Microsoft

Leeds Sharp
Microsoft Azure Networking for Developers

Jared Holgate

27th March 2025

Agenda

1. Introduction
2. Azure Networking Fundamentals
3. Azure Landing Zones and Azure Verified Modules
4. Azure Networking Resources Shallow Dive
5. Questions

About me

Jared Holgate

Senior Cloud Solution Architect

Global Customer Success Tech Strategy

Work

- Tech Lead for Terraform Azure Verified Modules
- Tech Lead for Terraform Azure Landing Zones
- Owner of IaC Accelerators for Azure Landing Zones

Community

- Yorkshire DevOps (yorkshiredevops.dev)
- Yorkshire Azure User Group (yorkshireazuregroup.cloud)

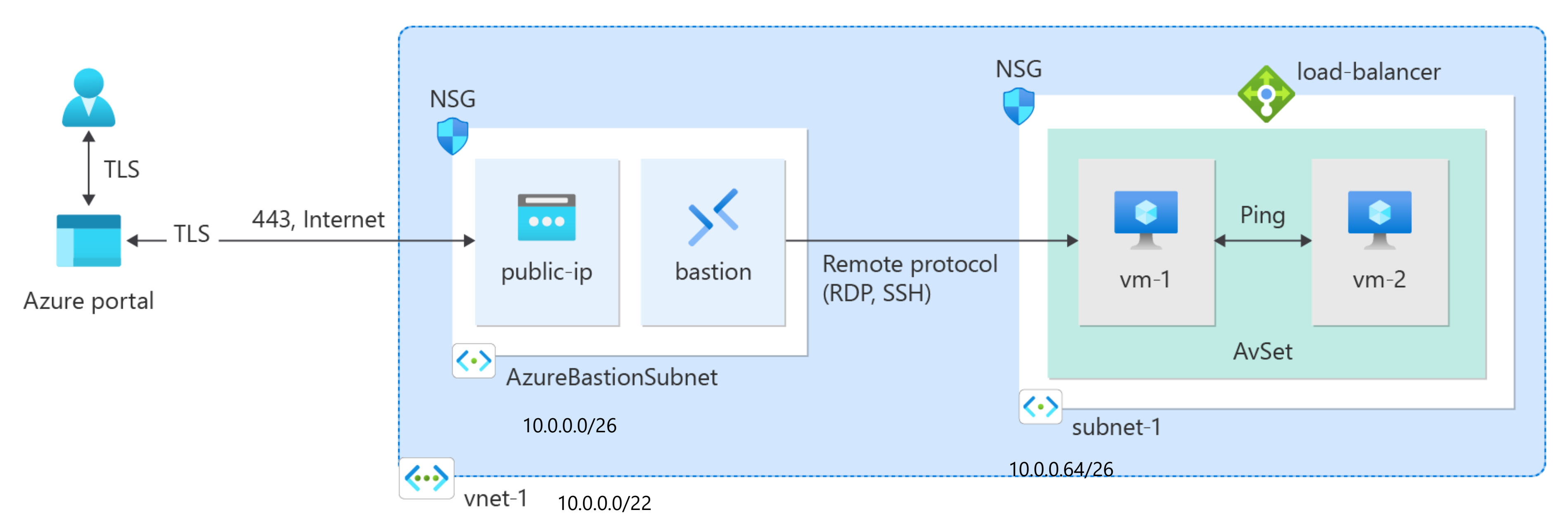
Also ask me about

- Infrastructure as Code (IaC)
- Terraform
- DevOps / Platform Engineering
- Anything…

Azure Networking Fundamentals

Fundamental building blocks

- Virtual Network (VNet)
- Subnet

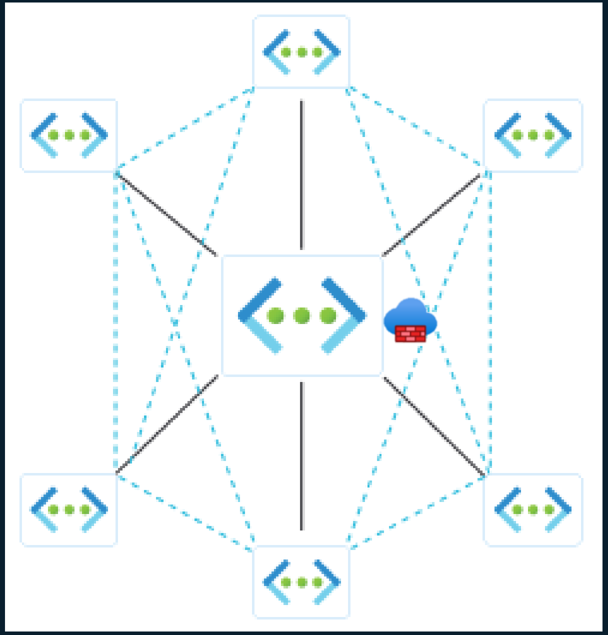


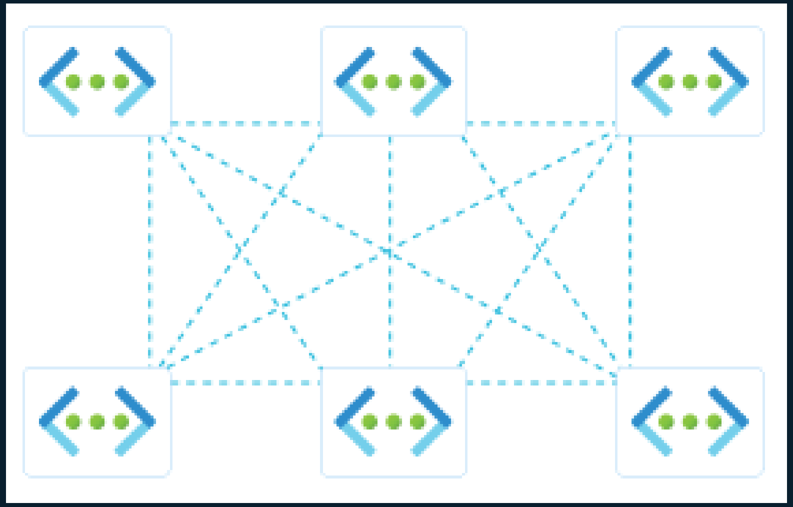
Both require an IP Prefix. VNet IP Prefixes can overlap, but you need to plan ahead!

Subnets can resolve and route by default

Network Topologies

- Design patterns for networking





Hub and Spoke

Mesh

Traditionally used with a central firewall

Zero trust with micro segmentation

How do I…

know if I need a network?

- ✅ IaaS
- ❔ PaaS (it depends)
- ✅ Private endpoints
- ✅ On premise connectivity to private resources

access the internet?

- ✅ Azure NAT Gateway on a subnet
- ✅ Central Azure Firewall / NVA
- ❔ Public Load Balancer
- ❔ Public IP on a VM NIC
- ❌ Default outbound access (goes away 30th September 2025)

- Consider: SNAT Port Exhaustion (Source Network Address Translation)

route traffic?

- ✅ Subnets in a VNet (via AzureSDN)
- ✅ User defined route tables
- ✅ VNet peering
- ✅ VNet gateways

- Consider

How do I...

resolve IP addresses to names?

- ✅ Azure DNS (via AzureSDN)
- ✅ Azure Firewall DNS Proxy / NVA
- ✅ Azure Private DNS Resolver

access a virtual machine?

- ✅ Azure Bastion Host
- ✅ Private Networking from On Premise
- ❌ Public IP on the VM NIC

Consider: Why do you need to access a VM? Immutable infrastructure, PaaS, Containers, etc are better solutions

access a service from the internet?

- ✅ Azure Firewall Public IP with DNAT (Destination Network Address Translation) or NVA
- ❔ Azure Public Load Balancer
- ✅ Azure Application Gateway
- ✅ Azure Front Door
- ✅ Azure Traffic Manager (when combined with another service)
- ✅ Azure API Management
- ❌ PaaS Public IP
- ❌ VM NIC Public IP

- Consider: TLS and Web Application Firewall somewhere in the stack

How do I…

filter traffic?

- ✅ Azure Network Security Group
- ✅ Azure Firewall / NVA

connect multiple networks?

