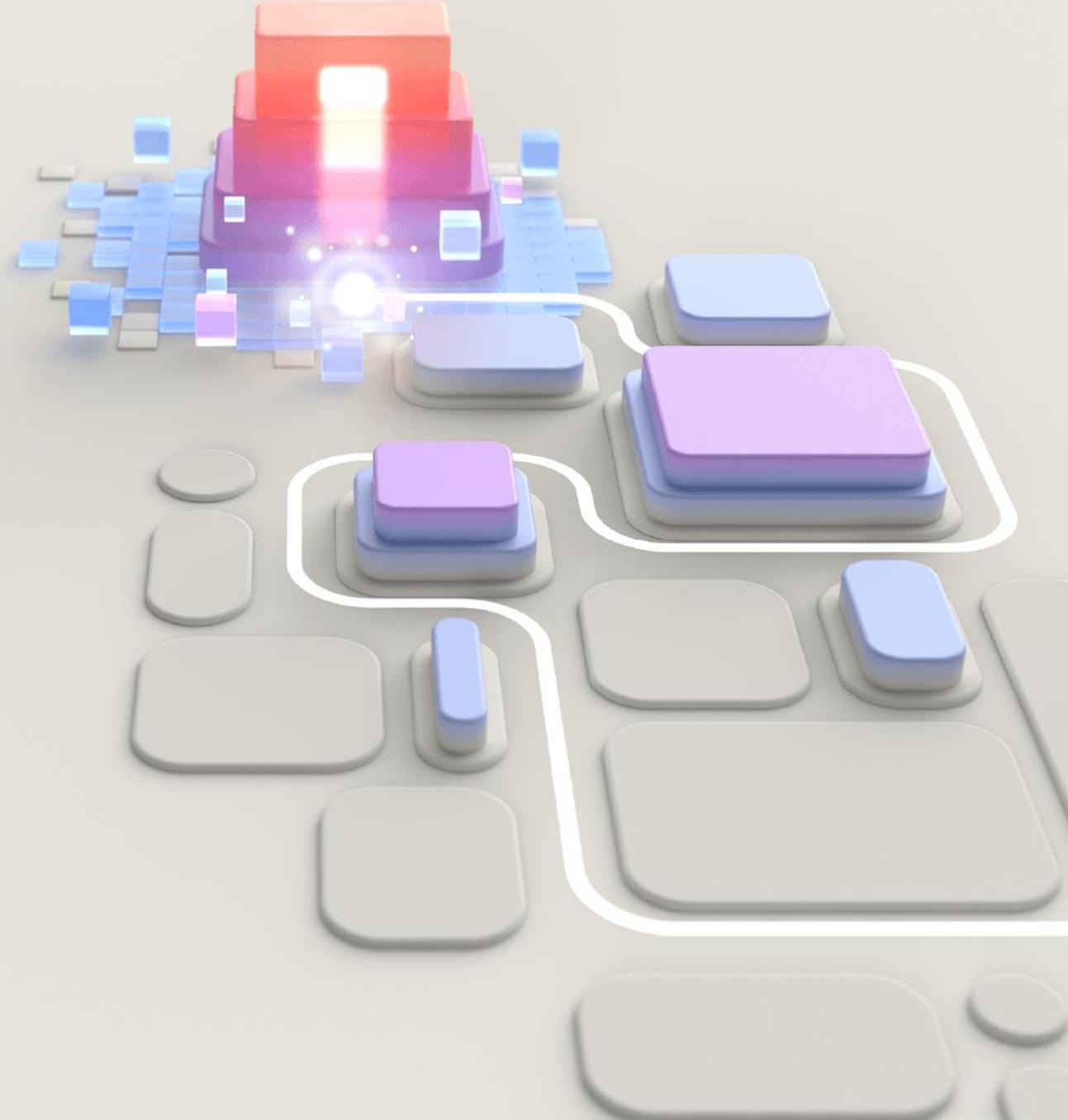


AZ-500
Microsoft Azure
Security Technologies

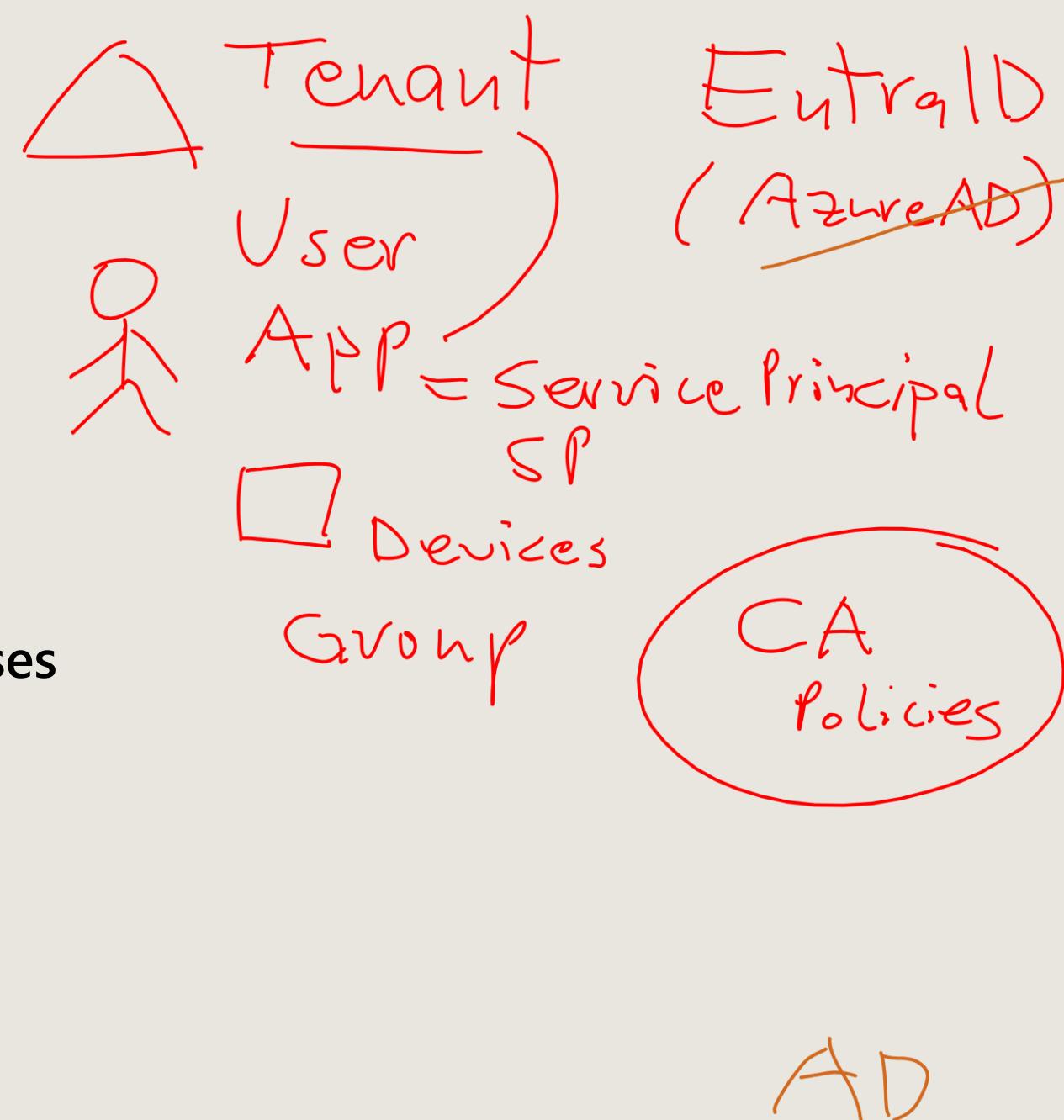
Guten Morgen!

Tag 2



Agenda

- 1 Manage identity and access
- 2 Secure networking
- 3 Secure compute, storage, and databases
- 4 Manage security operations



Learning path: Secure Networking

Plan and implement security for virtual networks

NSG ASG

Peering
VPN

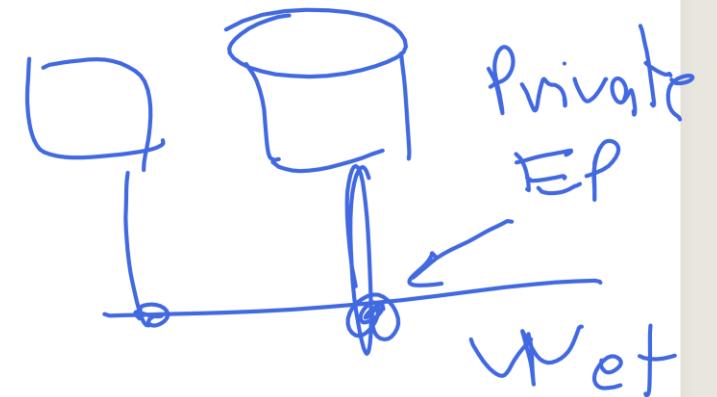
Plan and implement security for private access to Azure resources

