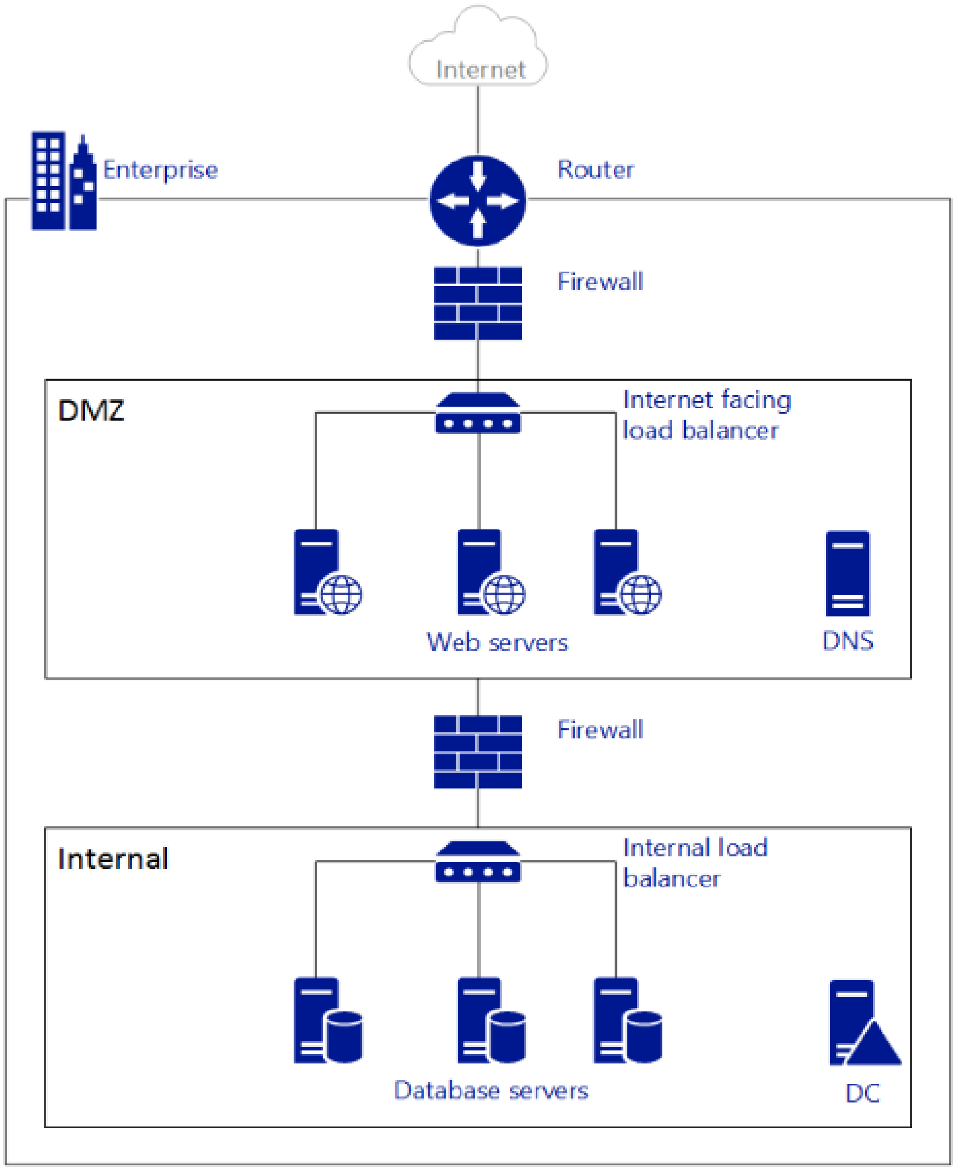