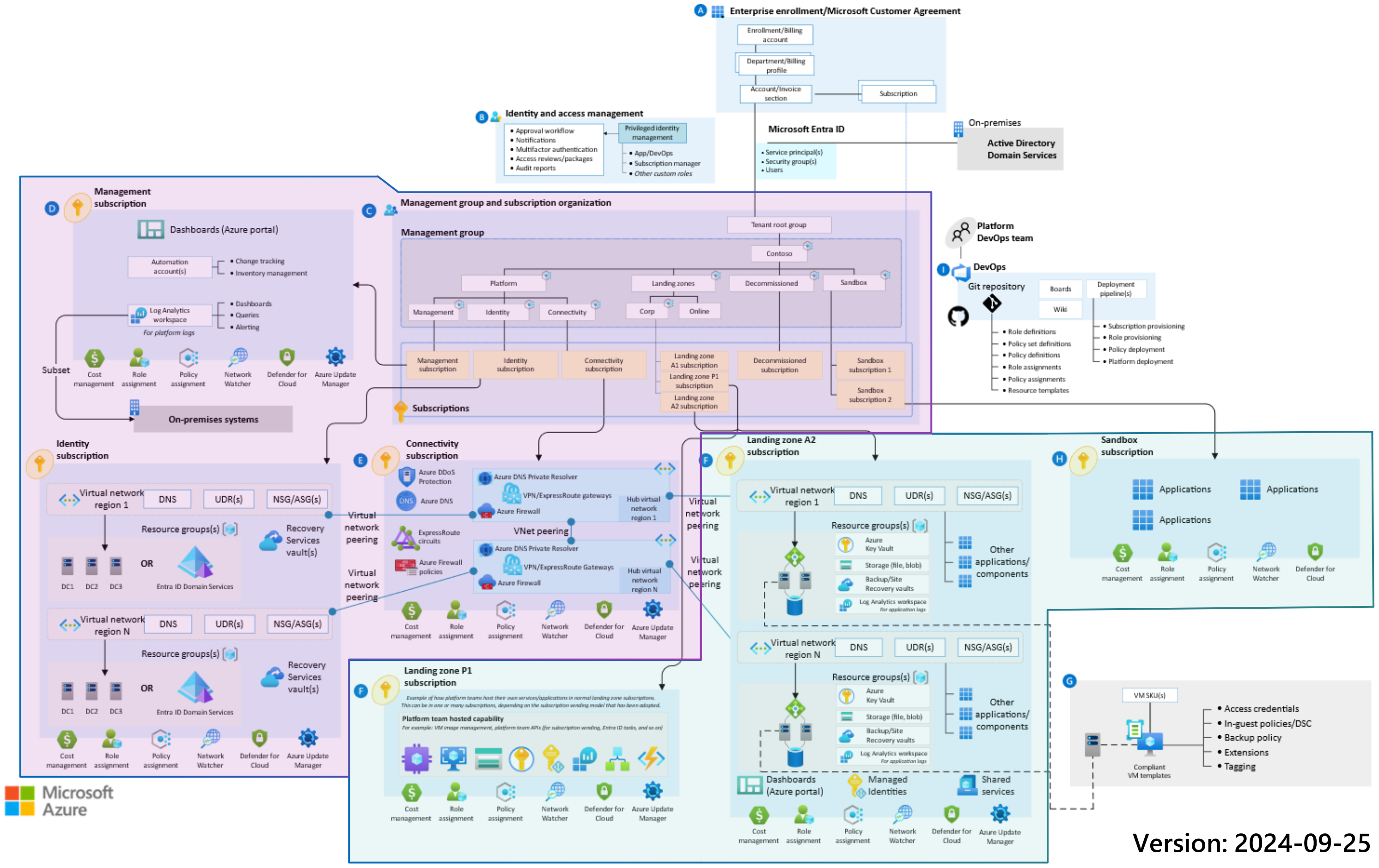
- ✅ VNet Peering
- ✅ VNet Gateways (ExpressRoute or VPN)

load balance?

- ✅ Azure Private Load Balancer
- ❔ Azure Public Load Balancer (for specific use cases like an NVA)
- ✅ Azure Application Gateway
- ✅ Azure Front Door
- ✅ Azure Traffic Manager
- ✅ Azure API Management

Azure Landing Zones and Azure Verified Modules

Platform Landing Zone vs Application Landing Zone



Version: 2024-09-25

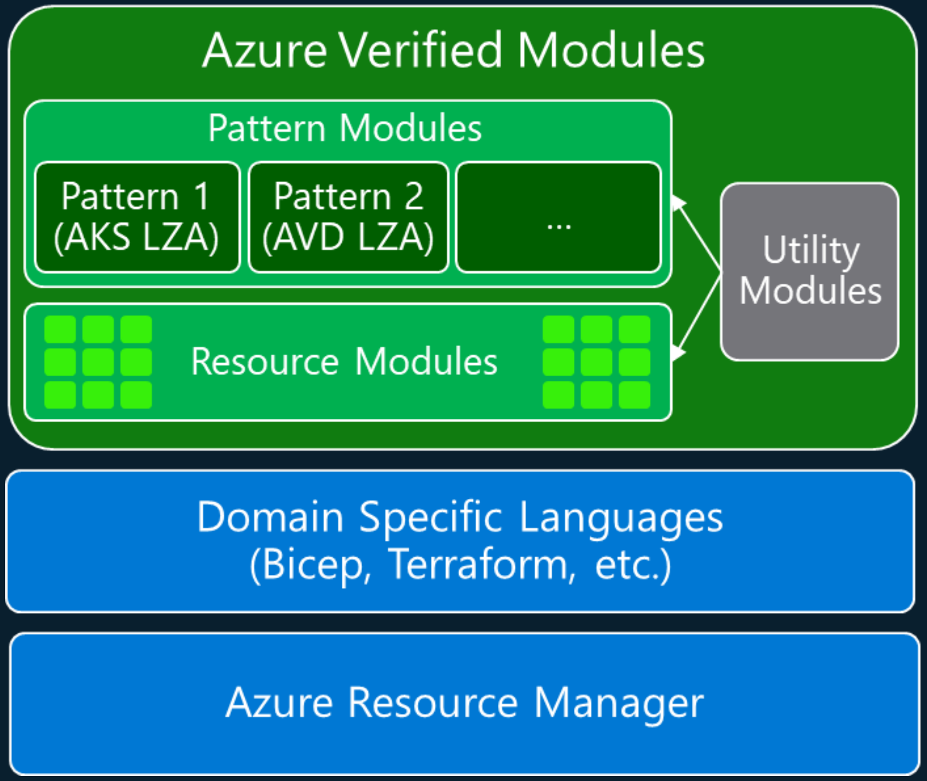
■ Platform Landing Zone

■ Application Landing Zones

aka.ms/alz

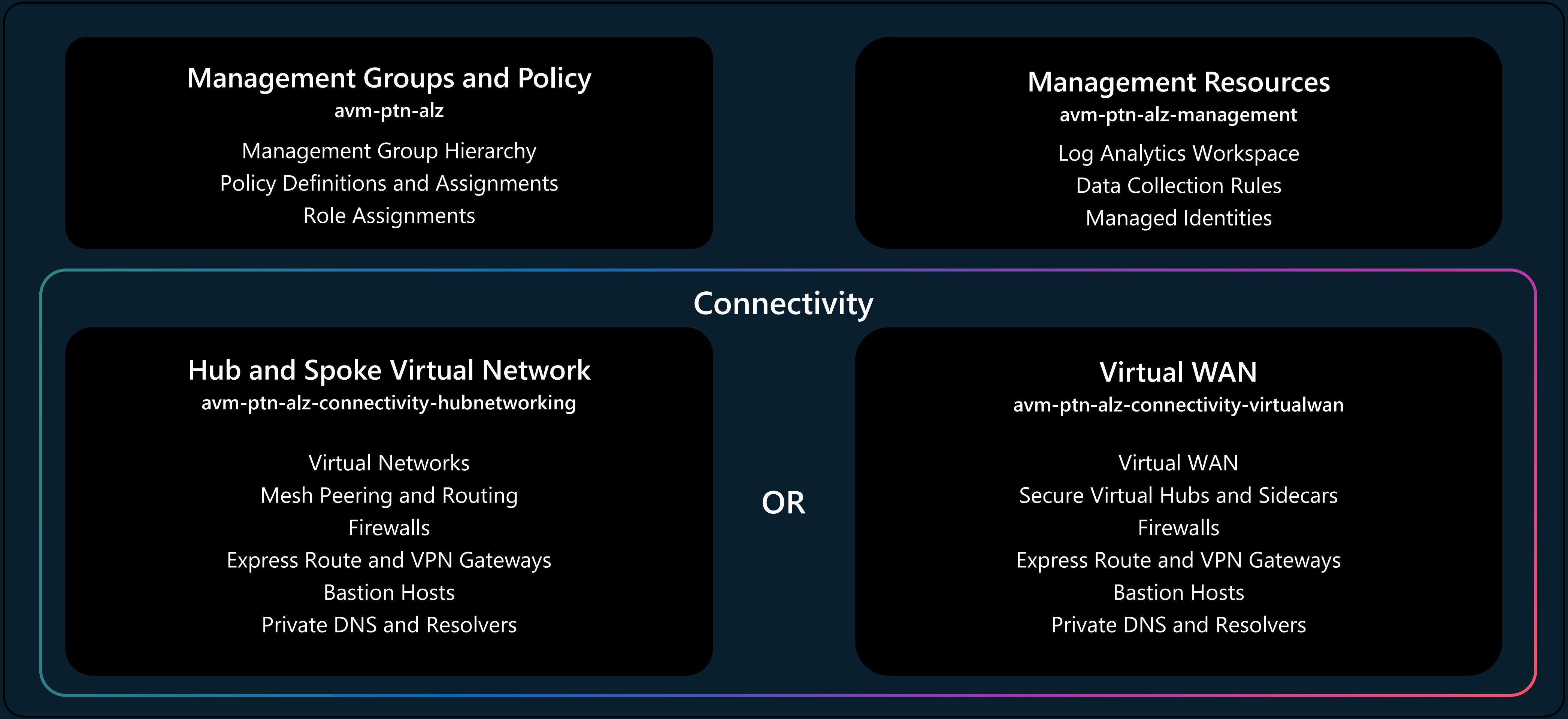
Azure Verified Modules

- Microsoft curated and supported Infrastructure as Code Modules for Bicep and Terraform
- Focus on quality and aligned to Well Architected Framework



aka.ms/avm

Azure Verified Modules for Platform Landing Zone (ALZ)



Management Groups and Policy

avm-ptn-alz

Management Group Hierarchy
Policy Definitions and Assignments
Role Assignments

Management Resources

avm-ptn-alz-management

Log Analytics Workspace
Data Collection Rules
Managed Identities

Connectivity

Hub and Spoke Virtual Network

avm-ptn-alz-connectivity-hubnetworking

Virtual Networks
Mesh Peering and Routing
Firewalls
Express Route and VPN Gateways
Bastion Hosts
Private DNS and Resolvers