Plan and implement security for public access to Azure resources

Module labs

2

NSG - ASG
Azure FW

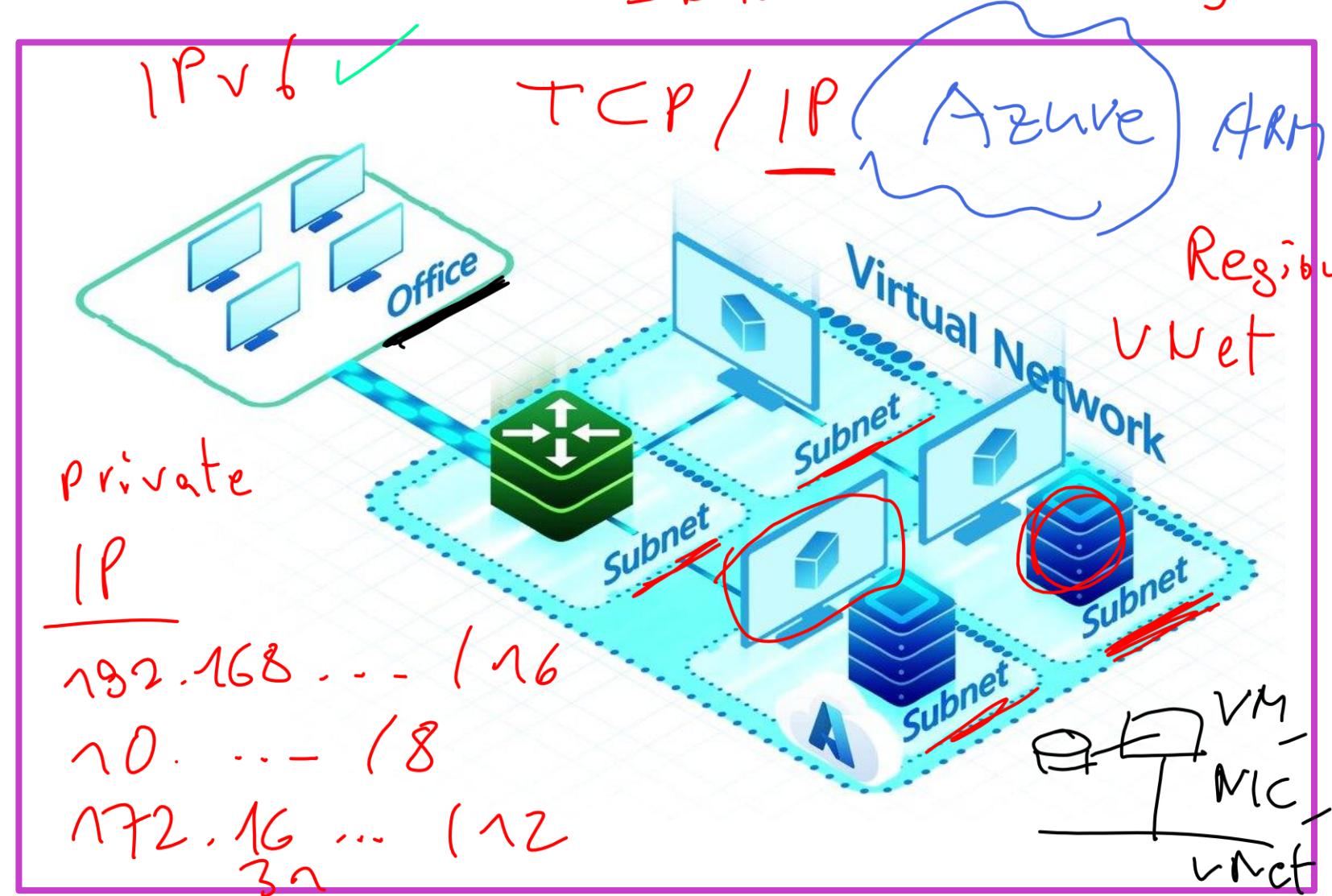


Plan and implement security for virtual networks

Azure Virtual Network

Software Defined
SDN Red Dog

- Azure Virtual Network enables secure communication among Azure resources, the internet, and on-premises networks, providing a scalable and isolated environment.
- It offers extensive networking features like traffic filtering, routing, and integration with Azure services, enhancing connectivity and security.
- Azure manages network configuration, including free control plane operations, while users pay only for resources like VMs.

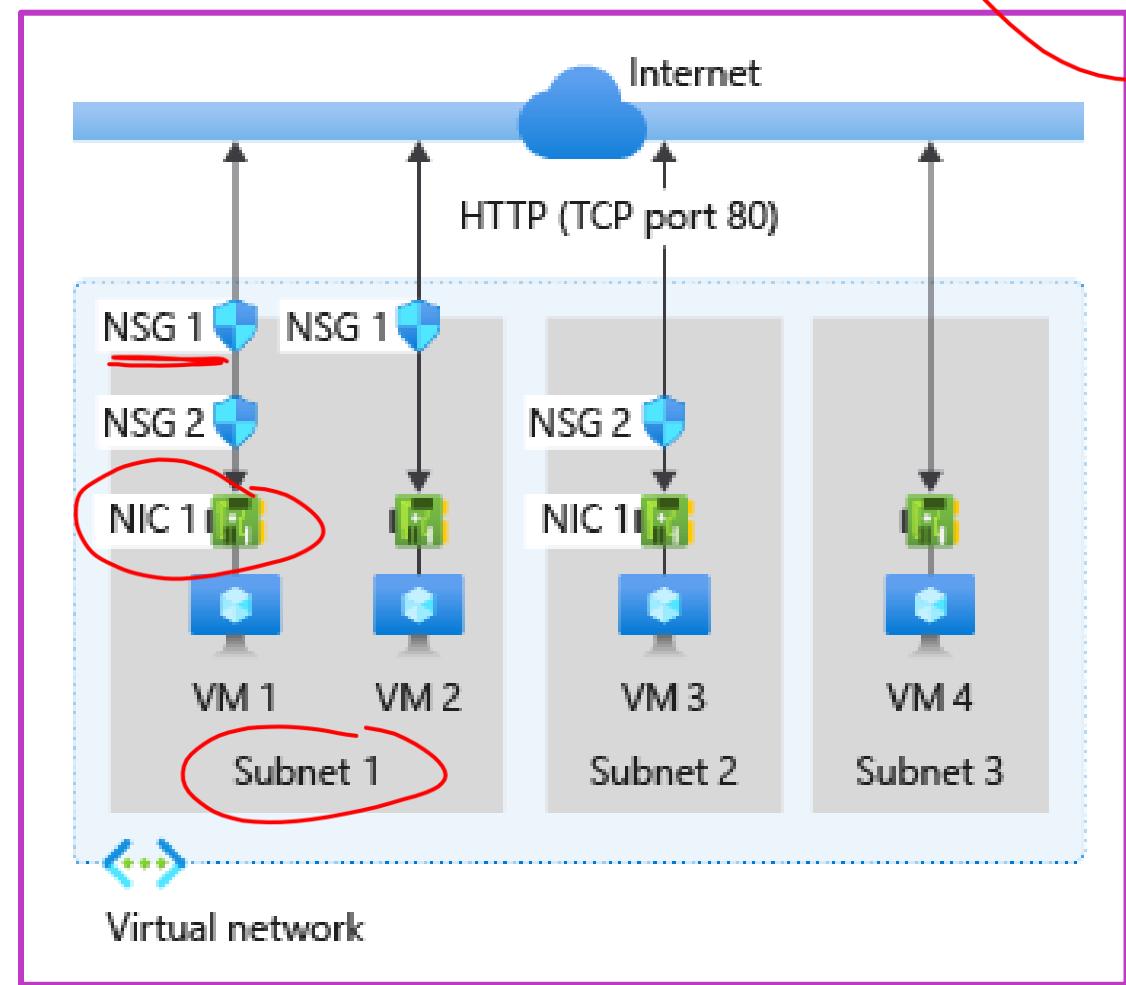


Plan and implement Network Security Groups (NSGs)



Network Security Groups

- Filter network traffic between Azure resources like a firewall.
- 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.

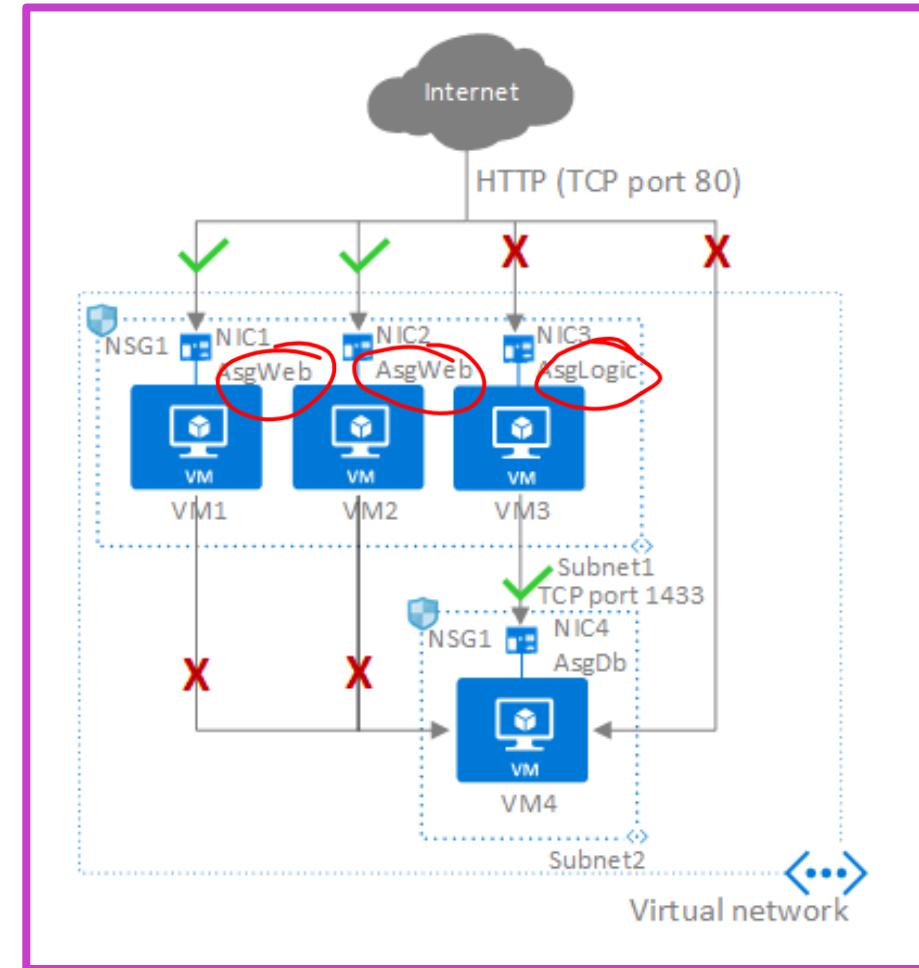


Plan and implement Application Security Groups (ASGs)



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.

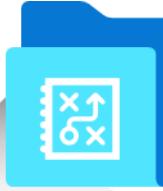


Plan and implement User-Defined Routes (UDRs)



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:

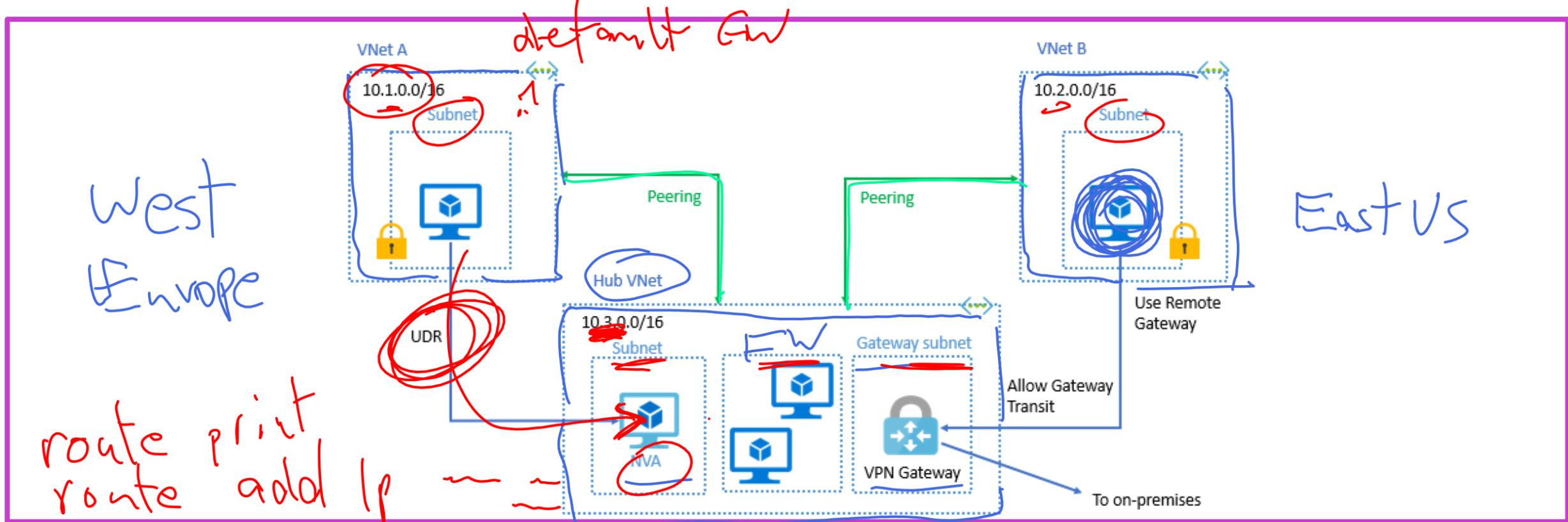
- Virtual appliance
- Virtual network gateway
- None
- Virtual network
- Internet



