plan and implement a Web Application Firewall (WAF)
- 6** Recommend when to use Azure DDoS Protection

Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management

By implementing TLS encryption, you can protect your applications with:



Strong authentication



Ease of deployment and use



Message privacy and integrity



Interoperability between systems



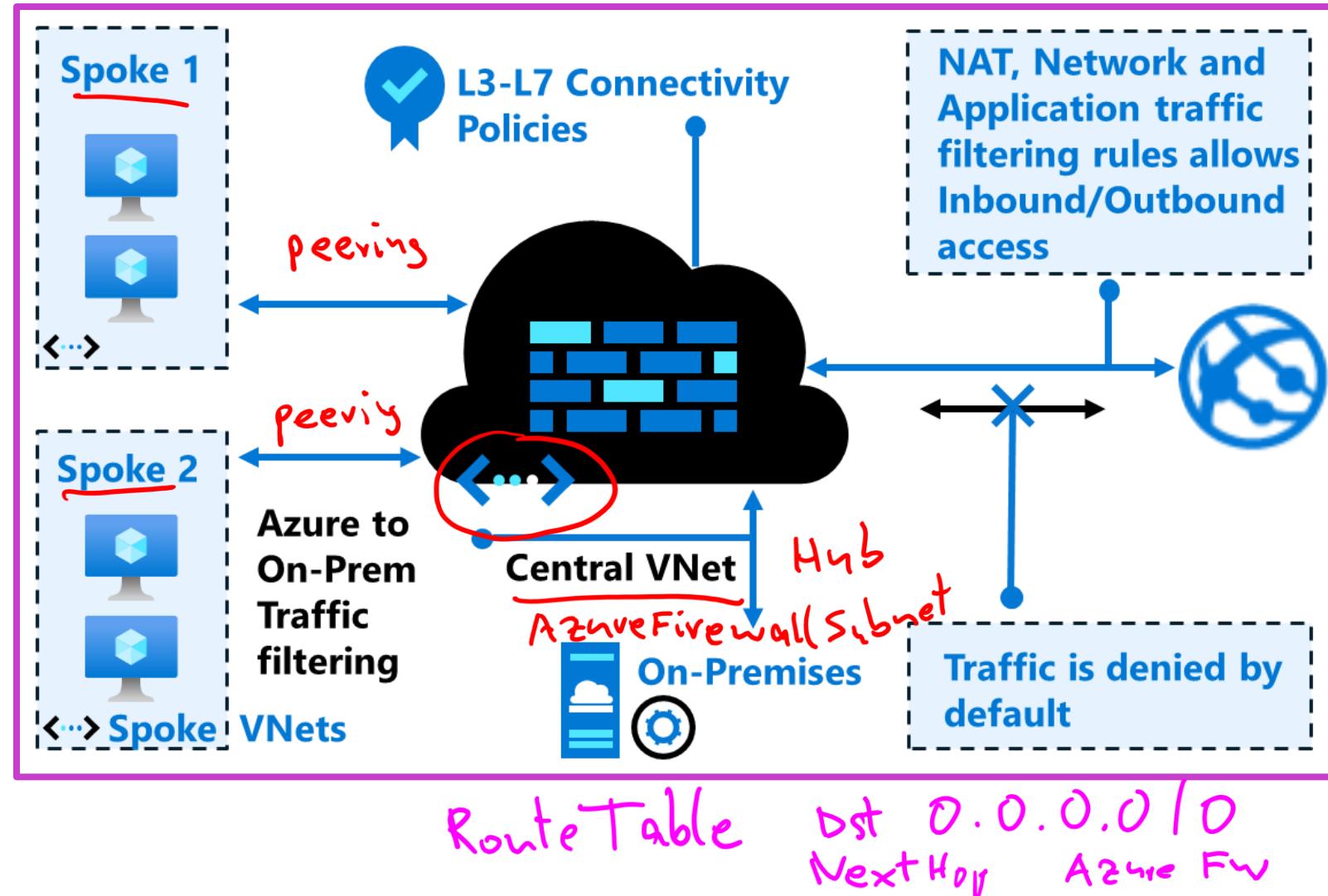
Algorithm flexibility



Perfect Forward Secrecy (PFS)