OR

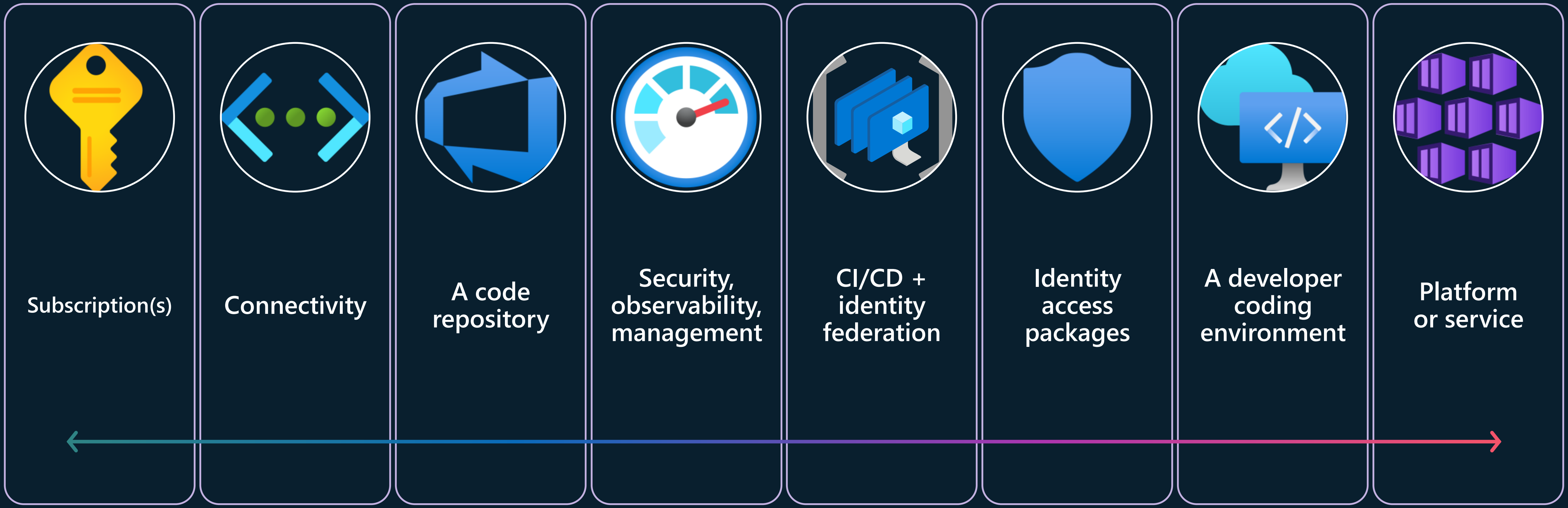
Virtual WAN

avm-ptn-alz-connectivity-virtualwan

Virtual WAN
Secure Virtual Hubs and Sidecars
Firewalls
Express Route and VPN Gateways
Bastion Hosts
Private DNS and Resolvers

Coming Soon: Application Landing Zones

- Extending our ALZ IaC Accelerator to bootstrap Application landing zones
- Networking
- Version control / CI CD
- Etc…



Subscription(s)

Connectivity

A code repository

Security, observability, management

CI/CD + identity federation

Identity access packages

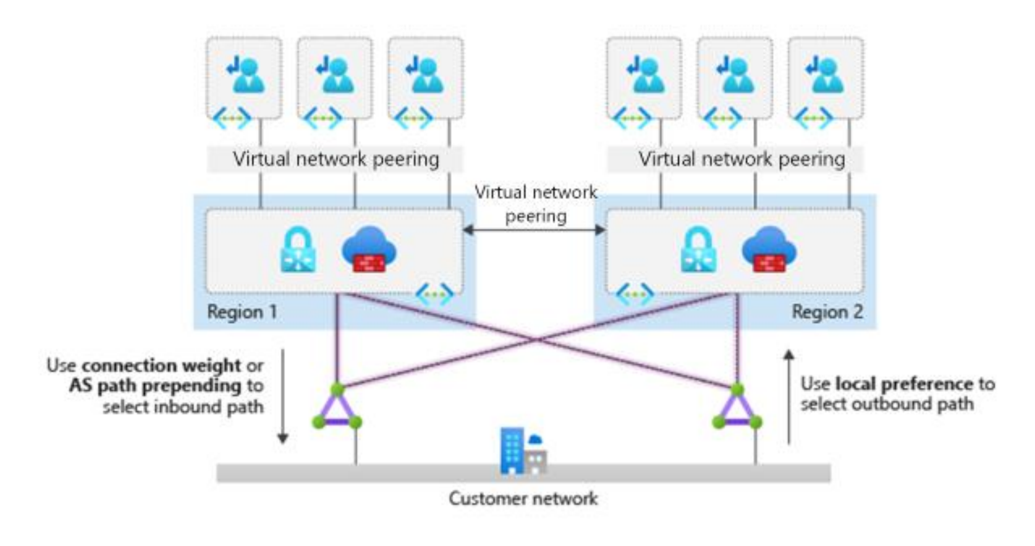
A developer coding environment

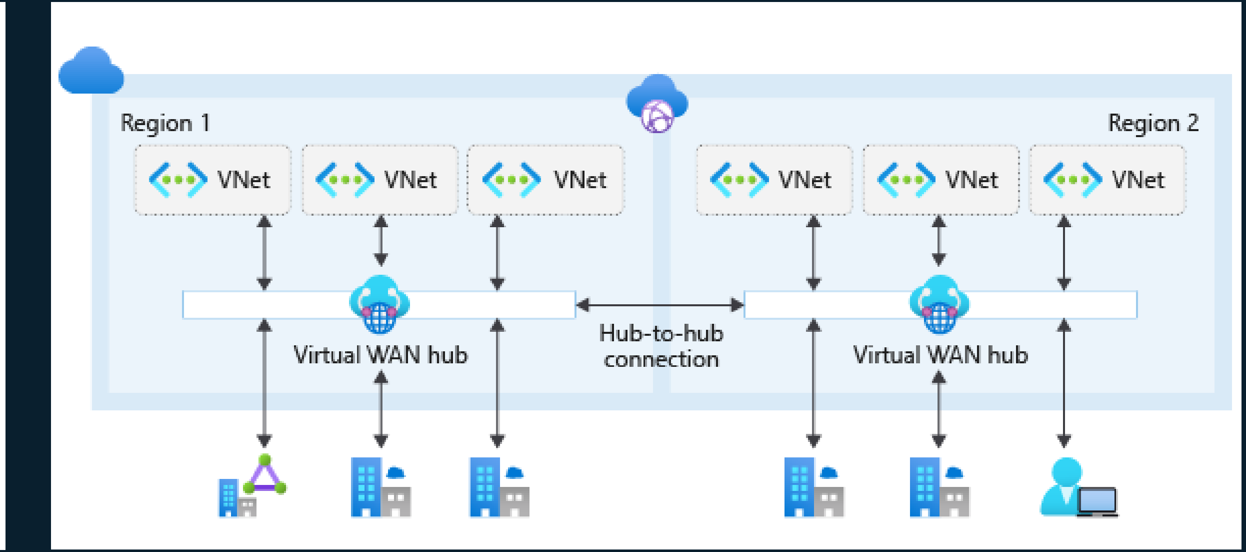
Platform or service

Azure Networking Resources

Peered Azure Virtual Networks or Azure Virtual WAN

Both implement the same hub and spoke design pattern


Virtual network peering
Virtual network peering
Virtual network peering
Region 1
Region 2
Use connection weight or AS path prepending to select inbound path
Use local preference to select outbound path
Customer network



Peered Azure Virtual Networks

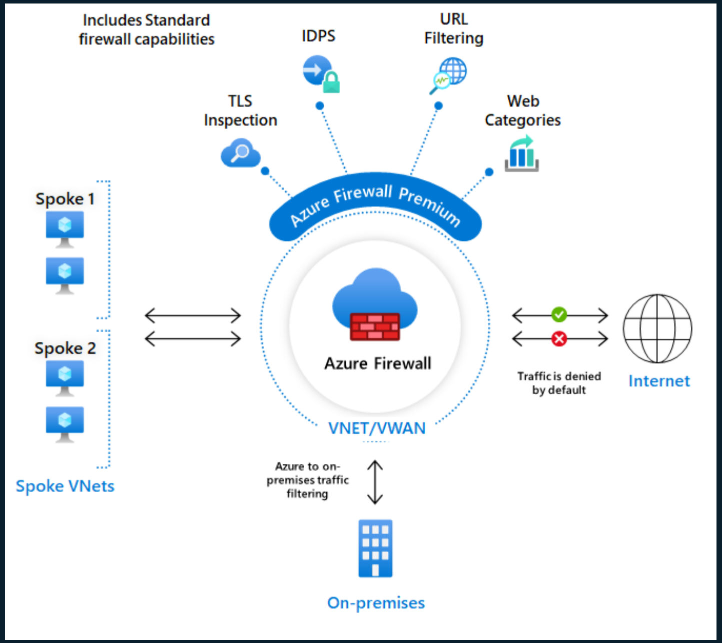
Offers more flexibility at the cost of complexity

Virtual WAN (managed service)

Offers 'simpler' management at the cost of limited capabilities

Azure Firewall or Third Party Network Virtual Appliance (NVA)

Both serve the same use cases of inbound and outbound internet connectivity, spoke to spoke restrictions, traffic inspection, etc