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



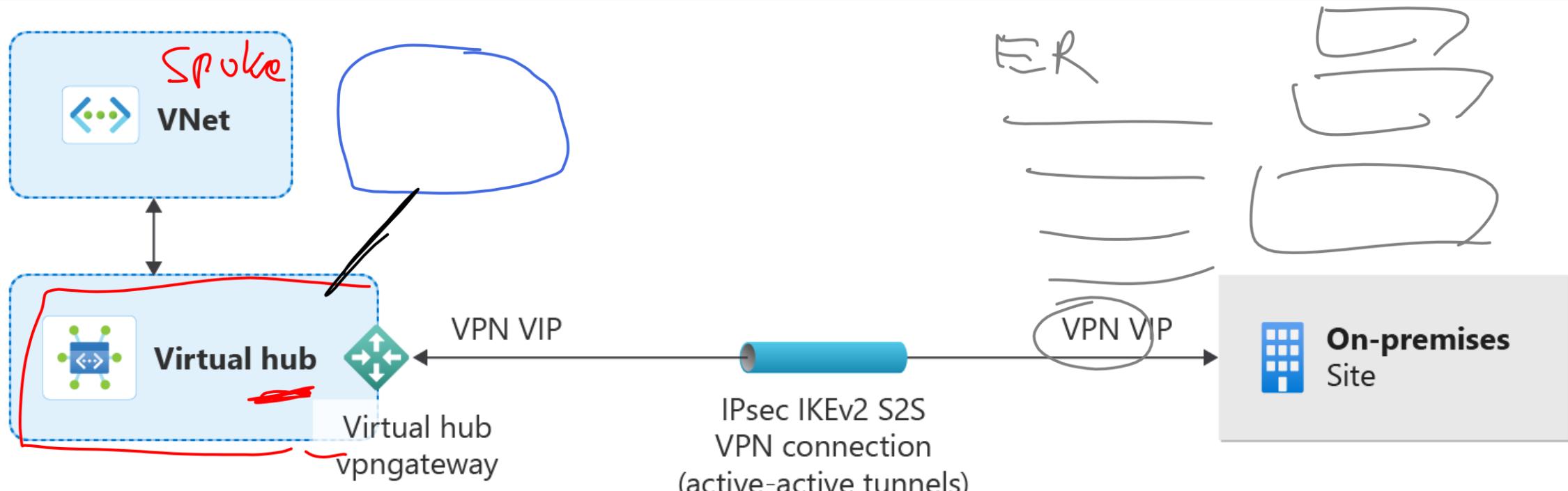
Plan and implement Virtual Network peering or VPN gateway



- Seamless connectivity: Azure virtual network peering connects networks across regions or tenants via Microsoft backbone.
- Scalability and security: Supports up to 1,000 peers with low latency, private traffic, and network security groups.
- Advanced configurations: Enables address resizing, service chaining, and gateway transit for complex topologies.

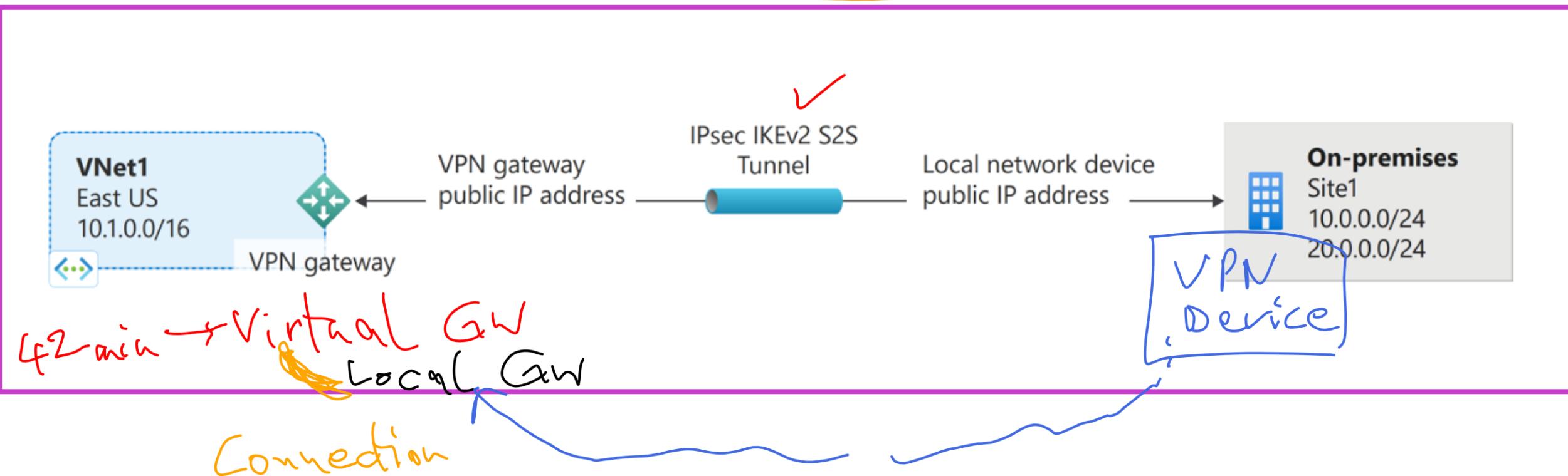
Plan and implement Virtual WAN, including secured virtual hub

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



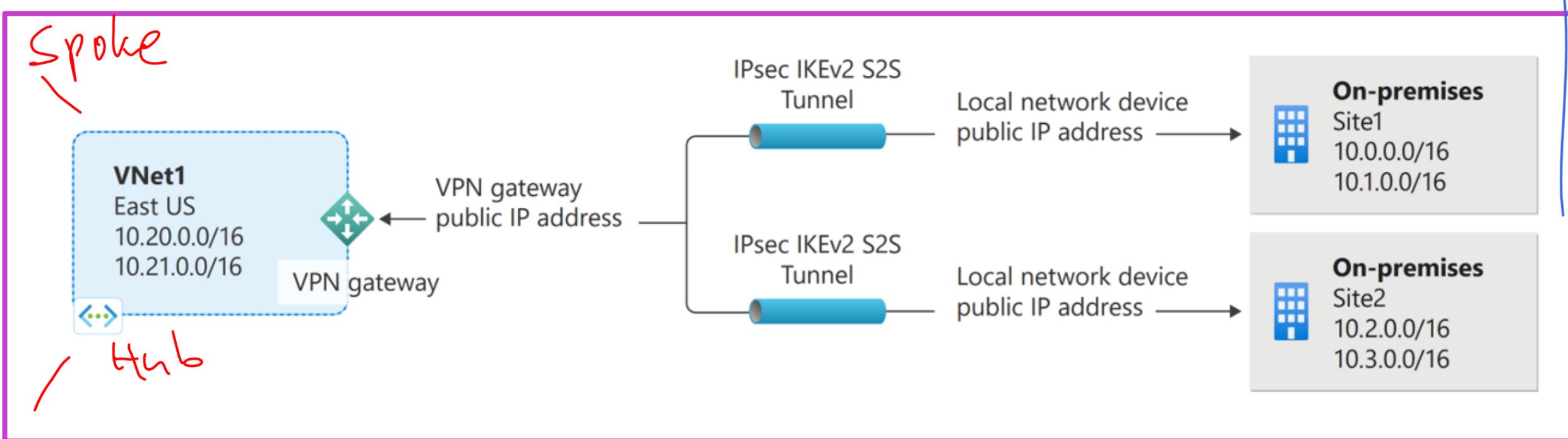
Secure VPN connectivity, including site-to-site and point-to-site

Site-to-site VPN



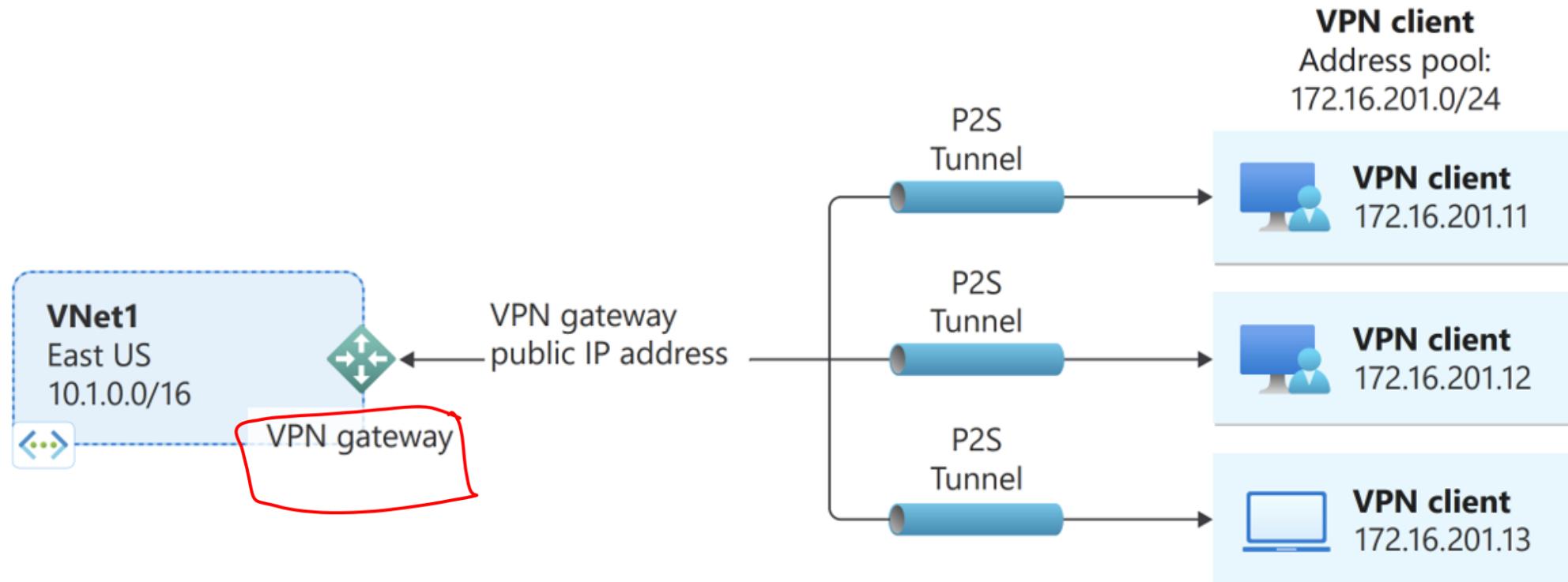
Secure VPN connectivity, including a site-to-site VPN with two IPsec IKEv2 tunnels