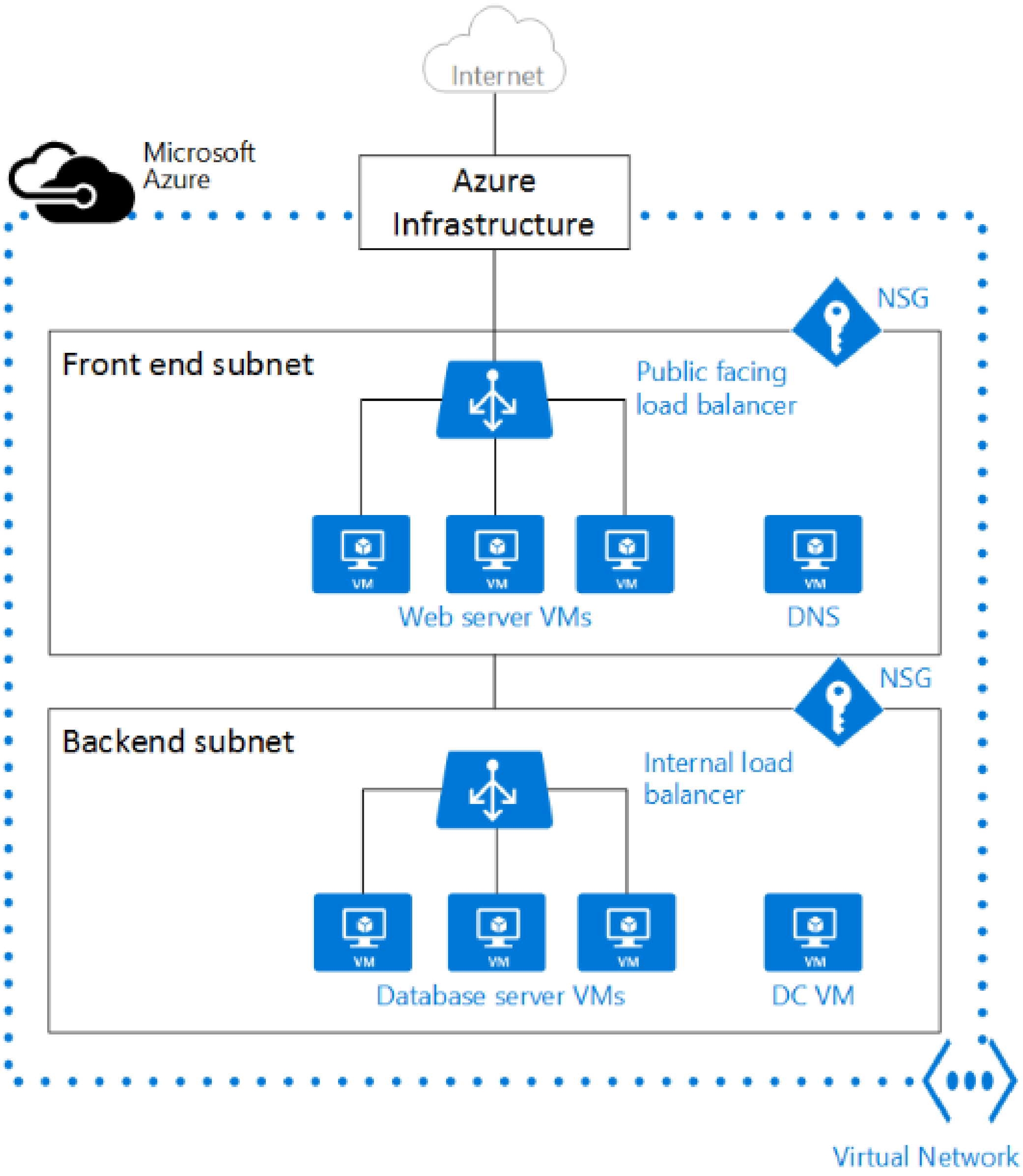
AzureCon