Azure Firewall

Azure native, simple to manage, feature rich

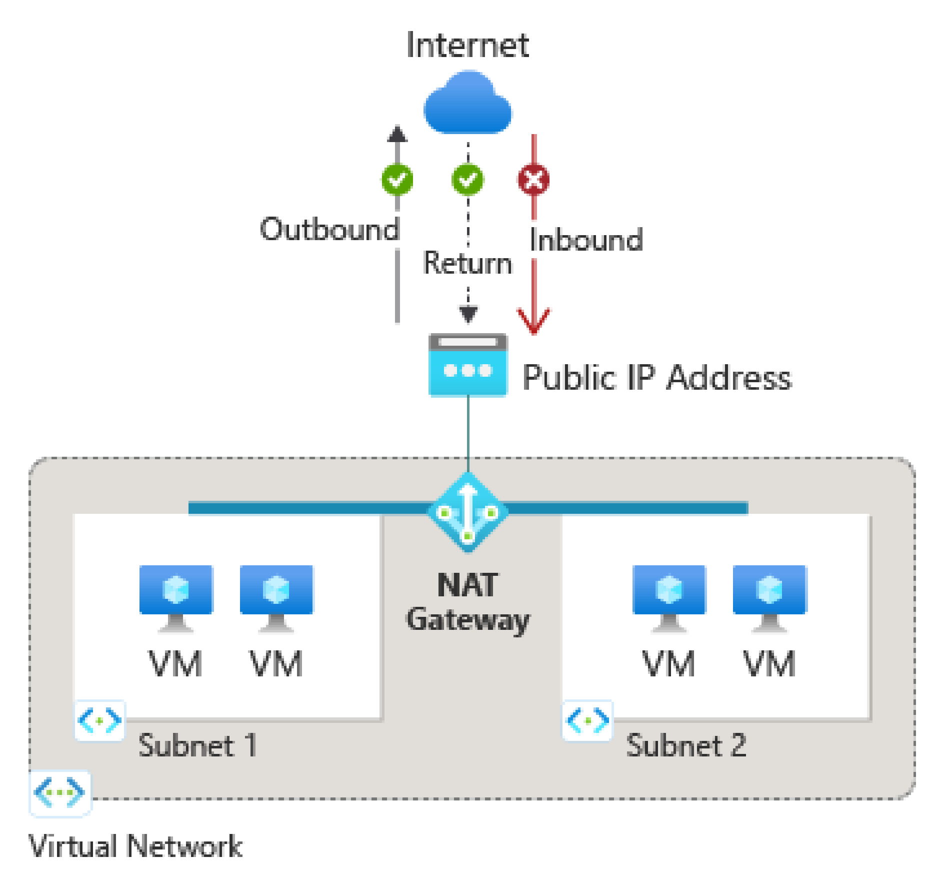
paloalto NETWORKS
CHECK POINT
Barracuda
Your business, secured.
FORTINET
CISCO
f5
Progress Kemp LoadMaster

Third-Party Network Virtual Appliance

Requires install and configuration on IaaS, plus networking, load balancers, etc. Can utilise an existing investment

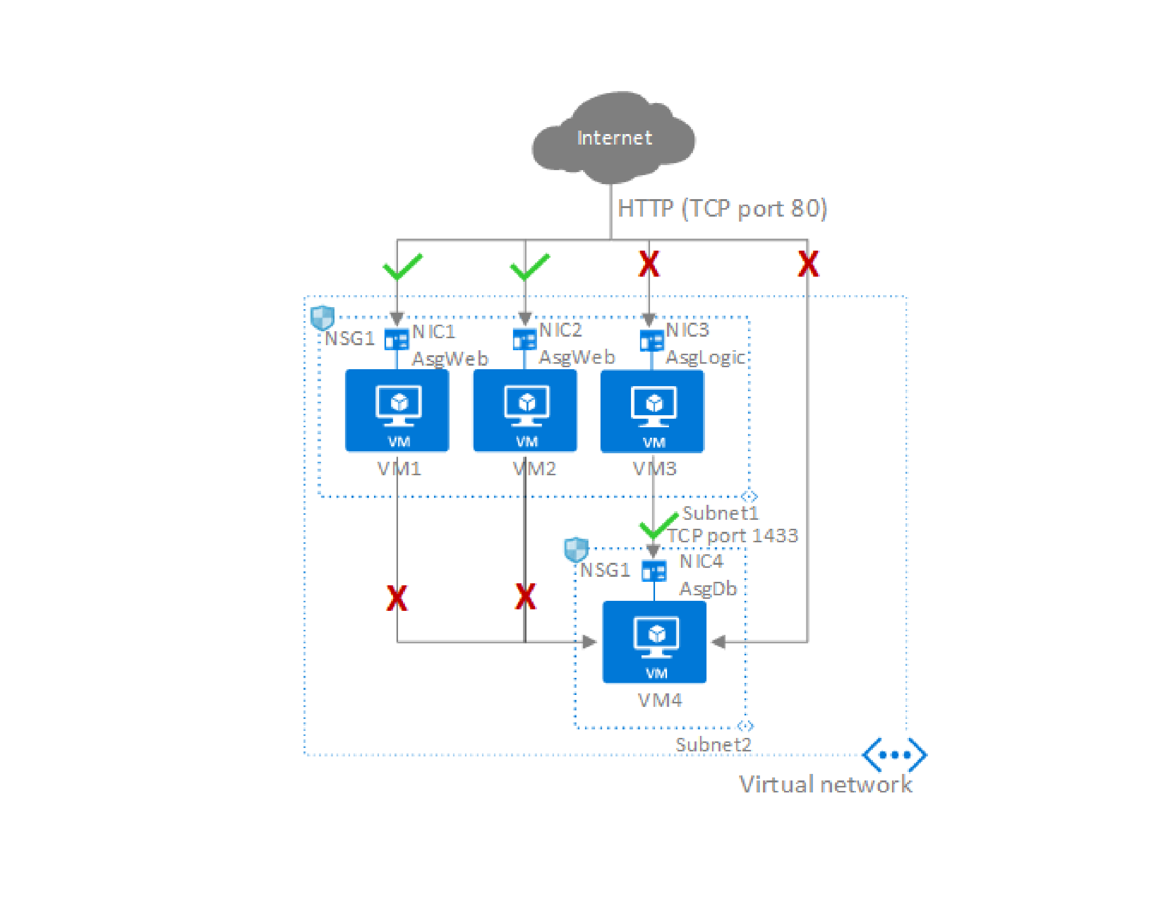
Outbound internet access with Azure NAT (Network Address Translation) Gateway

- Assigned to subnets
- Dynamically assigns ports to limit SNAT (Source Network Address Translation) port exhaustion



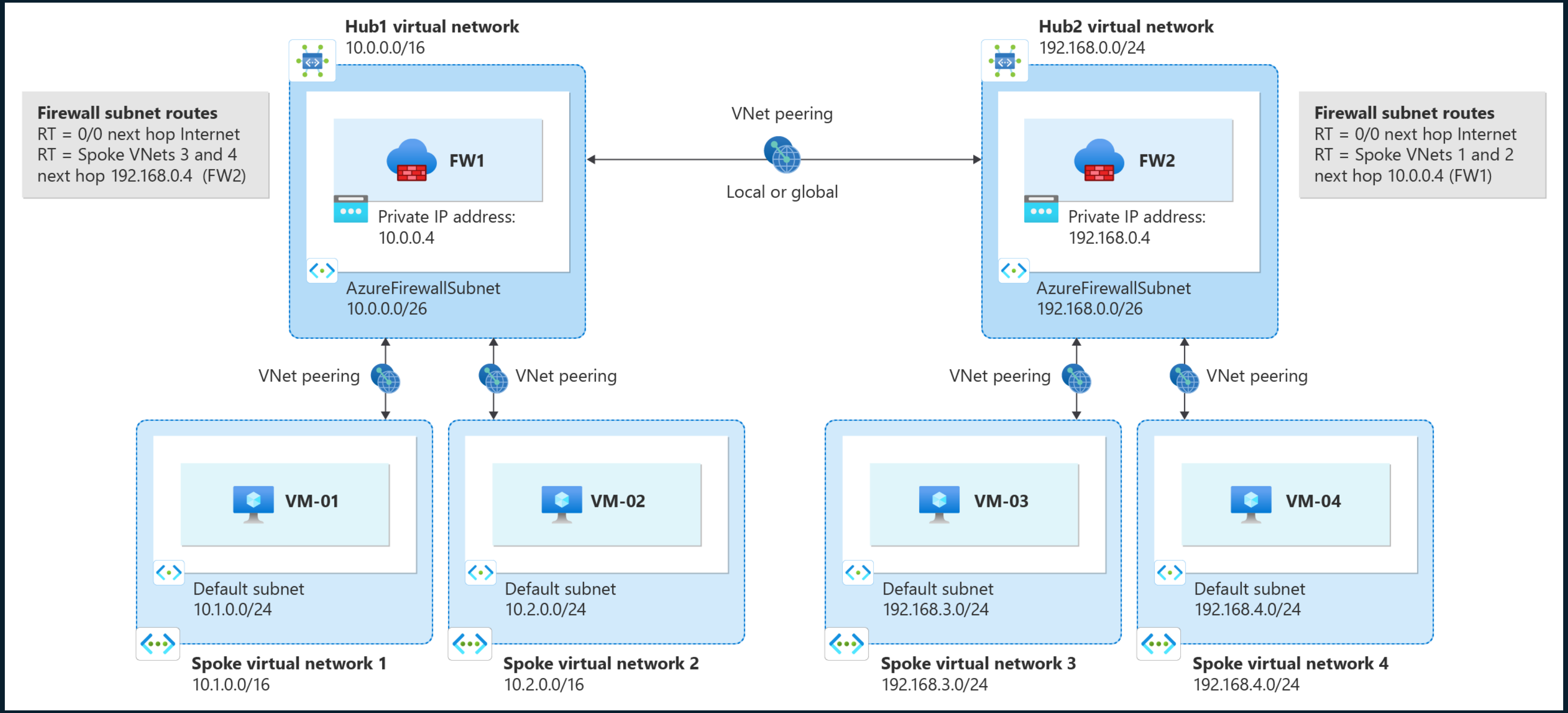
Micro-segmentation with Azure Network Security Groups