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



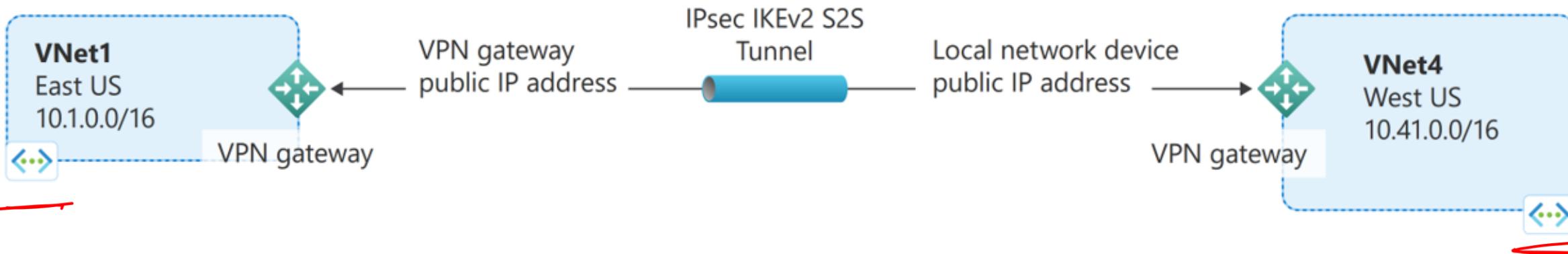
Point-to-site Virtual Private Network

Point-to-site (P2S) VPN gateway connection



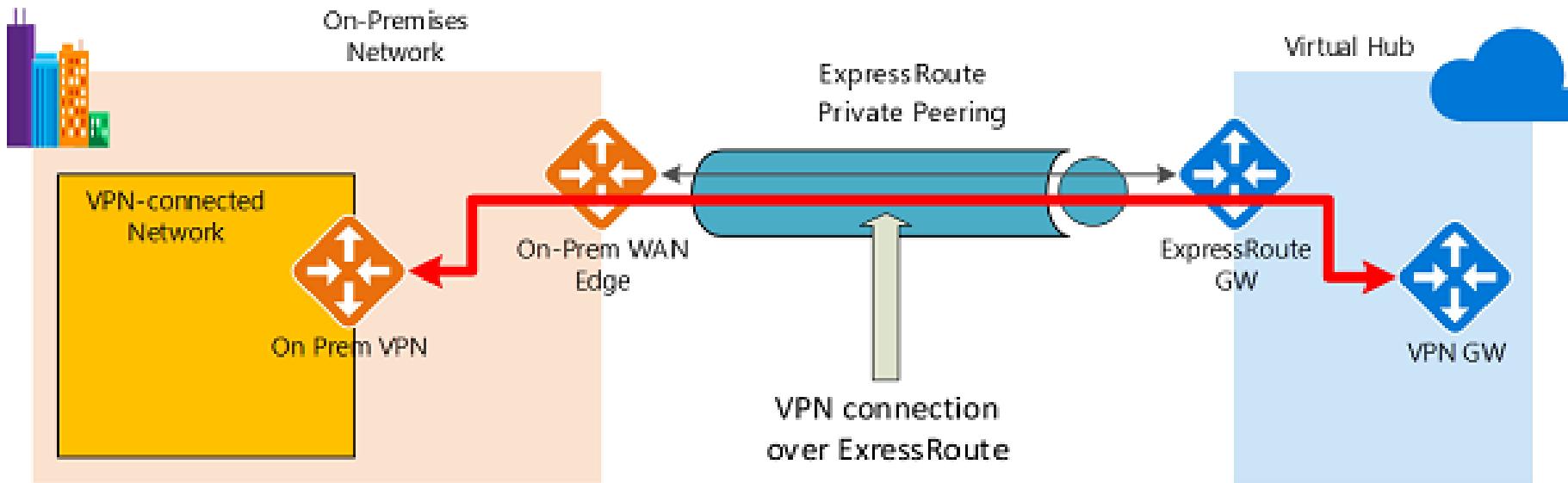
VNet-to-VNet connections (Internet Protocol Secure/Internet Key Exchange Virtual Private Network Tunnel)

VNet-to-VNet connection



Implement encryption over ExpressRoute

NO Ency.



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 Azure 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:

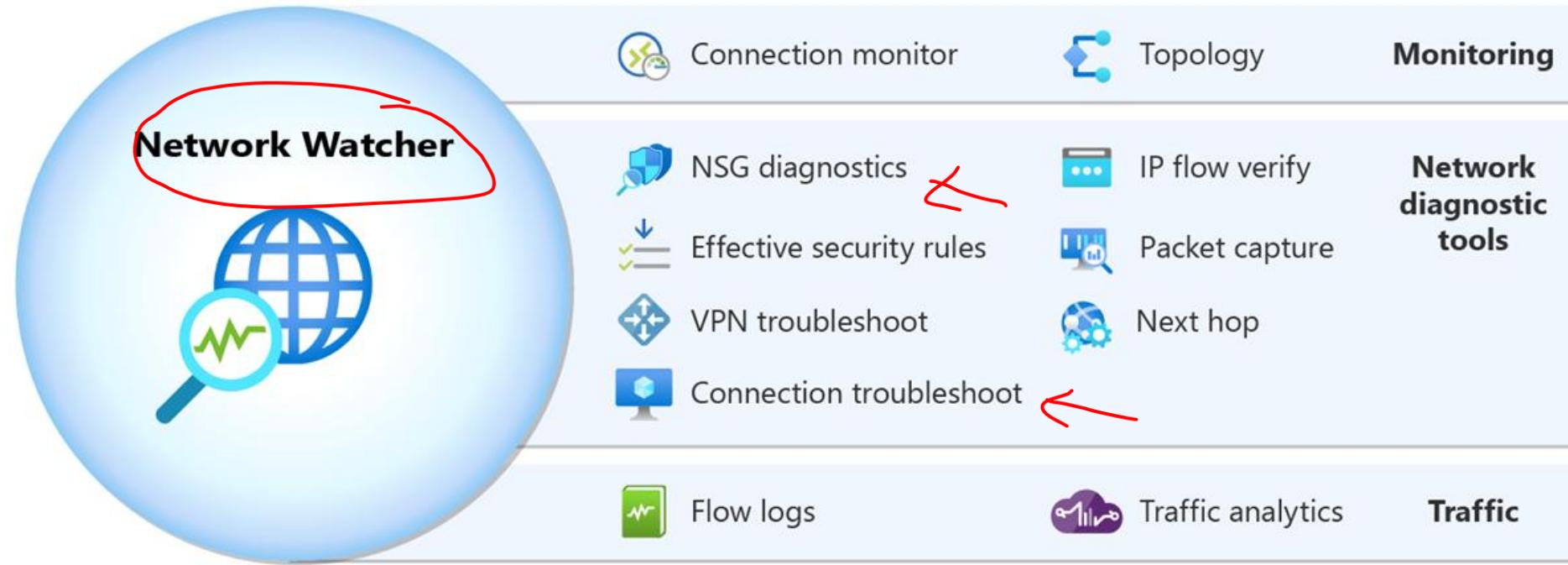


Terminate outside the firewall (the perimeter network paradigm)



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

Monitor network security by using Network Watcher



- Comprehensive Monitoring: Azure Network Watcher provides tools to monitor, diagnose, and log Azure IaaS resources.
- Network Diagnostics: Includes IP flow verification, routing checks, security rule analysis, and VPN troubleshooting.
- Traffic Analysis: Enables flow logs, traffic analytics, and visualizations for network traffic insights and management.

Plan and implement security for private access to Azure resources

Plan and implement virtual network Service Endpoints

= Routing

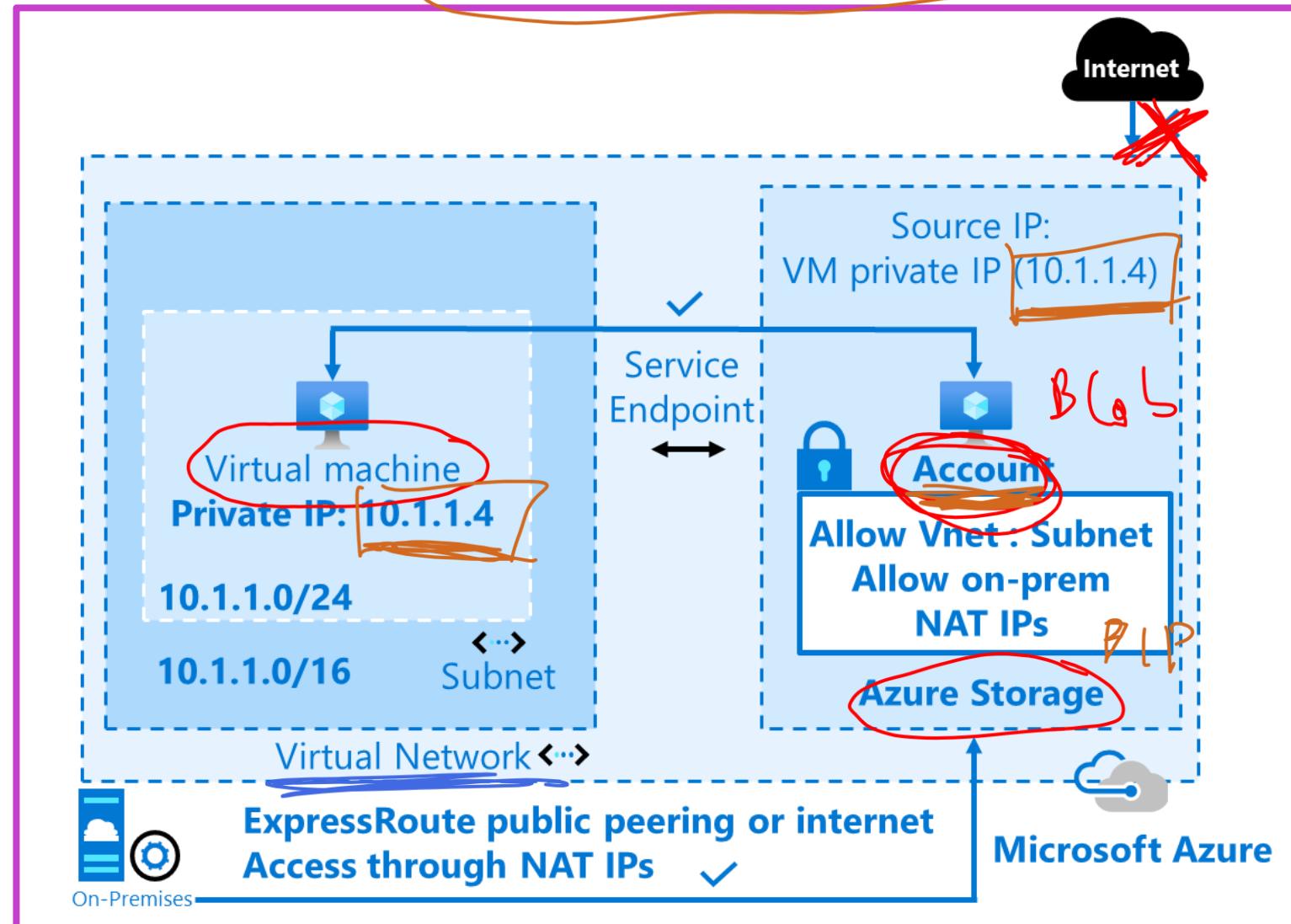
Endpoints limit network access to specific subnets and IP addresses