Azure Networking Overview

Abbas Mir
CSA

Azure Virtual Networks





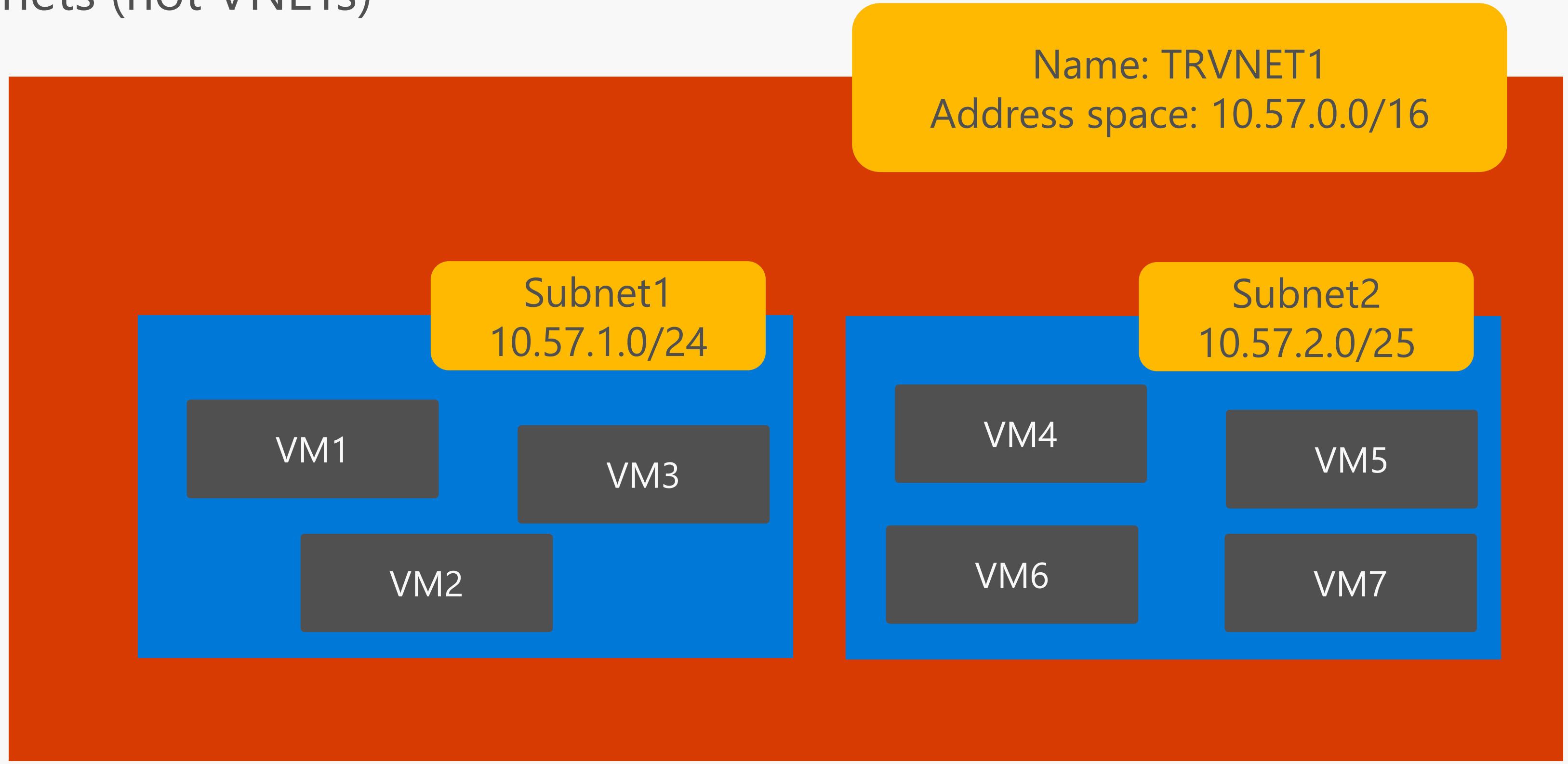
Subnet

IP subnet

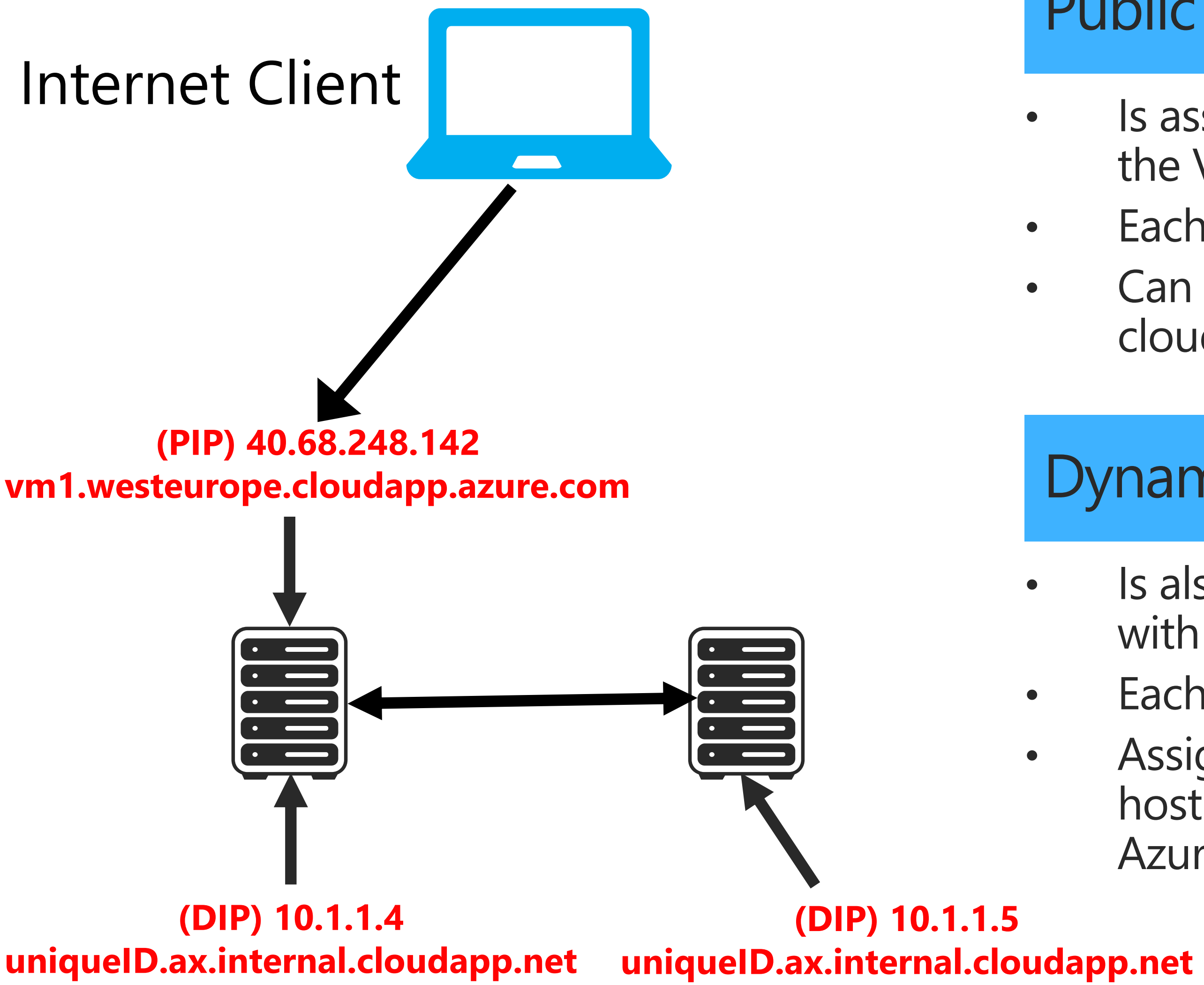
Provides full layer-3 semantics and partial layer-2 semantics (DHCP, ARP, no broadcast/multicast)

Subnets can span only one range of contiguous IP addresses

VMs can be deployed only to subnets (not VNETs)