- Part of a Zero Trust network design. Peer everything and control everything
- Enables subnet to subnet segmentation



Spoke to Hub and Spoke to Spoke Connectivity with VNet Peering and User Defined Routes

- A VNet Peering is a set of 2 peering's, one in each direction
- Peering allows routing between subnets in the peered Vnets
- Peering does not allow routing to VNets not peered directly
- We must use User Defined Route with Azure Firewall or NVA to traverse the hubs



Firewall subnet routes
RT = 0/0 next hop Internet
RT = Spoke VNets 3 and 4
next hop 192.168.0.4 (FW2)

Hub1 virtual network
10.0.0.0/16

FW1
Private IP address:
10.0.0.4

AzureFirewallSubnet
10.0.0.0/26

VNet peering
Local or global

Hub2 virtual network
192.168.0.0/24

FW2
Private IP address:
192.168.0.4

AzureFirewallSubnet
192.168.0.0/26

Firewall subnet routes
RT = 0/0 next hop Internet
RT = Spoke VNets 1 and 2
next hop 10.0.0.4 (FW1)

VNet peering

VNet peering

VNet peering

VNet peering

VM-01
Default subnet
10.1.0.0/24
Spoke virtual network 1
10.1.0.0/16

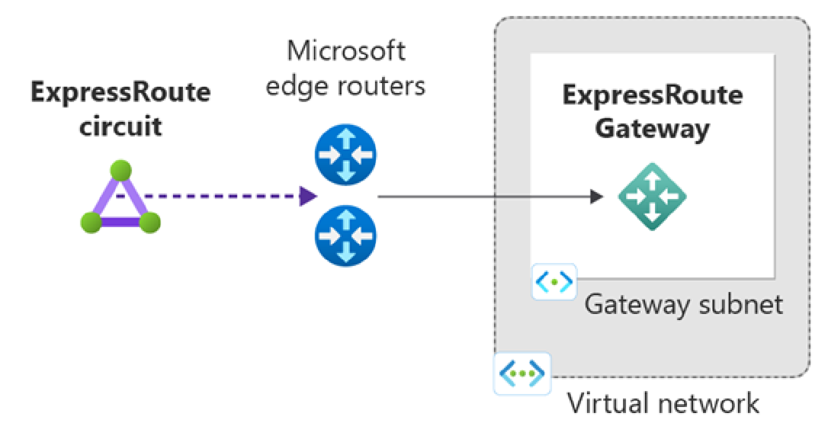
VM-02
Default subnet
10.2.0.0/24
Spoke virtual network 2
10.2.0.0/16

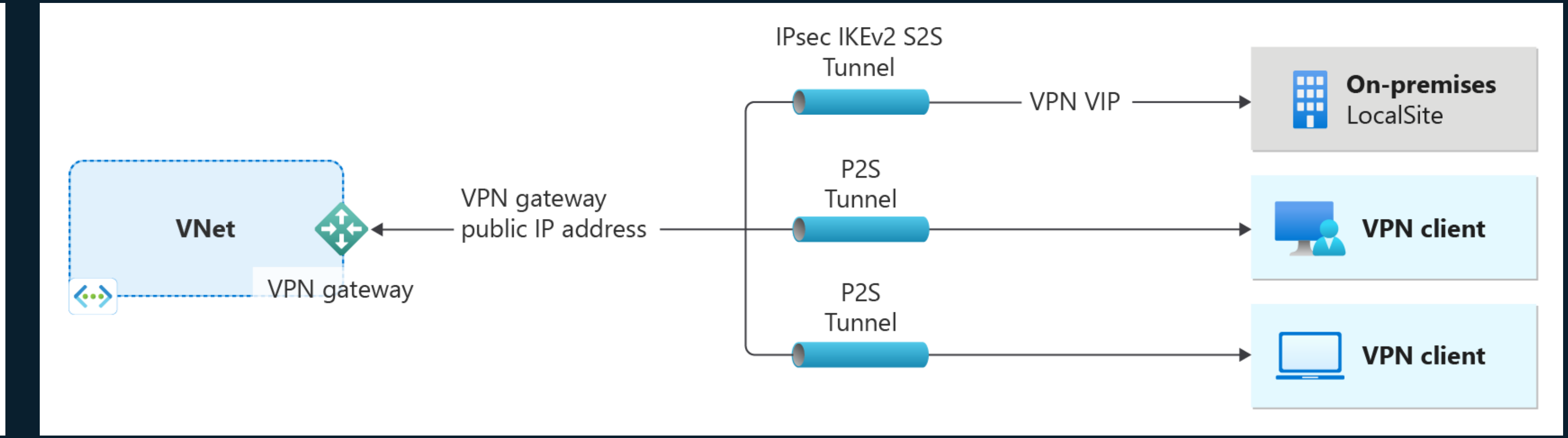
VM-03
Default subnet
192.168.3.0/24
Spoke virtual network 3
192.168.3.0/24

VM-04
Default subnet
192.168.4.0/24
Spoke virtual network 4
192.168.4.0/24

Multi-Cloud or On-premise Connectivity to Azure

- Virtual Network Gateways in the Hub Virtual Networks or Virtual WAN Hubs





ExpressRoute

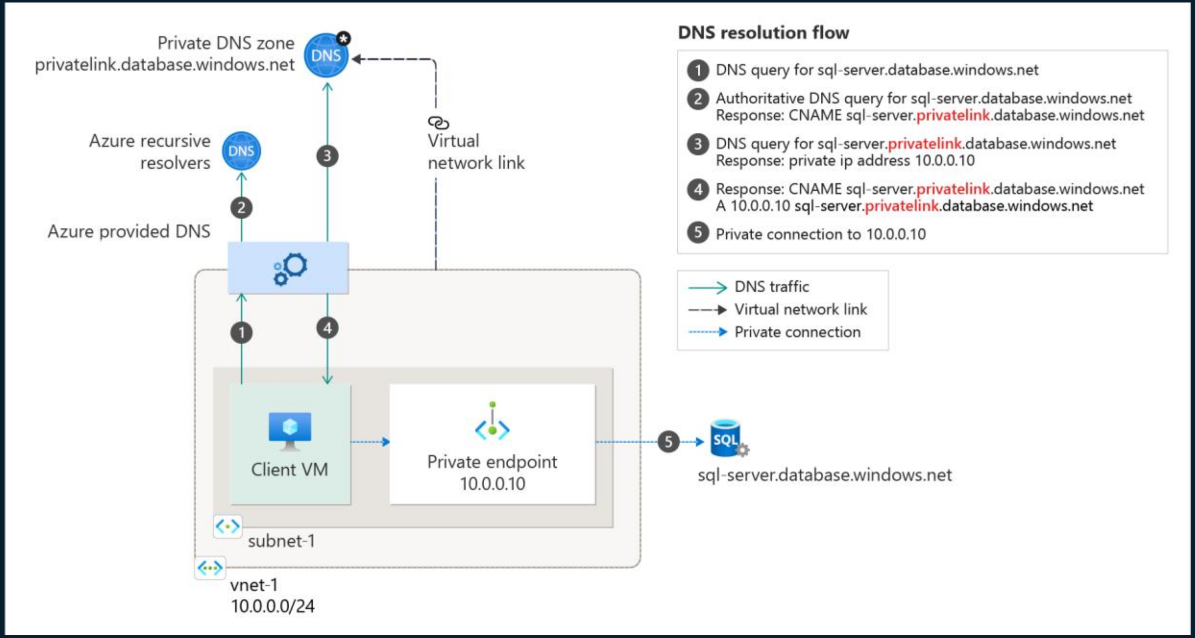
Fast and secure connectivity with an SLA

VPN

Supports Point to Site, Site to Site, and VNet to VNet

Private Networking for PaaS with VNet integration and Private Endpoint

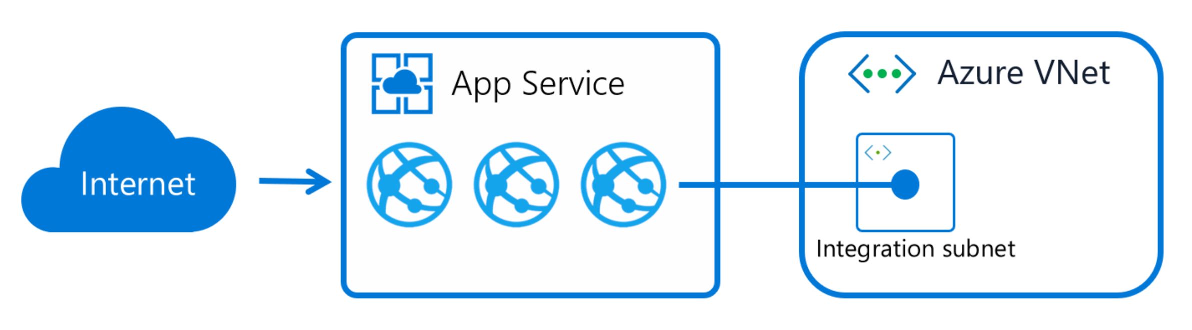
- PaaS service are hosted by Microsoft, so their network is not directly accessible
- A private endpoint can be used to connect to the PaaS service
- VNet integration can be used for PaaS compute service to connect to other services