Improved security for your Azure service resources

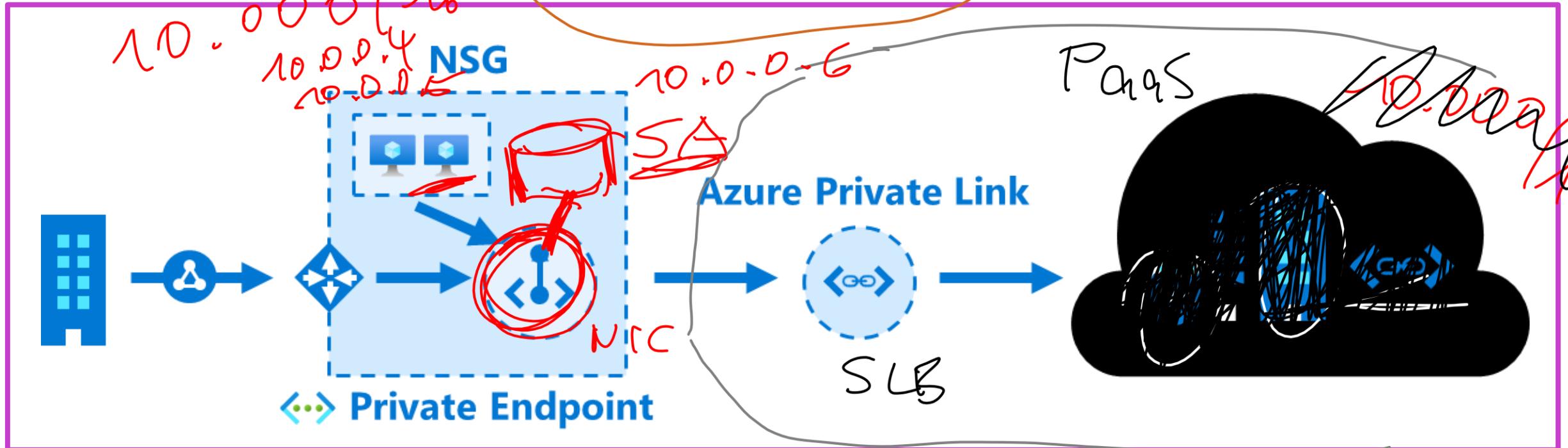
Optimal routing for Azure service traffic from your virtual network

Endpoints use the Microsoft Azure backbone network

Simple to set up with less management overhead



Plan and implement Private Endpoints



Private connectivity to services on Azure

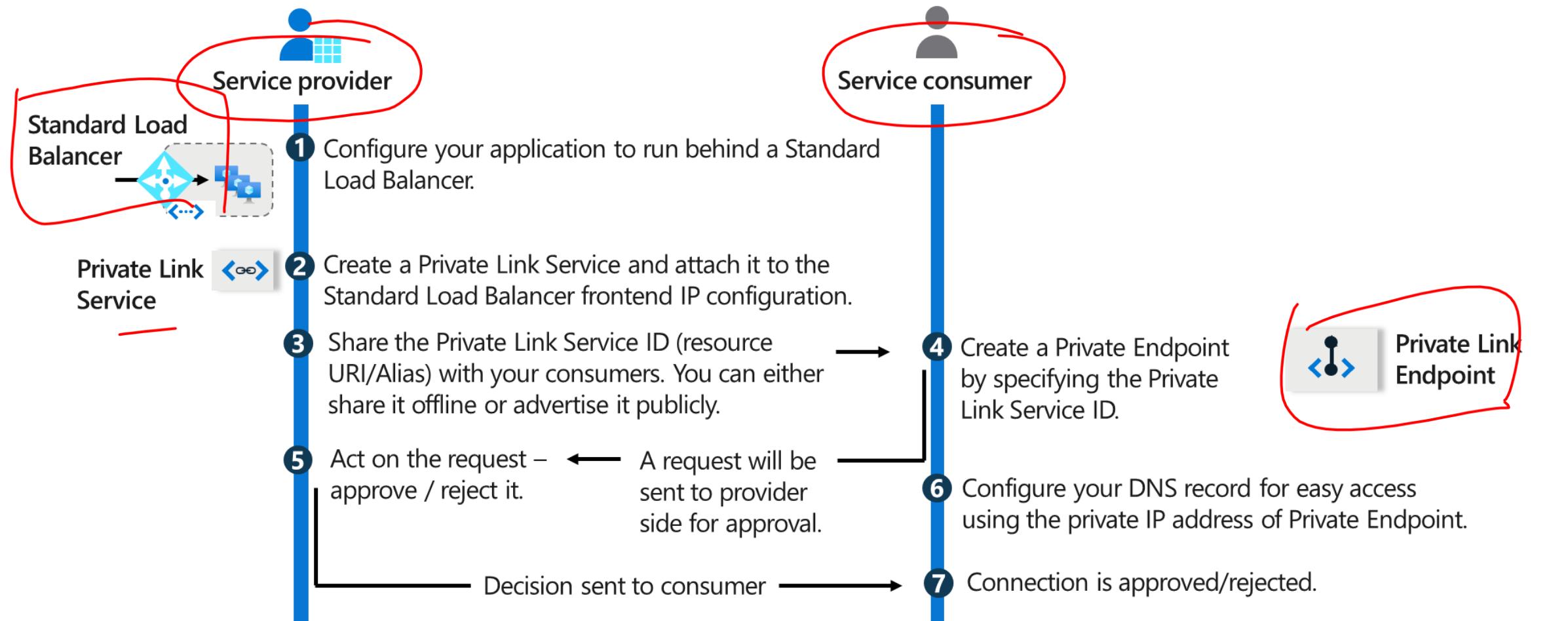
Integration with on-premises and peered networks

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

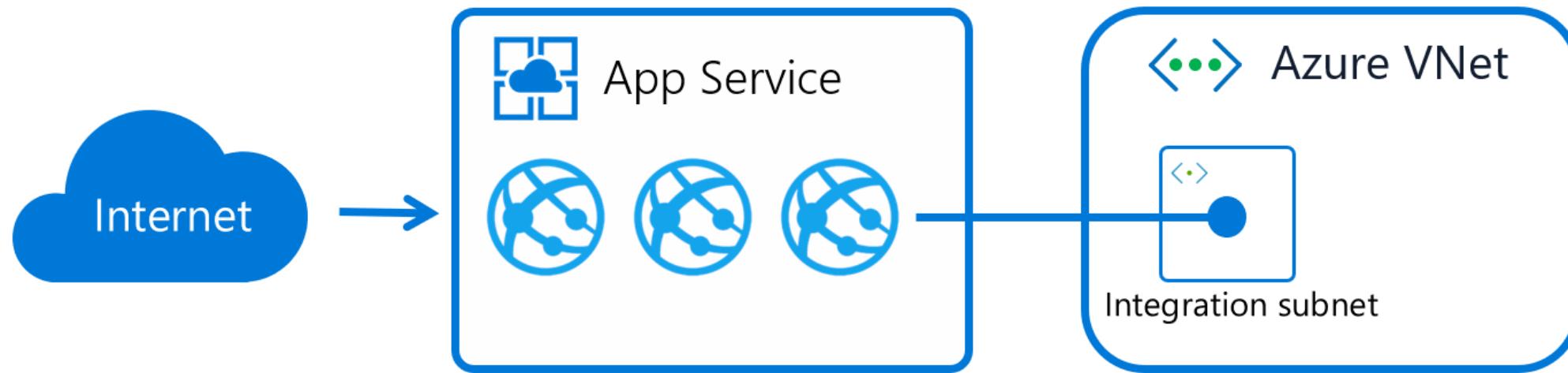
During a security incident within your network, only the mapped resource would be accessible

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



- Azure Virtual Network Integration: Enables outbound app traffic to access virtual network resources securely.
- Supports scalability: Works with multiple pricing tiers, regional connections, and peered virtual networks.
- Networking features: Leverages NSGs, route tables, NAT gateways, and private endpoints for routing and security.