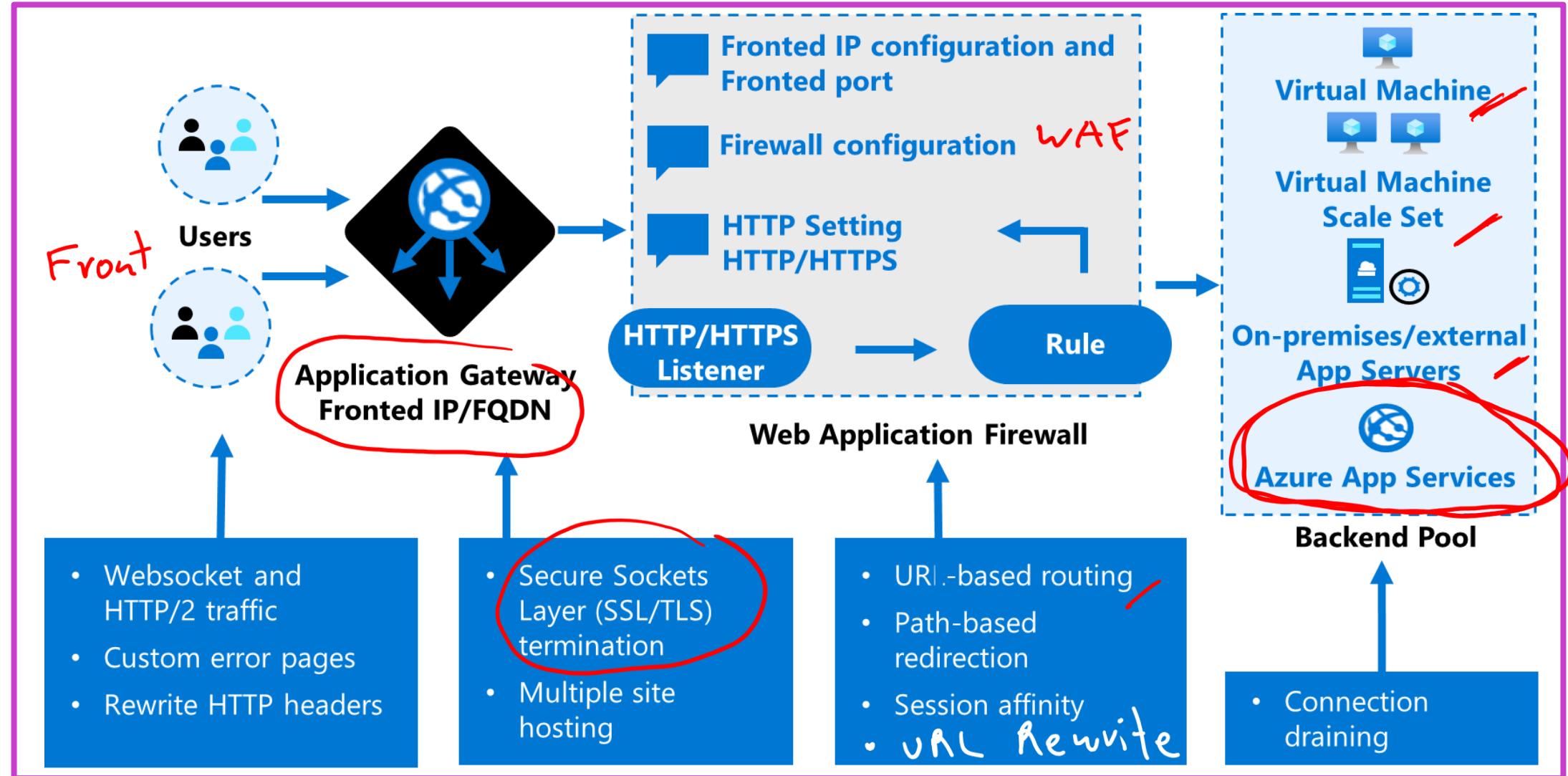
Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies

- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN tags
- Outbound SNAT
- Inbound DNAT support
- L3-L7 connectivity policies
- Separate firewall subnet
- Static public IP address
- Forced tunnelling – Push all internet Traffic for specific next hop (example – on-premises device).