Single VM Connectivity



Internet Client

(PIP) 40.68.248.142
vm1.westeurope.cloudapp.azure.com

(DIP) 10.1.1.4
uniqueID.ax.internal.cloudapp.net

(DIP) 10.1.1.5
uniqueID.ax.internal.cloudapp.net

Public IP Address

- Is assigned to the VM NIC and allows direct communication with the VM over the Internet
- Each individual VM NIC can reserve a separate public IP address
- Can be assigned to a DNS A record which is stored in the cloudapp.azure.com zone on Azure internal DNS servers

Dynamic IP Address

- Is also assigned to the VM NIC and allows direct communication with other VM's in the same or other VNet's
- Each individual VM NIC can reserve a separate private IP address
- Assigned to a DNS A record with an auto generated unique hostname and is stored in the ax.internal.cloudapp.net zone on Azure internal DNS servers

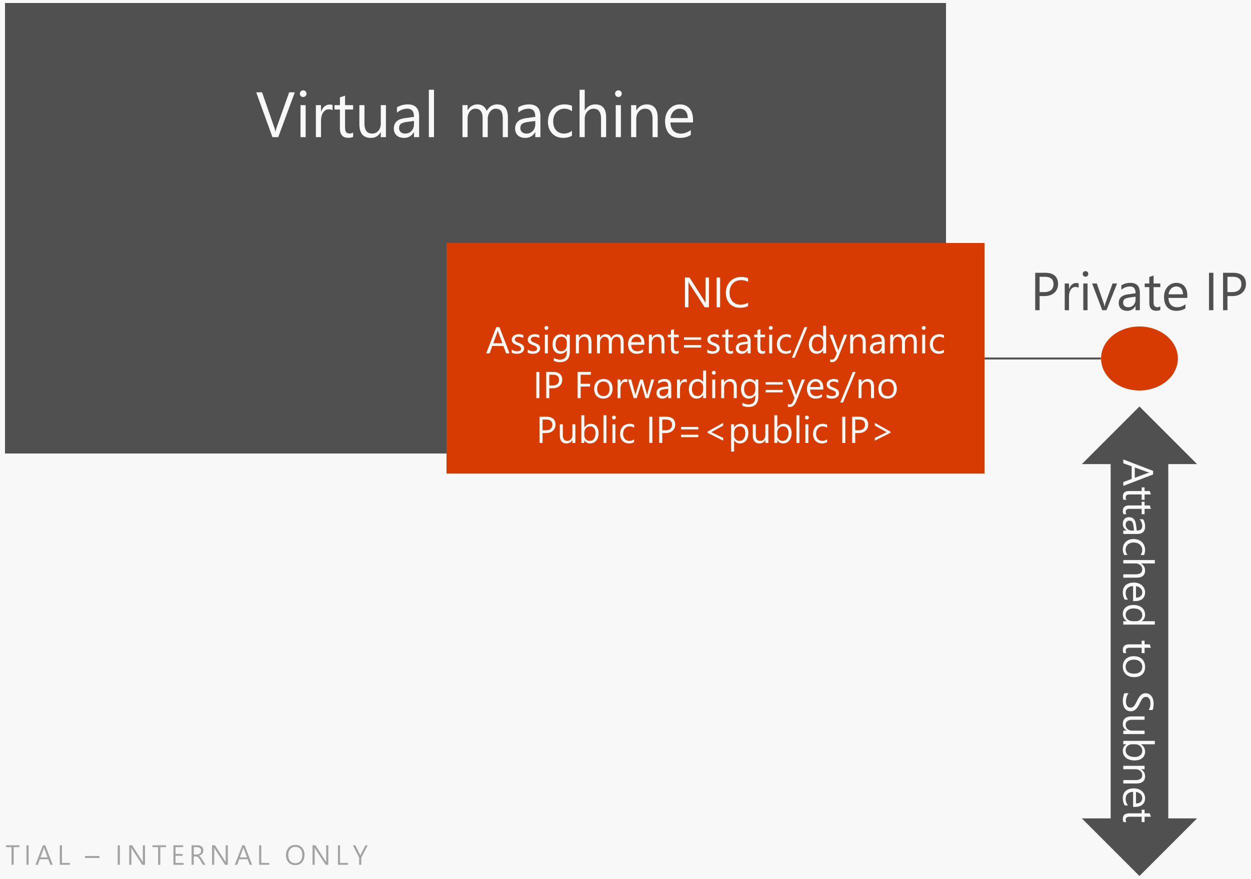
Network Interface

Virtual NIC that connects a VM to a Subnet

One private IP address (private == included in the subnet's IP range, not necessarily RFC1918)