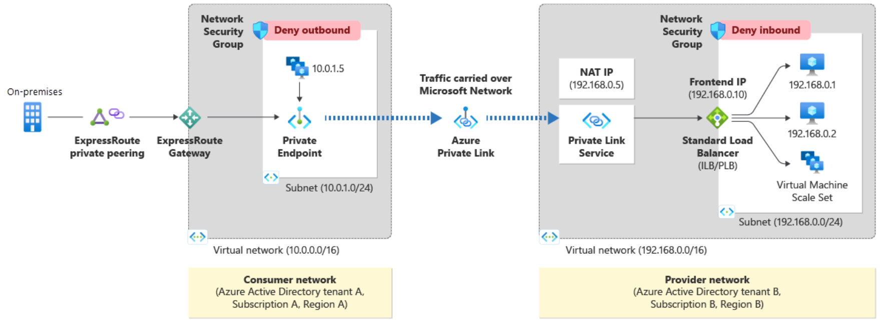
DNS resolution flow

1. DNS query for sql-server.database.windows.net
2. Authoritative DNS query for sql-server.database.windows.net
   Response: CNAME sql-server.privatelink.database.windows.net
3. DNS query for sql-server.privatelink.database.windows.net
   Response: private ip address 10.0.0.10
4. Response: CNAME sql-server.privatelink.database.windows.net
   A 10.0.0.10 sql-server.privatelink.database.windows.net
5. Private connection to 10.0.0.10

Azure Private Endpoint



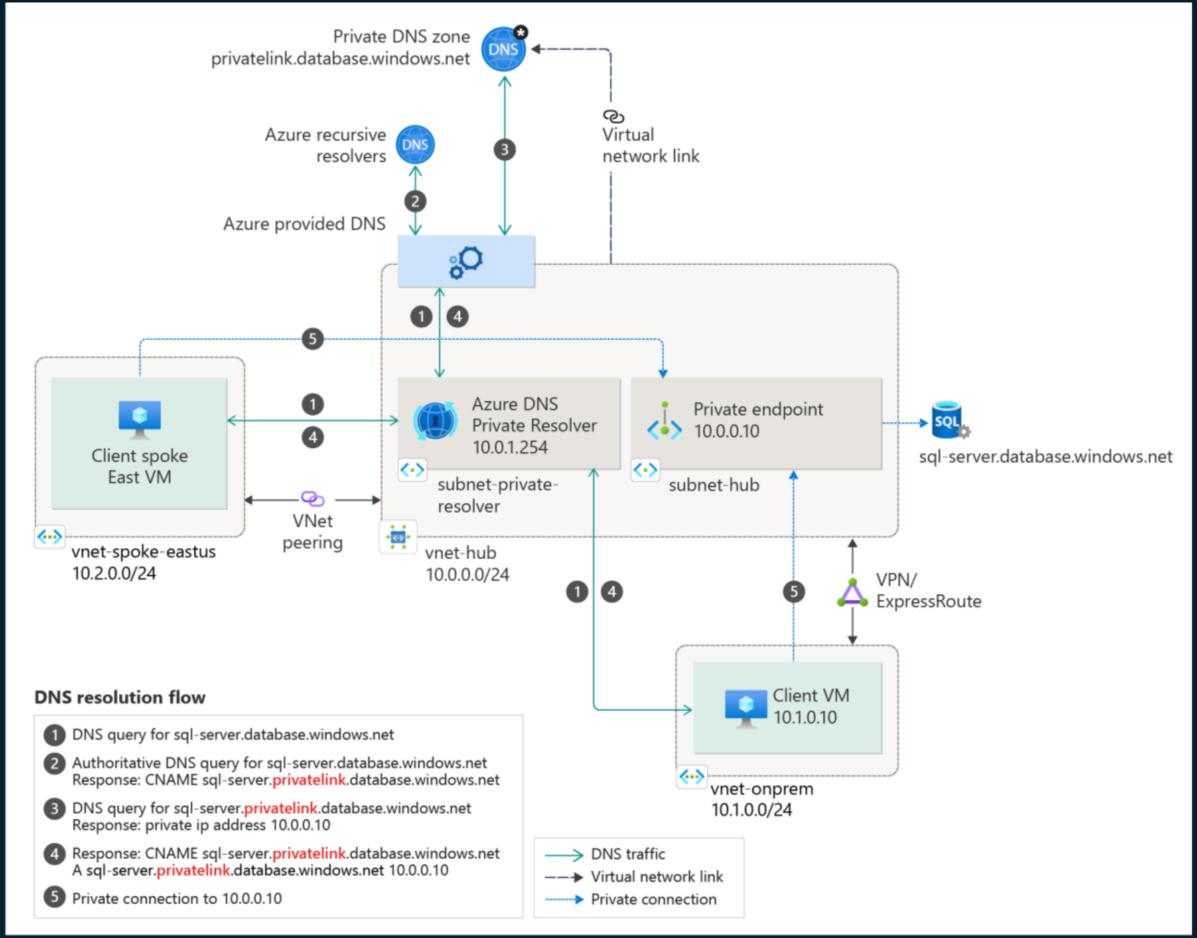
VNet Integration



Azure Private Link Service?

DNS Resolution across peered VNETs or from on-prem with Private Endpoints

- Azure Private DNS Resolver is deployed in the hub VNet or sidecar for Virtual WAN
- Spoke VNet has DNS server set to the private resolver IP

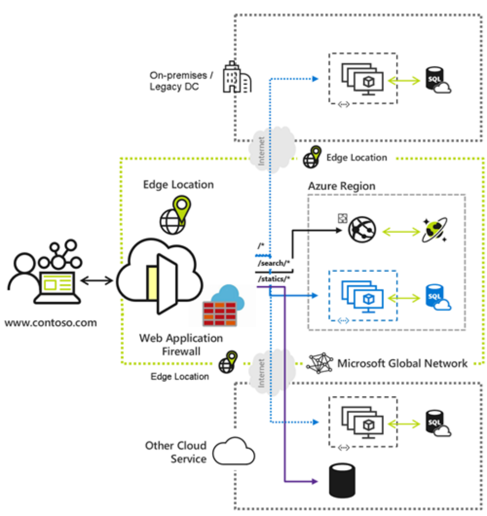


DNS resolution flow

1. DNS query for sql-server.database.windows.net
2. Authoritative DNS query for sql-server.database.windows.net
   Response: CNAME sql-server.privatelink.database.windows.net
3. DNS query for sql-server.privatelink.database.windows.net
   Response: private ip address 10.0.0.10
4. Response: CNAME sql-server.privatelink.database.windows.net
   A sql-server.privatelink.database.windows.net 10.0.0.10
5. Private connection to 10.0.0.10

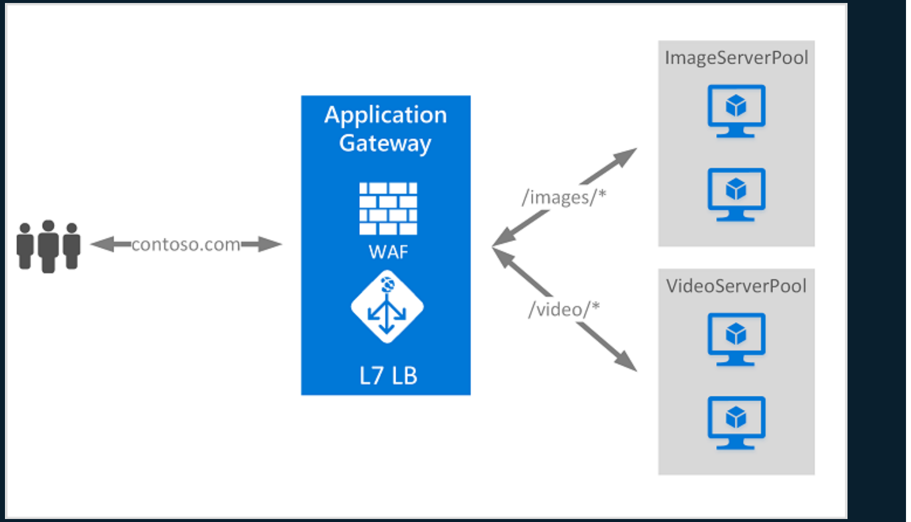
Ingress to Web Apps and APIs with load balancing

- Azure Front Door and / or Azure Application Gateway both offer WAF capabilities
- Azure Front Door can front Azure API Management