Nic - ASG

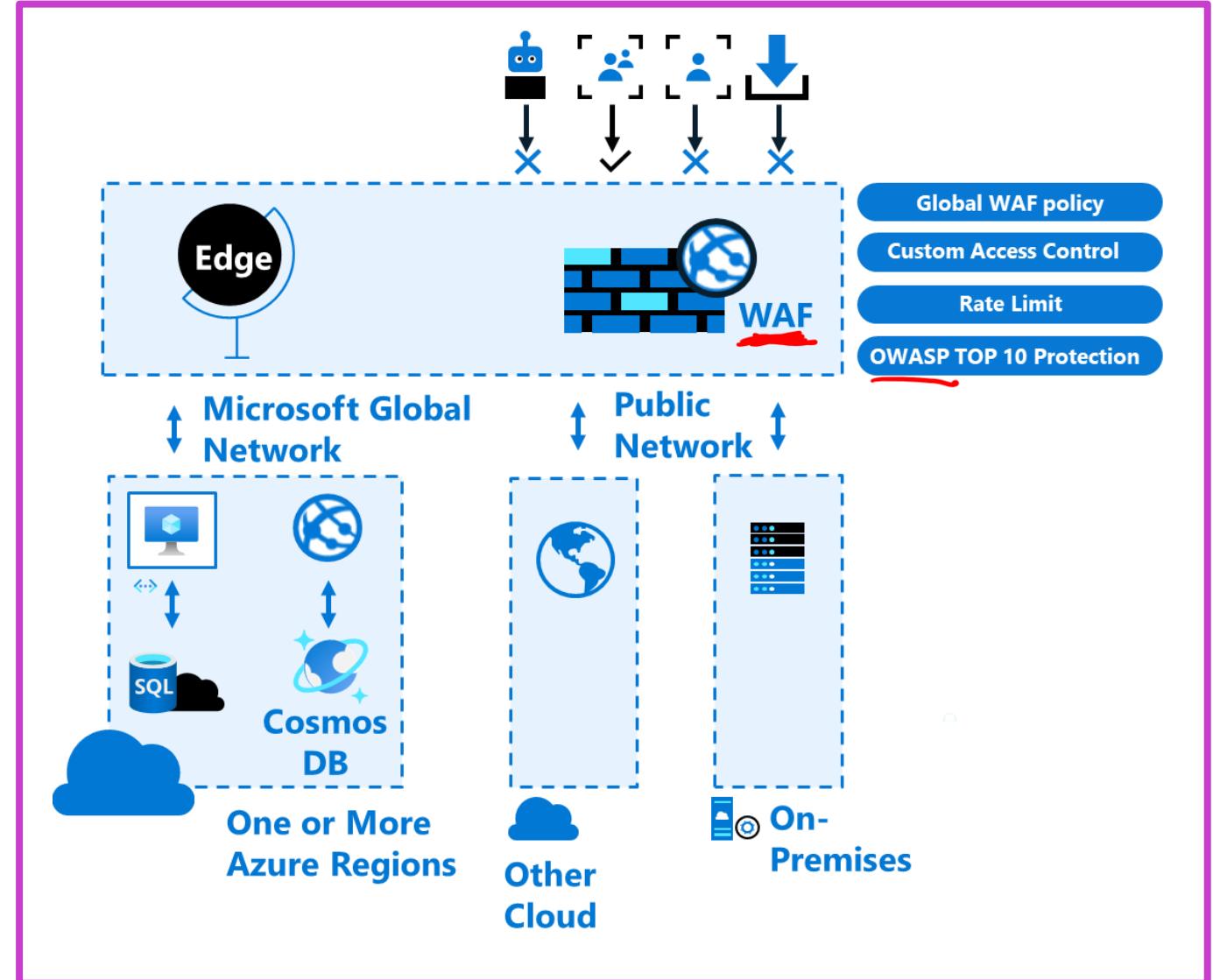
Plan and implement an Azure Application Gateway



Plan and implement a Web Application Firewall (WAF)