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



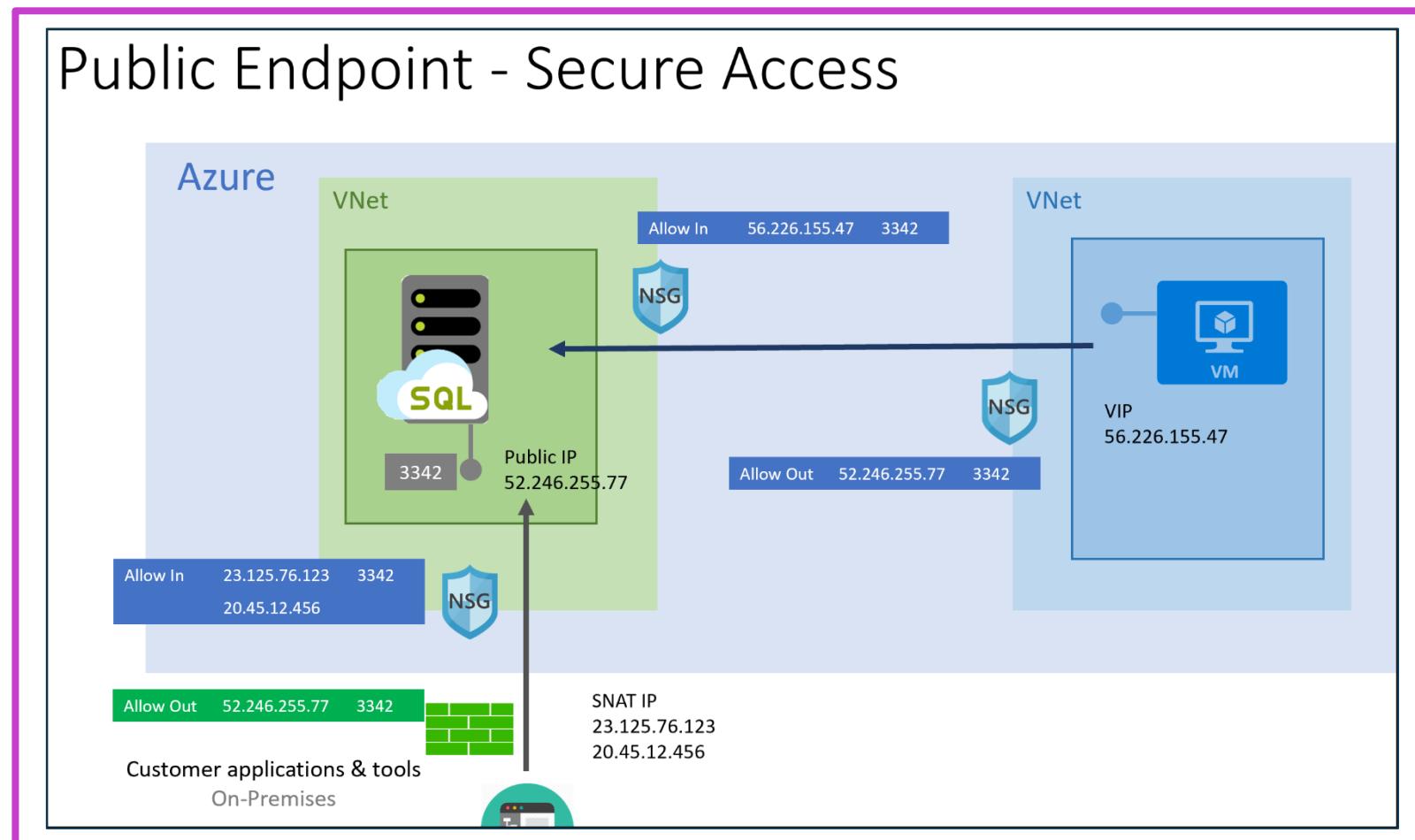
Integrate DDoS Protection



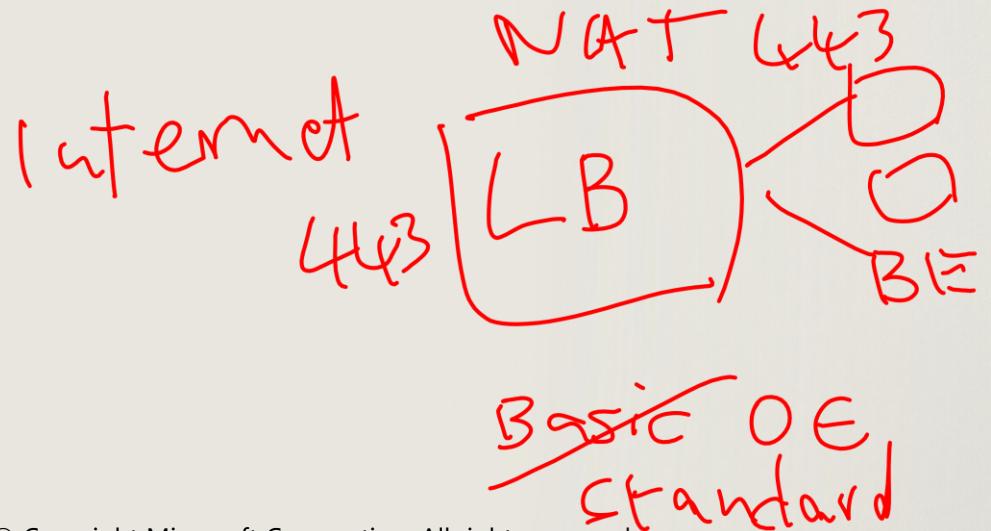
Implement and Fine-Tune the Web Application Firewall (WAF)

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

- Public Endpoint Scenarios: Enables Azure SQL Managed Instance connectivity for multi-tenant PaaS, high throughput, or policy constraints.
- Secure Connections: Encrypts data, uses Azure backbone, and recommends ExpressRoute for on-premises connections.
- Network Security: Leverage NSGs, trusted IPs, and private peering to restrict public endpoint access.



Plan and implement security for public access to Azure resources



Redirect
URL Rewrite



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



Message privacy and integrity



Algorithm flexibility



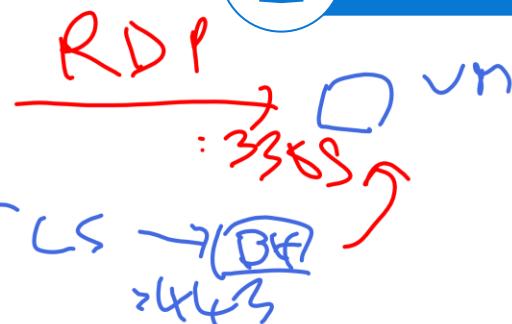
Ease of deployment and use



Interoperability between systems



Perfect Forward Secrecy (PFS)



RSA
2048
4096
bit

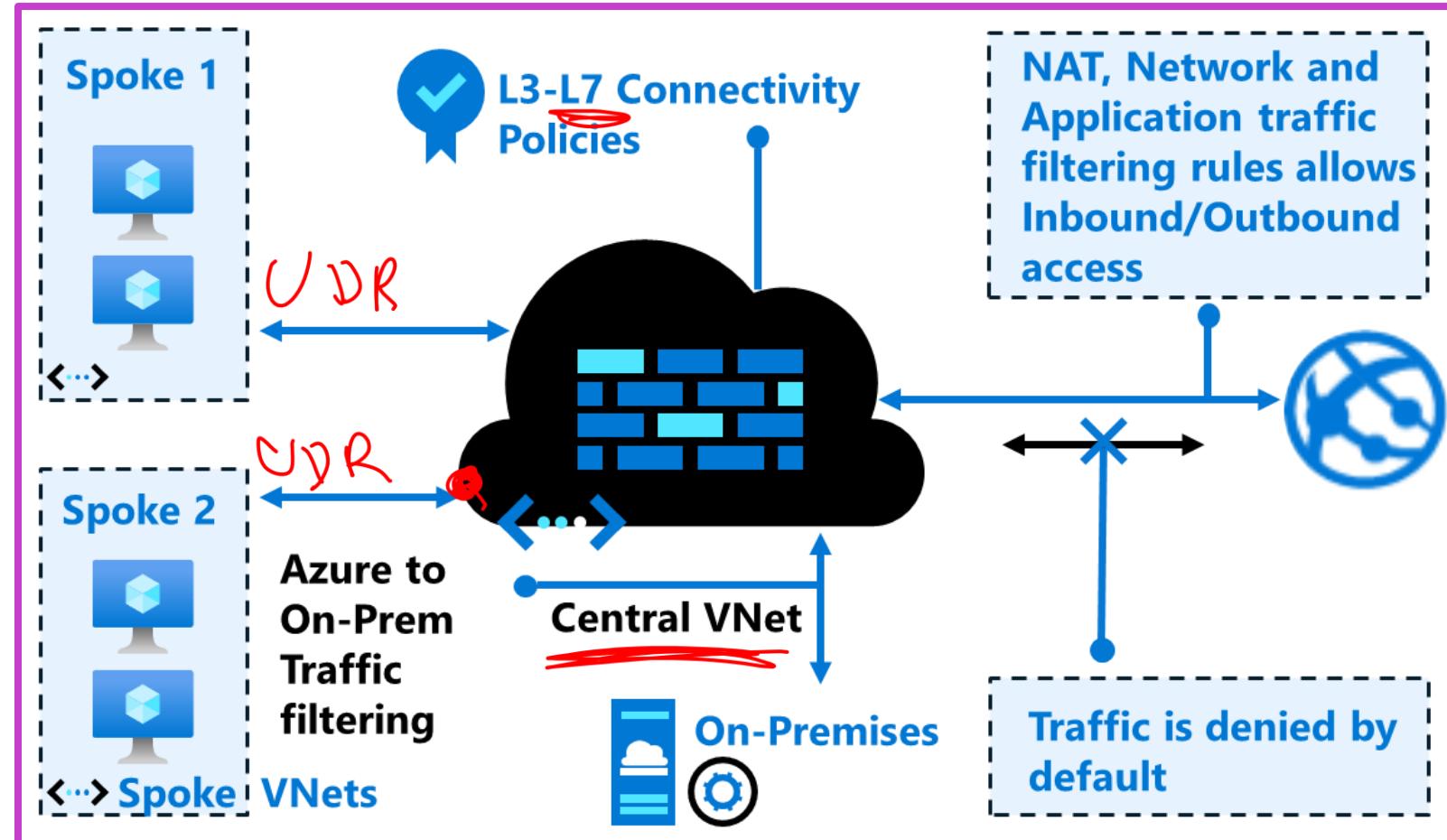
ARM API

QC

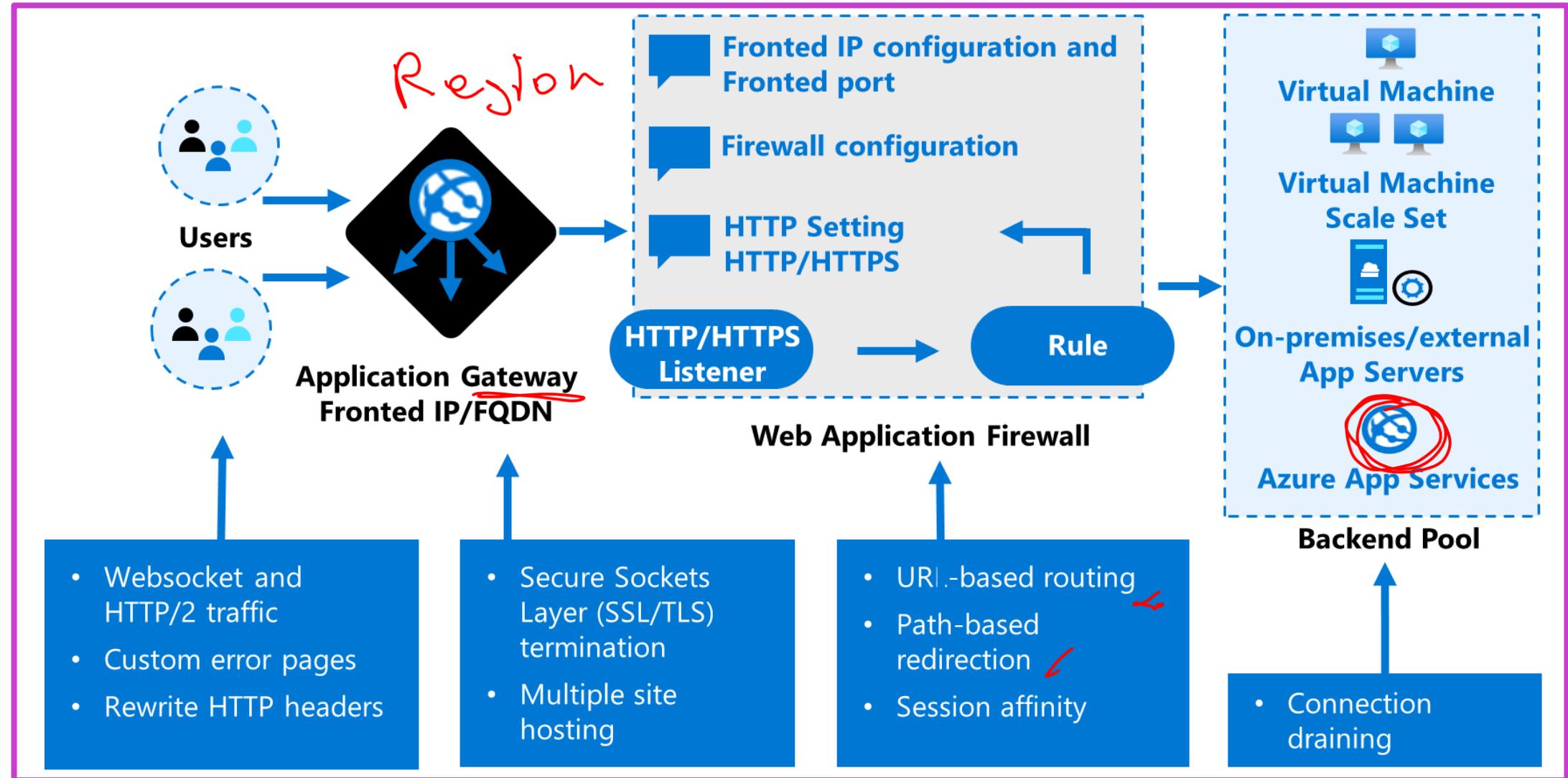
Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies

NAT

- 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).