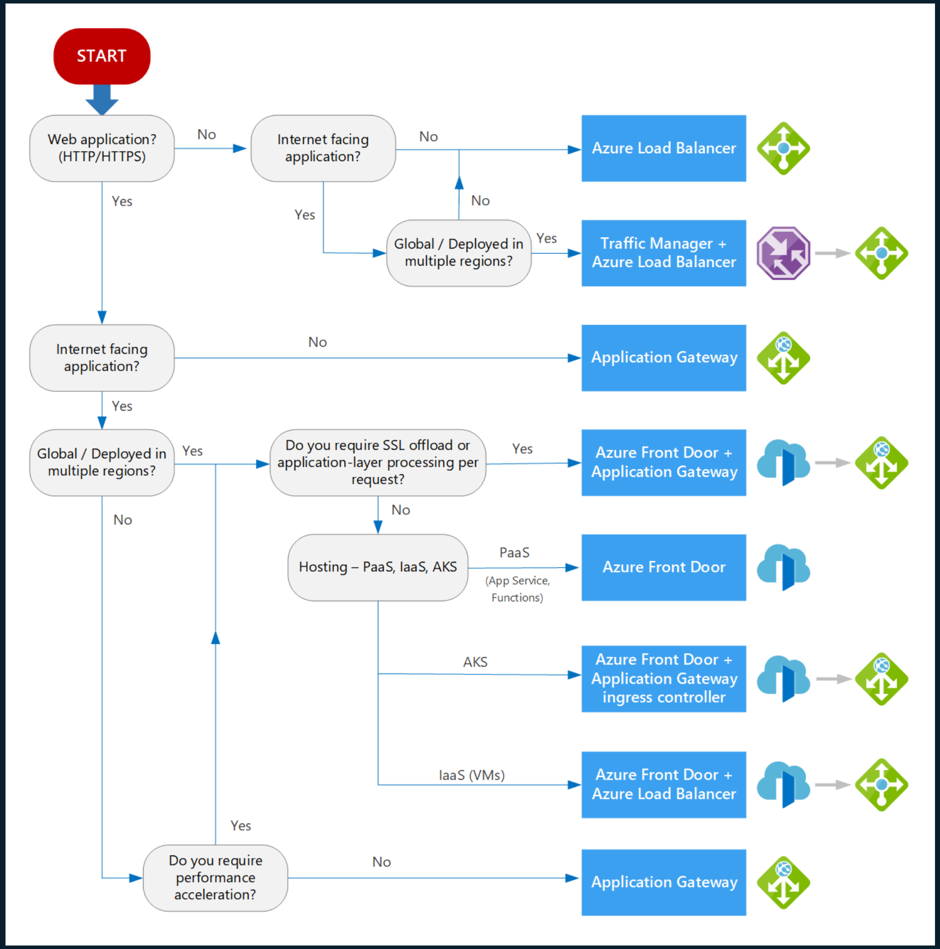
Azure Front Door

Public and supports 118 edge locations



Azure Application Gateway

Can be private



START

Web application? (HTTP/HTTPS)

No

Internet facing application?

No

Azure Load Balancer

Yes

No

Global / Deployed in multiple regions?

Yes

Traffic Manager + Azure Load Balancer

Yes

Internet facing application?

No

Application Gateway

Yes

Global / Deployed in multiple regions?

Yes

Do you require SSL offload or application-layer processing per request?

Yes

Azure Front Door + Application Gateway

No

No

Hosting – PaaS, IaaS, AKS

PaaS (App Service, Functions)

Azure Front Door

AKS

Azure Front Door + Application Gateway ingress controller

IaaS (VMs)

Azure Front Door + Azure Load Balancer

Yes

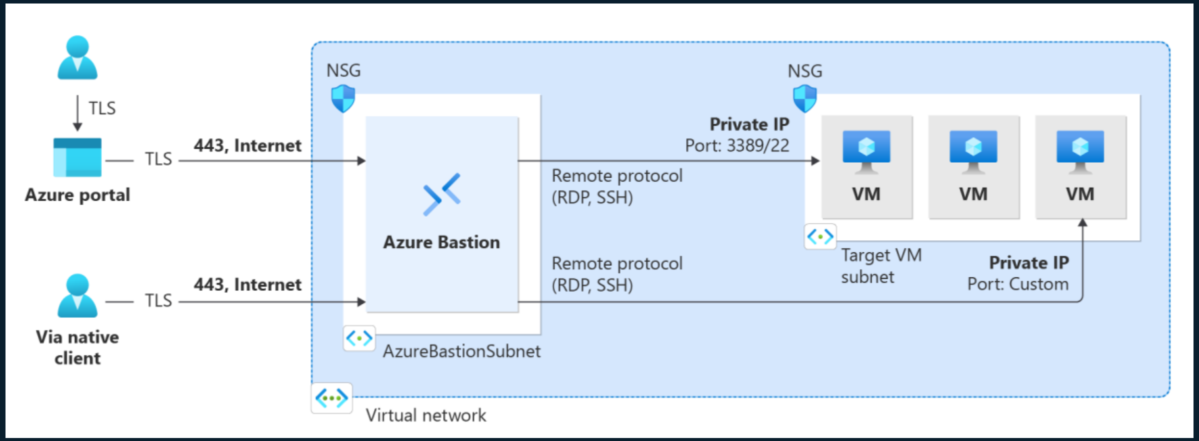
Do you require performance acceleration?

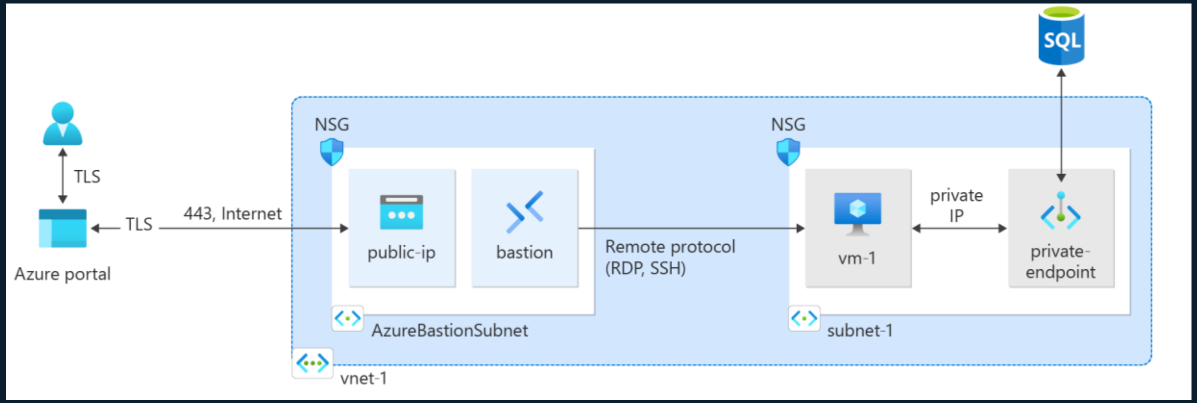
No

Application Gateway

Accessing Virtual Machines / Admin Servers via Azure Bastion

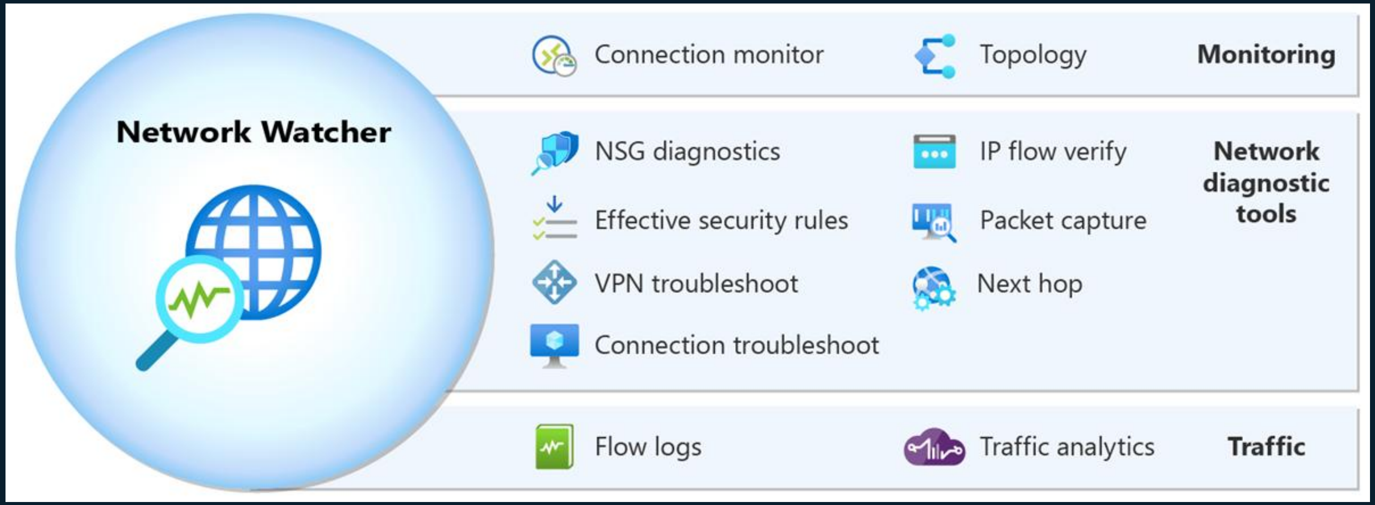
- Azure Bastion is a PaaS service for a public or private secure access method
- It is useful where private networking is use throughout, but you need break glass access to hosts
- E.g. Use a VM as a jump server to connect to a private Azure SQL Database via its private endpoint