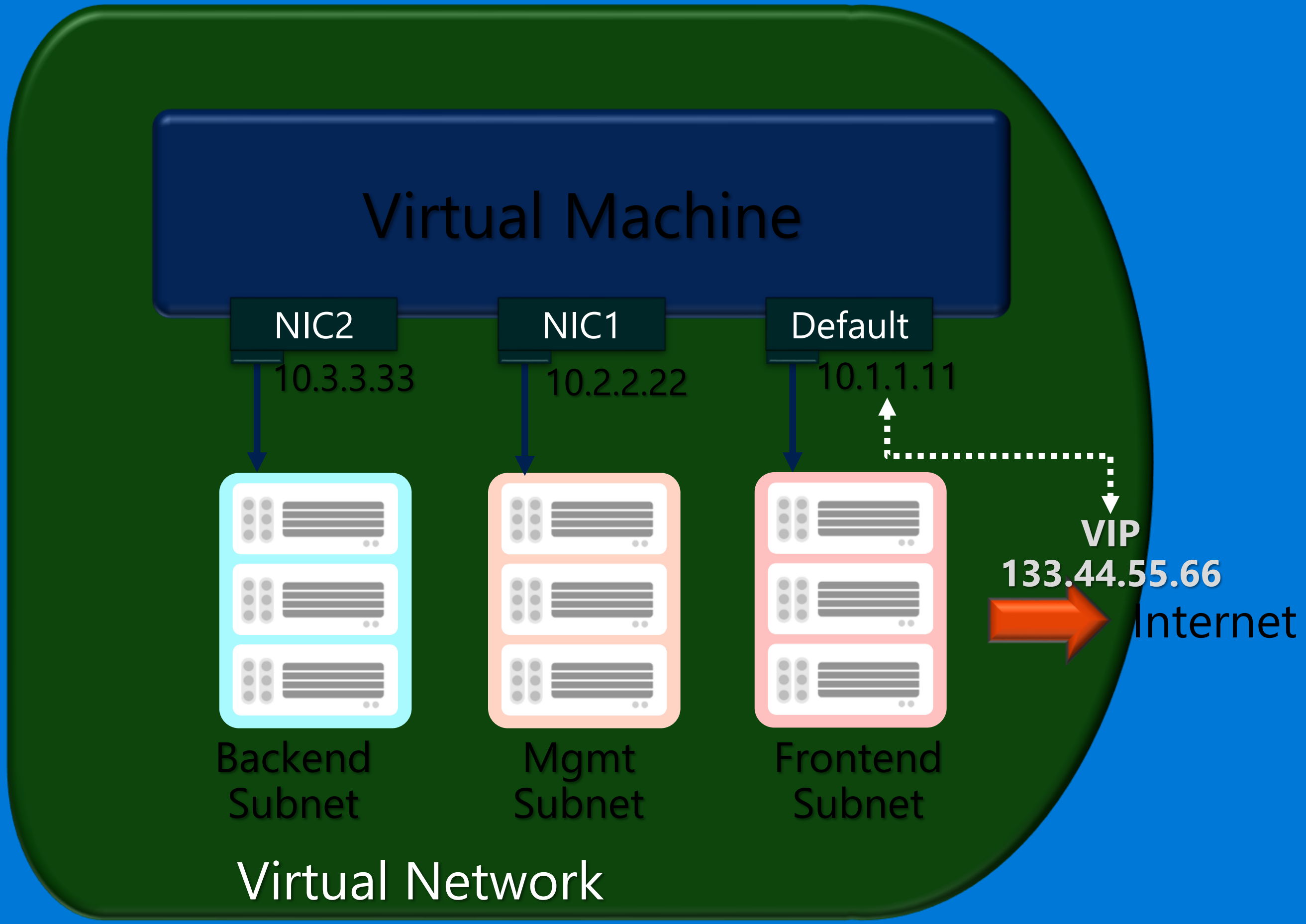
Private IP address always assigned via Azure DHCP