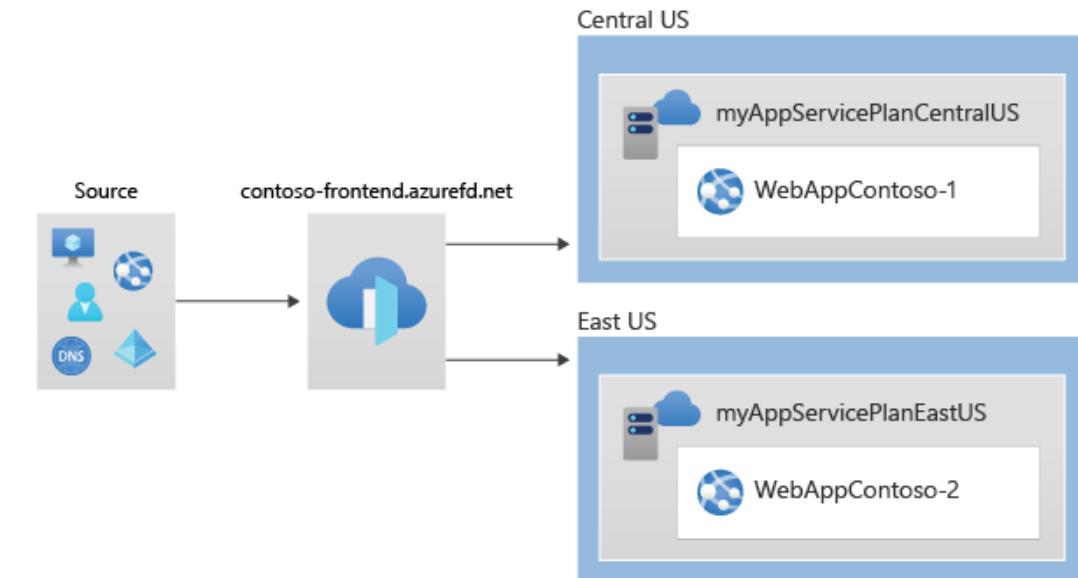
App Gw
Front D...
CDN

- Protects against cross-site scripting and SQL injection
- OWASP Core Rule sets 3.1, 3.0, 2.29
- Custom access control
- Supports Azure Front Door, Azure Application Gateway, and CDN (preview)