Monitoring network traffic with Azure Network Watcher and VNet flow logs

- NSG flow logs are deprecated, use VNet flow logs

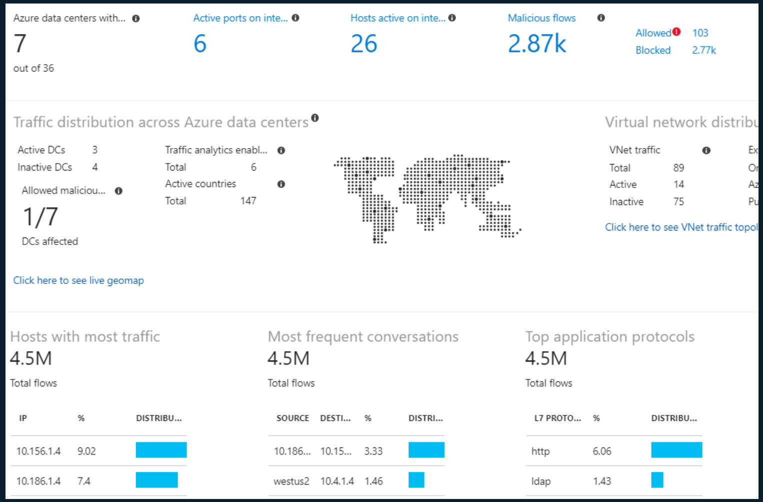


Network Watcher

Connection monitor · Topology — Monitoring

NSG diagnostics · IP flow verify · Effective security rules · Packet capture · VPN troubleshoot · Next hop · Connection troubleshoot — Network diagnostic tools

Flow logs · Traffic analytics — Traffic



Azure data centers with... 7 out of 36

Active ports on inte... 6

Hosts active on inte... 26

Malicious flows 2.87k — Allowed 103, Blocked 2.77k

Traffic distribution across Azure data centers

Active DCs 3
Inactive DCs 4

Allowed maliciou... 1/7 DCs affected

Traffic analytics enabl... Total 6

Active countries Total 147

Click here to see live geomap

Virtual network distribu

VNet traffic
Total 89
Active 14
Inactive 75

Click here to see VNet traffic topol

Hosts with most traffic
4.5M
Total flows

IP	%	DISTRIBU...
10.156.1.4	9.02	
10.186.1.4	7.4	

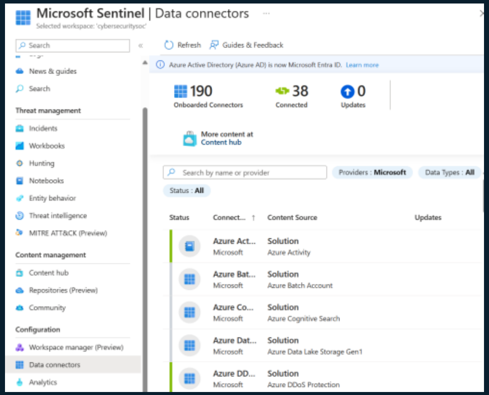
Most frequent conversations
4.5M
Total flows

SOURCE	DESTI...	%	DISTRI...
10.186...	10.15...	3.33	
westus2	10.4.1.4	1.46	

Top application protocols
4.5M
Total flows

L7 PROTO...	%	DISTRIBU...
http	6.06	
ldap	1.43	

Traffic Analytics



Microsoft Sentinel | Data connectors
Selected workspace: 'cybersecuritysoc'

Search · Refresh · Guides & Feedback

News & guides
Search

Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)

Content management
Content hub
Repositories (Preview)
Community

Configuration
Workspace manager (Preview)
Data connectors
Analytics

Azure Active Directory (Azure AD) is now Microsoft Entra ID. Learn more

190 Onboarded Connectors · 38 Connected · 0 Updates

More content at Content hub

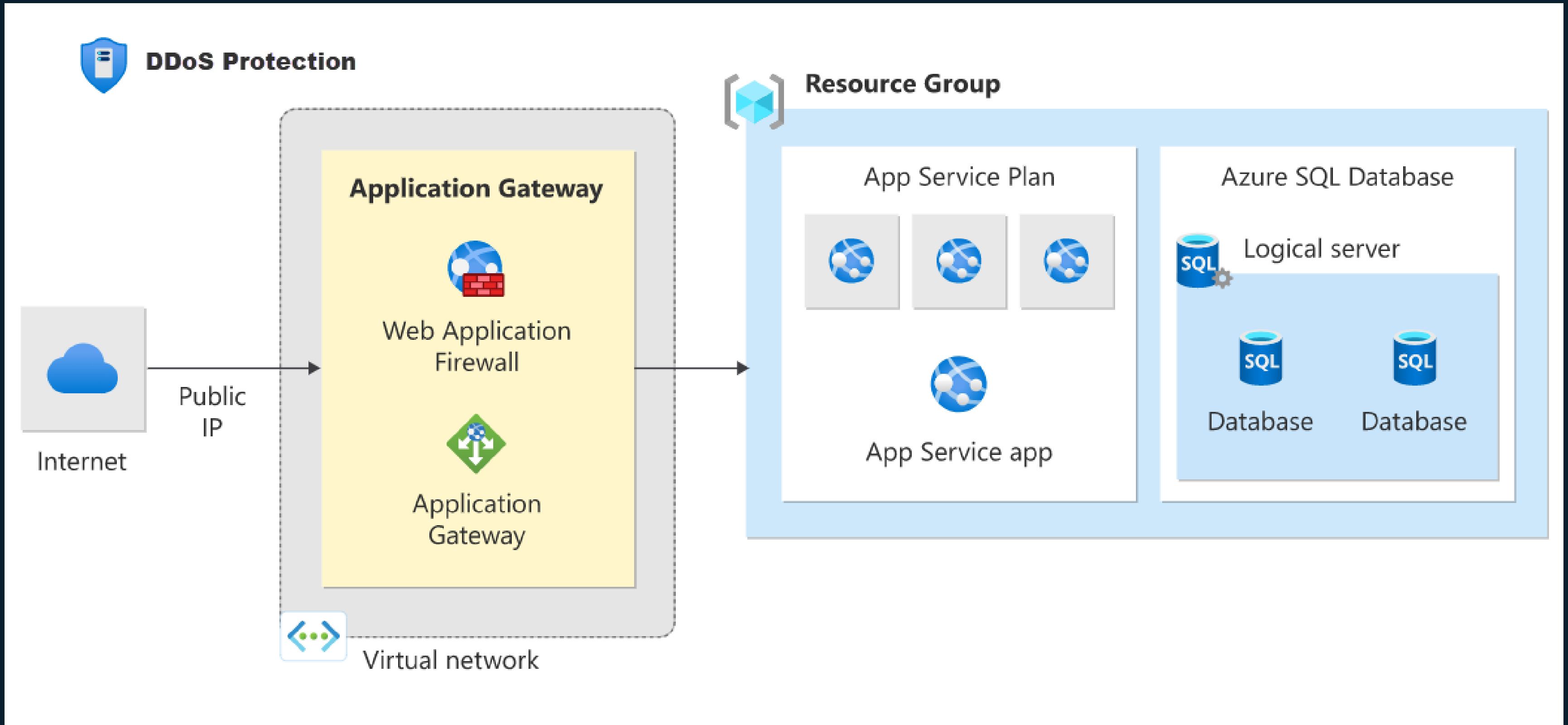
Search by name or provider · Providers : Microsoft · Data Types : All · Status : All

Status	Connect... ↑	Content Source	Updates
	Azure Act... Microsoft	Solution Azure Activity	
	Azure Bat... Microsoft	Solution Azure Batch Account	
	Azure Co... Microsoft	Solution Azure Cognitive Search	
	Azure Dat... Microsoft	Solution Azure Data Lake Storage Gen1	
	Azure DD... Microsoft	Solution Azure DDoS Protection	

Microsoft Sentinel
(SIEM – Security Information and Event Management)

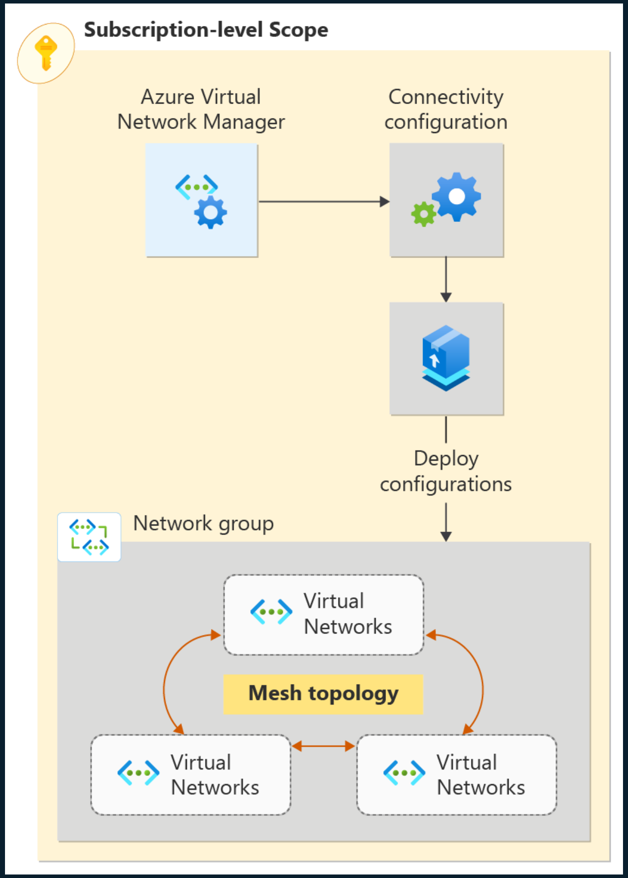
Distributed Denial of Service (DDOS) Protection

- Single plan for all VNet (more cost effective at scale)
- Per public IP



Azure Virtual Network Manager

- A single pane of glass to configure:
  - Peering
  - Routing
  - Network Security Group Rules
  - IP Address Management (IPAM)



Quiz

- Which network resource can be used to micro-segment a network?

Microsoft

Thank you

© Copyright Microsoft Corporation. All rights reserved.