- Dynamic assignment = DHCP assigns new IP when VM is restarted
- Static assignment =DHCP assigns always the same IP
- IP forwarding = NIC can receive packets with destination IP address different from its private IP
- Public IP = NAT address associated to the NIC (more on this later)



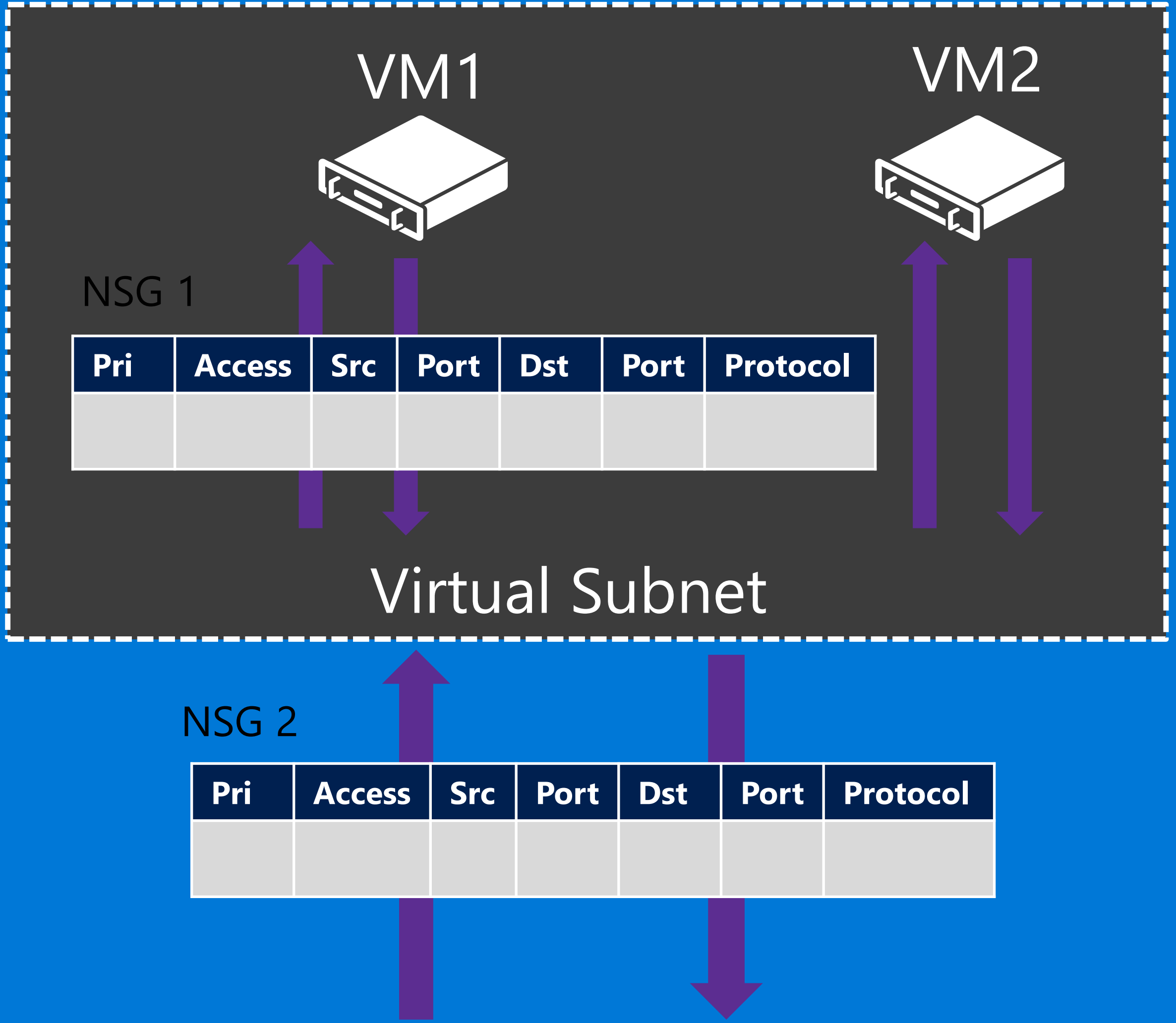
Multiple NICs in Azure VMs

- Up to 16 NICs per VM
- NSG and Routes on all NICs
- Can separate frontend, backend, and management



Network Security Group (NSG)

- Prioritized set of rules