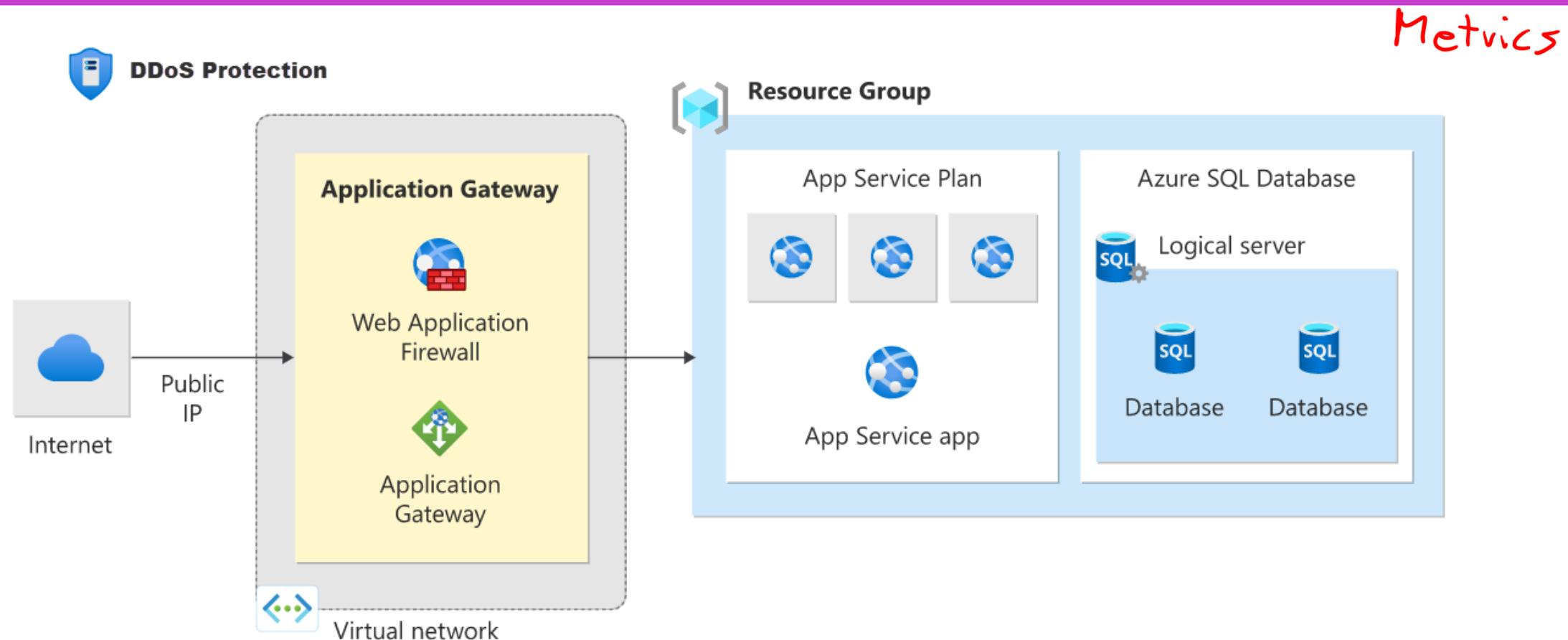


Plan and implement an Azure Front Door, including Content Delivery Network (CDN)

- Layer 7 global routing
- Accelerate application performance with anycast and split TCP
- URL-based routing and session affinity
- Multiple-site hosting
- Custom domains and certificate management
- Application layer security - WAF
- URL redirection and URL rewrite
- Protocol support - IPv6 and HTTP/2 traffic



Recommend when to use Azure DDoS Protection Standard



- **Basic and Standard (multiple subscriptions) service tiers**
- Mitigates volumetric attacks, protocol attacks, and application layer attacks
- Checks for malformed packets and spoofing

Additional study – Network security

Microsoft Learn
Modules
([docs.microsoft.com/
Learn](https://docs.microsoft.com/Learn))