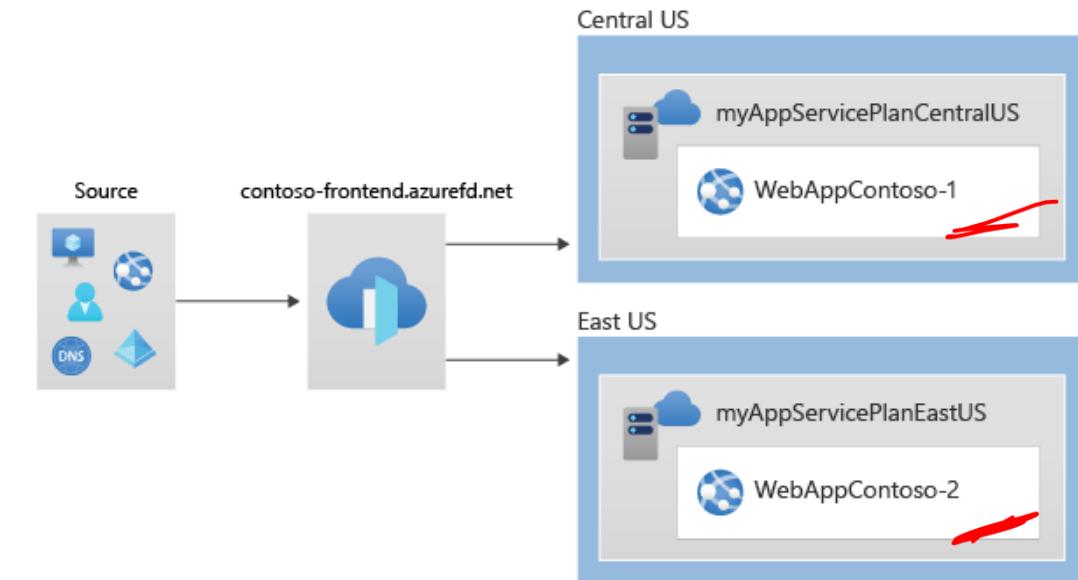


Plan and implement an Azure Application Gateway



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



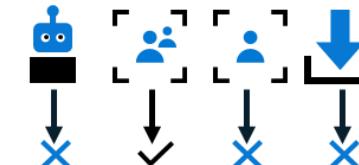
Plan and implement a Web Application Firewall (WAF)

Protects against cross-site scripting and SQL injection

OWASP Core Rule sets 3.1, 3.0, 2.29

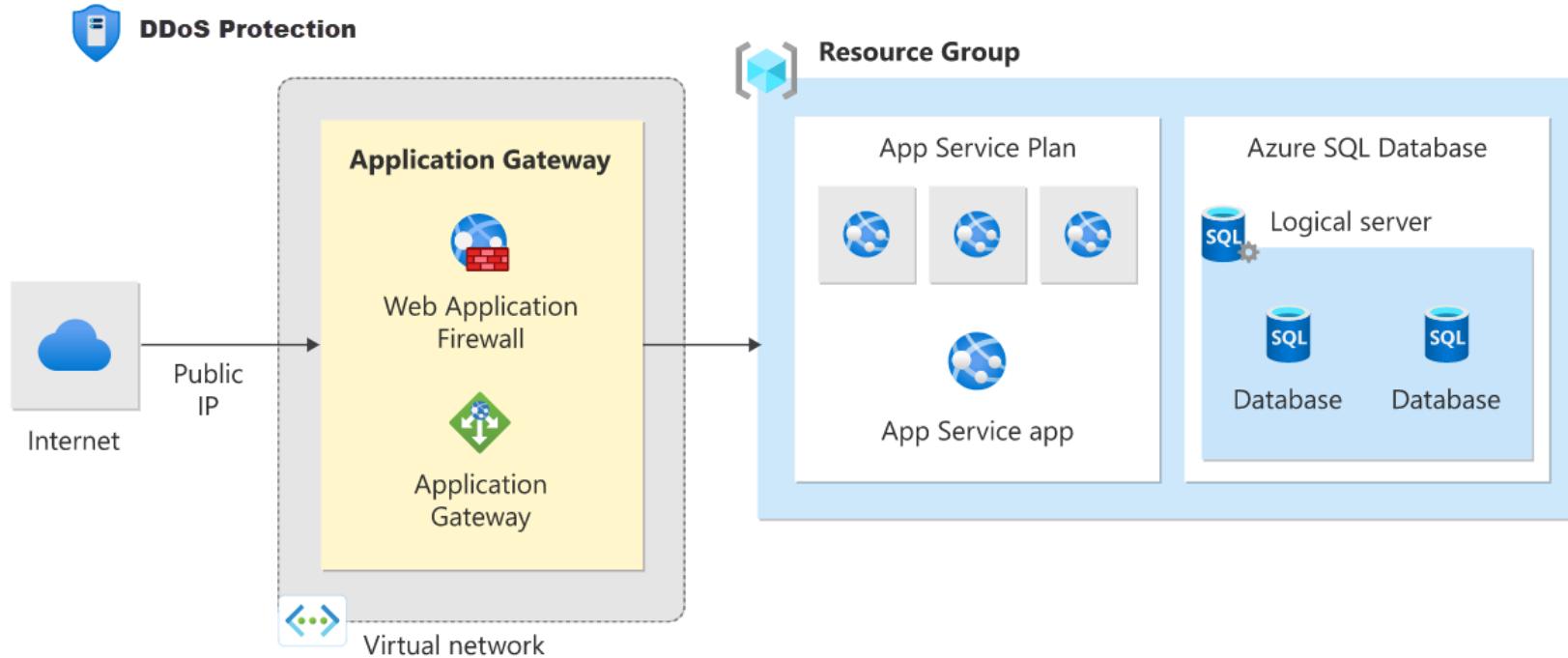
Custom access control

Supports Azure Front Door, Azure Application Gateway, and CDN (preview)



- Global WAF policy
- Custom Access Control
- Rate Limit
- OWASP TOP 10 Protection

Recommend when to use Azure DDoS Protection

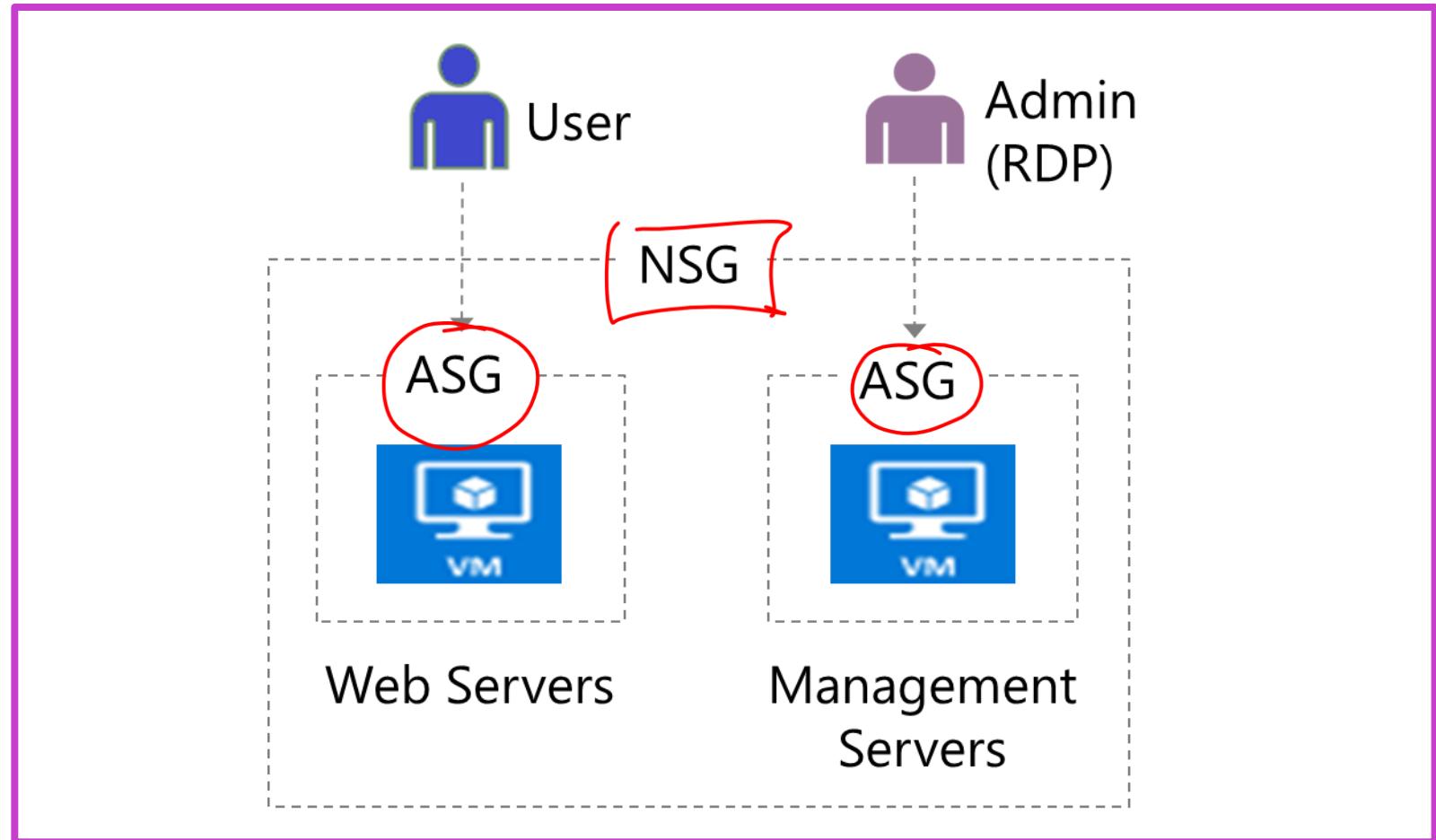


- Comprehensive Protection: Azure DDoS Protection defends against Layer 3-4 attacks with adaptive, always-on monitoring.
- Scalable Solutions: Offers Network and IP Protection tiers with analytics, alerts, and rapid response support.
- Multi-Layered Security: Integrates with WAF for complete network and application layer defense.