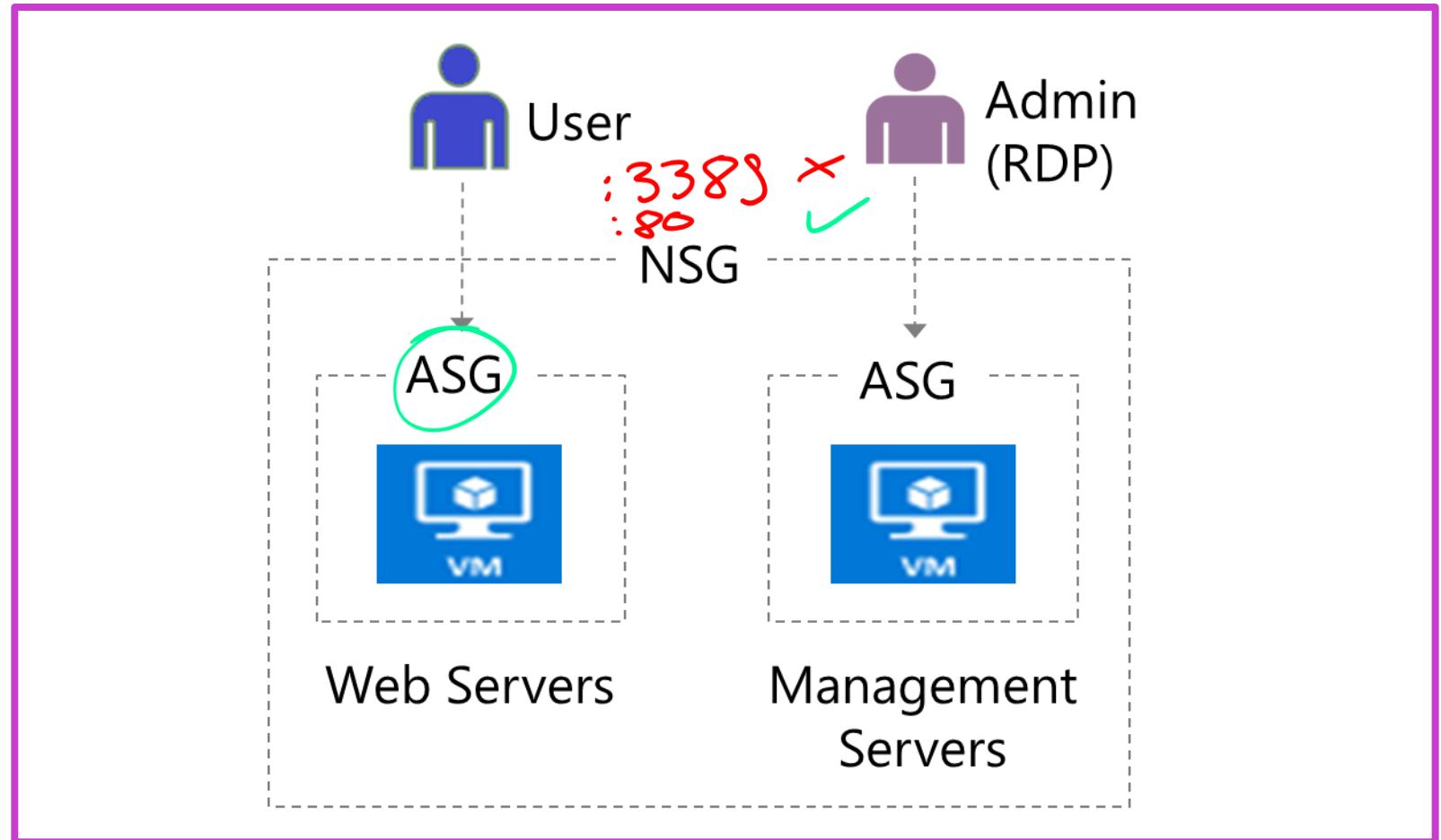
Module Review Questions

- Encrypt network traffic end to end with Azure Application Gateway (Exercise)
- Connect your on-premises network to the Microsoft global network by using ExpressRoute
- Design a hybrid network architecture on Azure
- Secure and isolate access to Azure resources by using network security groups and service endpoints (Exercise)