Module Labs

Lab 02 – Network Security 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

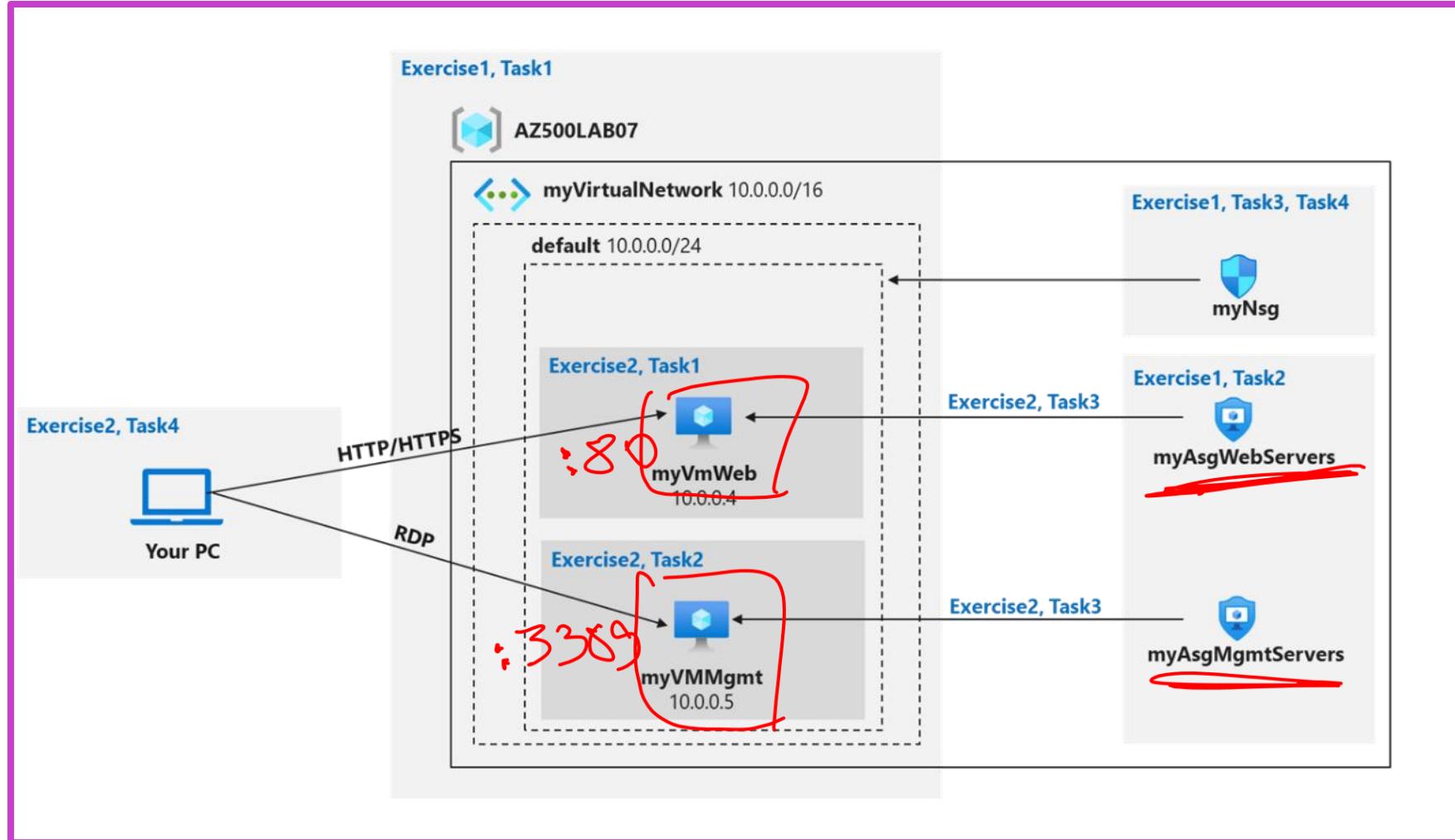


Lab 02 – Network Security Groups and Application Security Groups



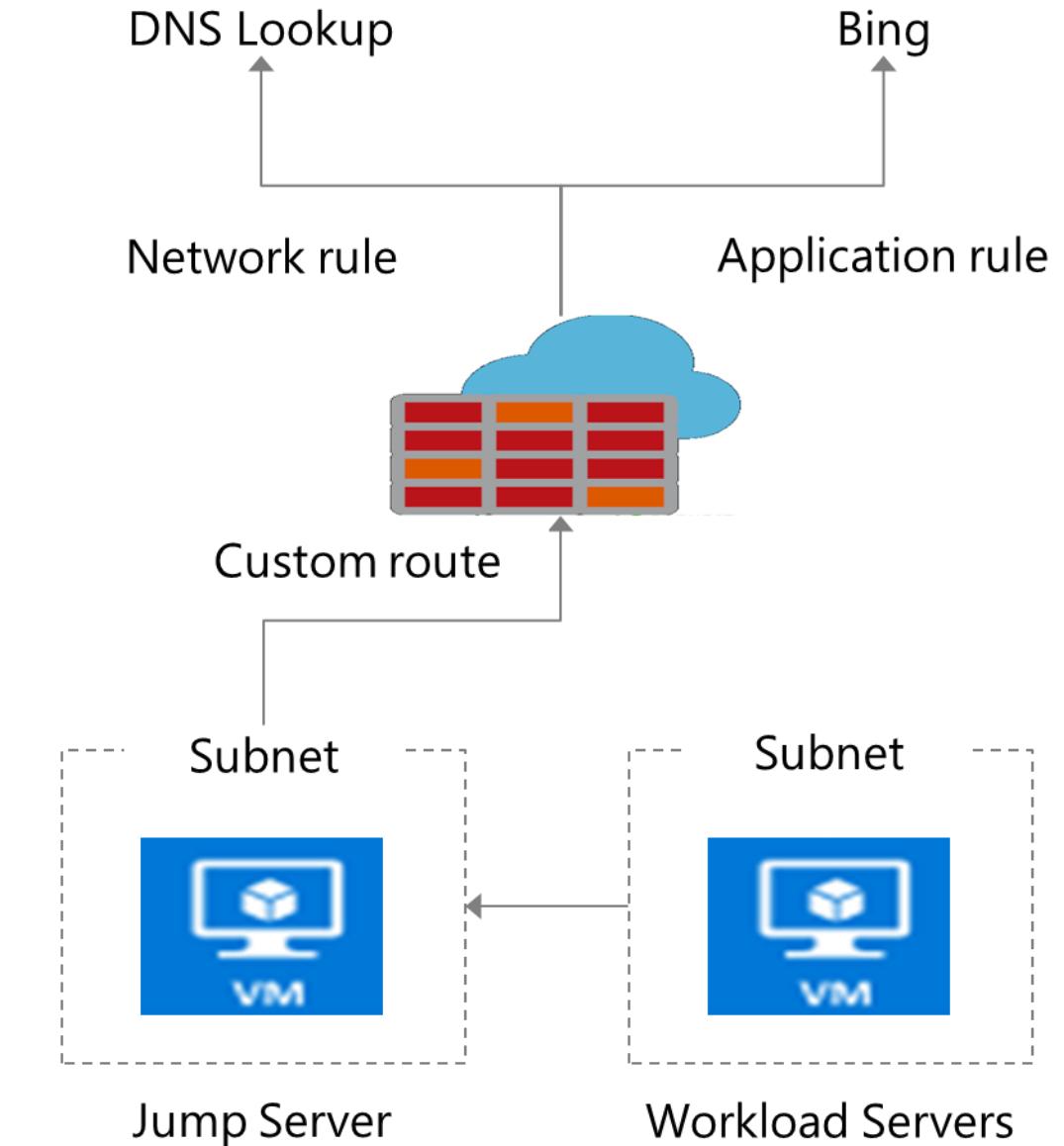
This exercise teaches students how to implement your organization's virtual networking infrastructure and test to ensure it is working correctly.

[Launch this Exercise in GitHub](#)



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

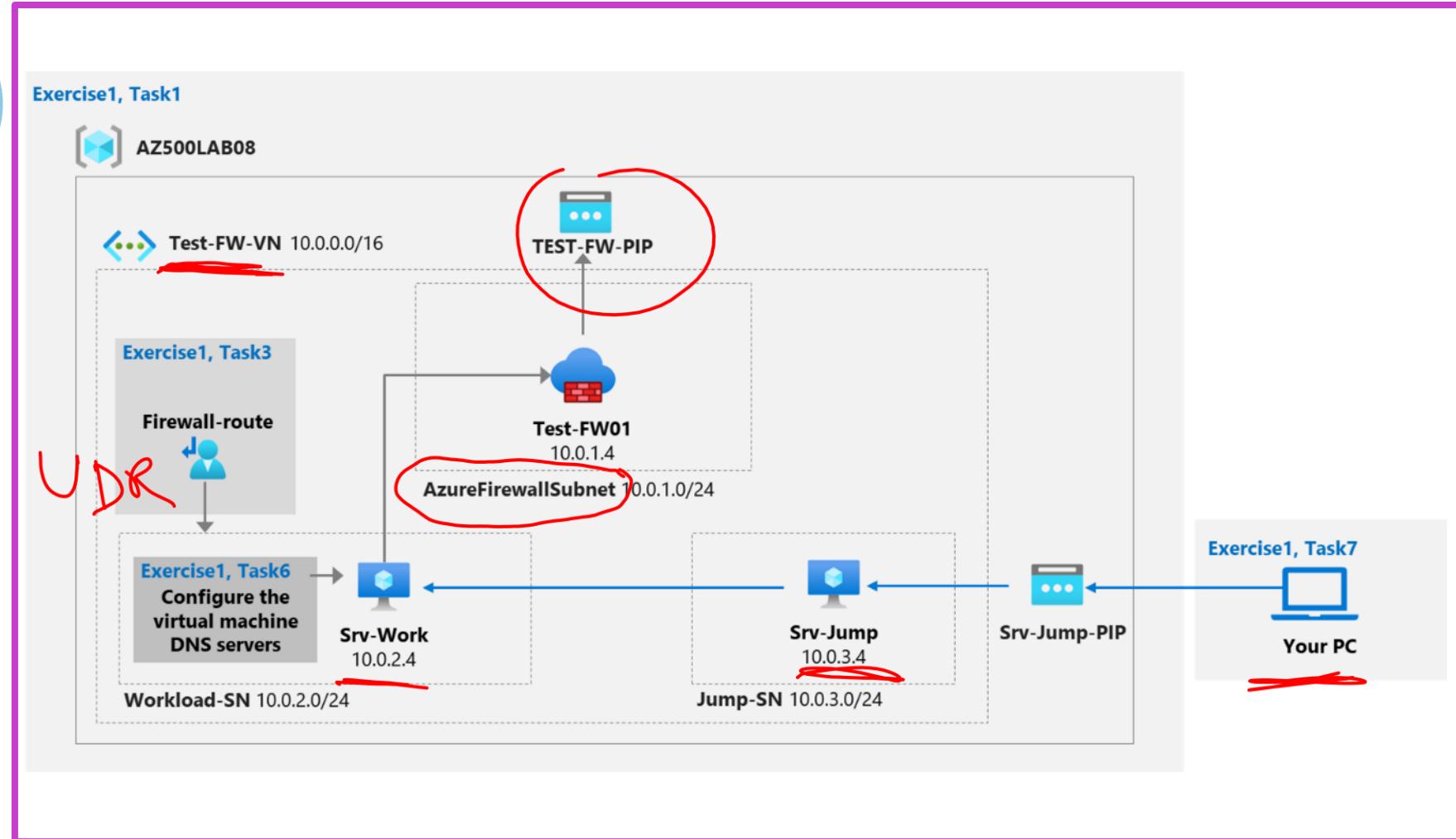


Lab 03 – Azure Firewall



This exercise teaches students how to install Azure Firewall to control inbound and outbound network access—an essential part of a network security plan—and to create and test the following infrastructure components.

[Launch this Exercise in GitHub](#)



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