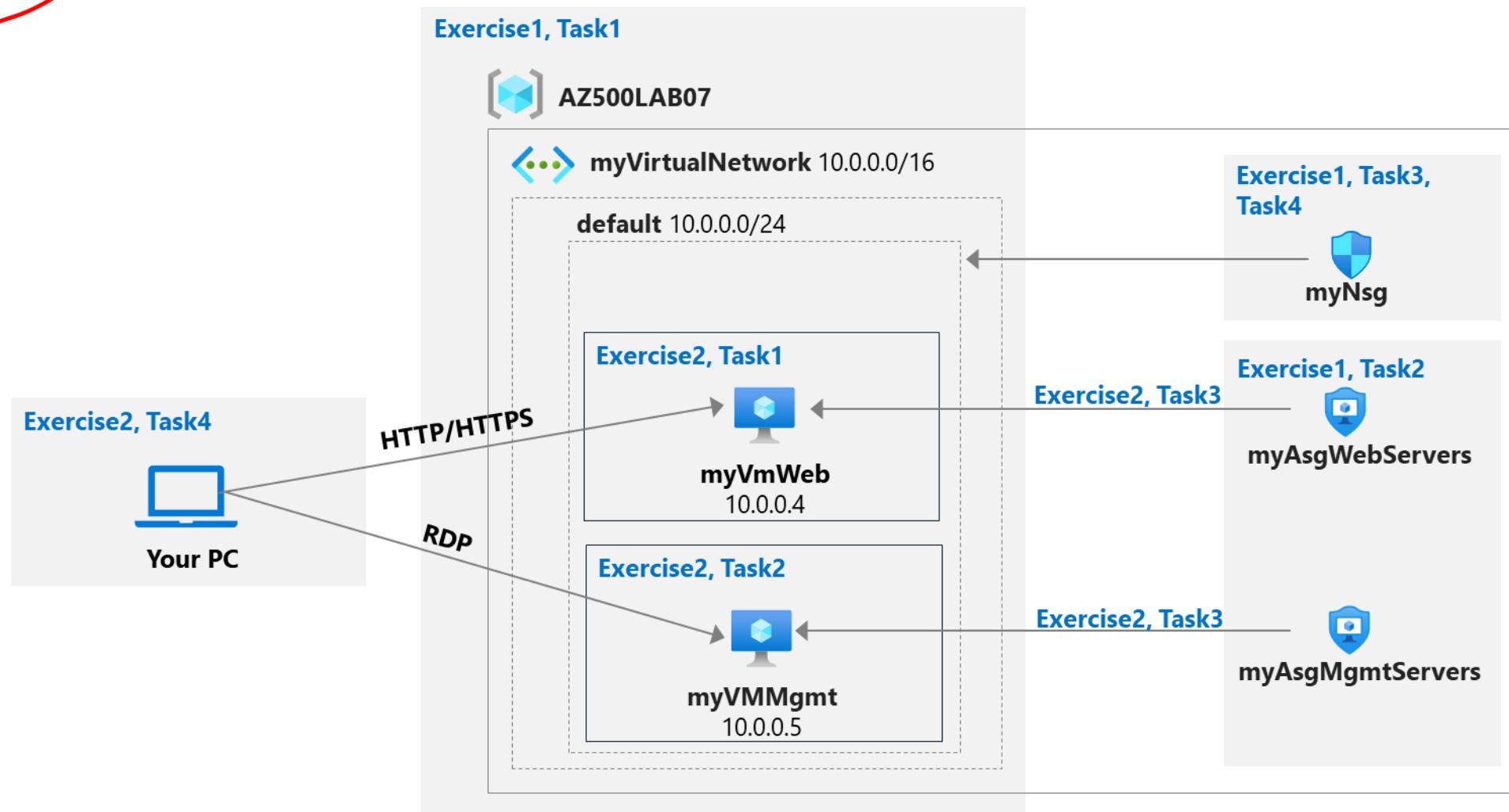
Module Labs

Lab 02 – Network and application security groups

- Create application security groups
- Wrap the ASGs with a Network Security Group (NSG)
- Use NSG rules to route traffic:
 - Admins can RDP to the management servers but not the web servers
 - Users can access the web servers and see the default IIS page

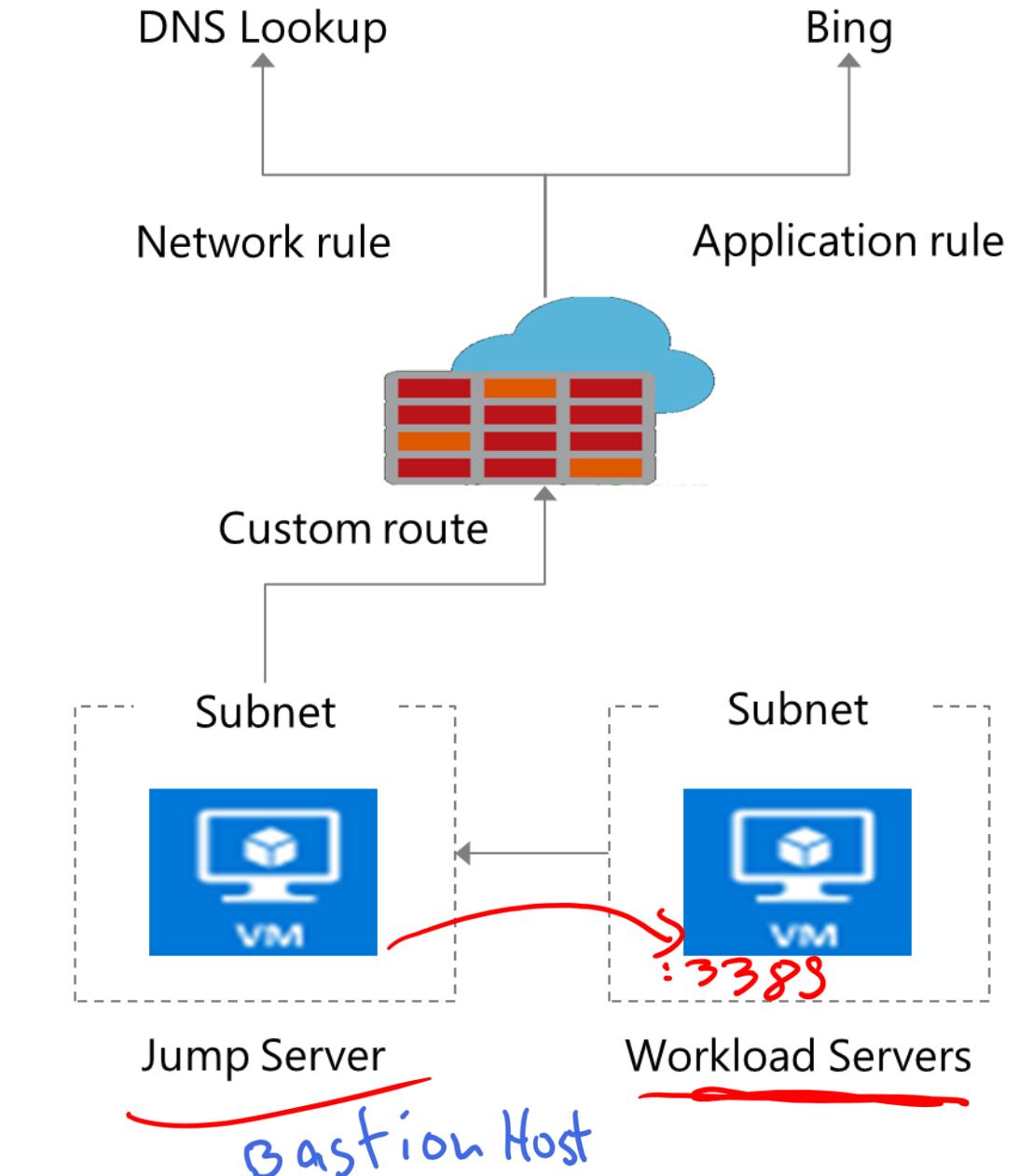


Lab 02 – Network and application security groups



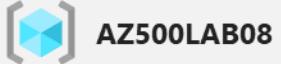
Lab 03 – Azure firewall

- Create a Workload subnet and Jump subnet each with a virtual machine
- Create a custom route to ensure outbound traffic from the workload subnet goes to the firewall
- Create firewall application rules to allow traffic to Bing
- Create firewall network rules to allow traffic to DNS lookup servers



Lab 03 – Azure firewall

Exercise1, Task1



Test-FW-VN 10.0.0.0/16

Exercise1, Task3

Firewall-route



TEST-FW-PIP
TEST-FW01
10.0.1.4

AzureFirewallSubnet 10.0.1.0/24

Exercise1, Task6
Configure the
virtual machine
DNS servers

Srv-Work
10.0.2.4

Workload-SN 10.0.2.0/24

Jump-SN 10.0.3.0/24

Srv-Jump
10.0.3.4

Srv-Jump-PIP

Exercise1, Task7



Your PC

Knowledge check



1 What is the primary purpose of Azure Network Security Groups (NSGs)?

- Managing user access to Azure resources
- Safeguarding data within virtual machines
- Filtering inbound and outbound traffic to and from Azure resources

2 Which security technology is commonly used to establish secure communication between a user's device and a corporate network?

- Intrusion Detection System (IDS)
- Virtual Local Area Network (VLAN)
- Virtual Private Network (VPN)

3 What is the purpose of an Intrusion Detection System (IDS) in host security?

- Protecting data at rest in storage accounts
- Monitoring and detecting unauthorized activities on a host
- Preventing network-based attacks

Learning Path Recap

In this learning path, we:

Learned to secure virtual networks using NSGs, ASGs, UDRs, VNET peering, VPNs, Virtual WAN, ExpressRoute encryption, and Network Watcher monitoring.

Addressed private Azure resource access with Service Endpoints, Private Endpoints, Private Link services, and integrations for App Service, Azure SQL, and ASE.

Delved into public Azure access security through TLS, Azure Firewall, Application Gateway, Front Door, WAF, and Azure DDoS Protection recommendations.

End of presentation