- Applied at the VM and/ or Subnet
- Applies to Internal and External traffic
- Default Tags: Virtual Network, Internet, AzureLoadBalancer
- Default rules: 65000 and above
- API audit logs



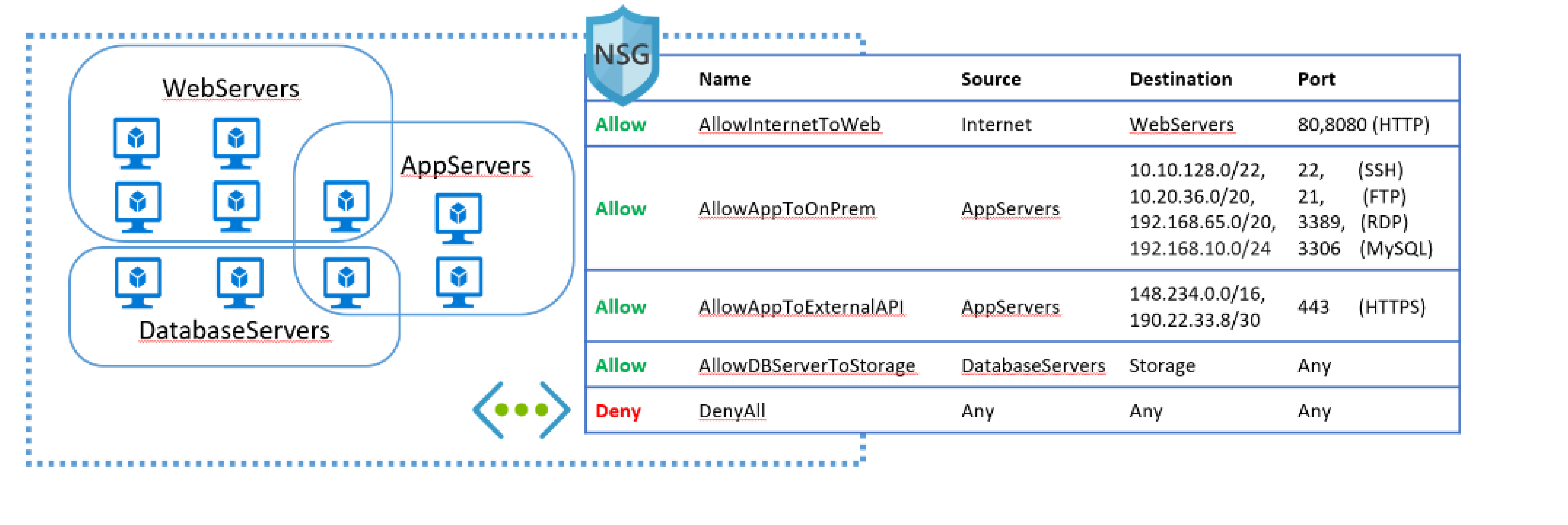
Pri	Access	Src	Port	Dst	Port	Protocol

Pri	Access	Src	Port	Dst	Port	Protocol

Simplifying NSG Management

New

- Service Tags: Symbolic monikers instead of IP addresses for Azure Services
- Application Security Groups: User defined monikers for grouping VMs
- Augmented NSG Rules: Simplified rule expressions

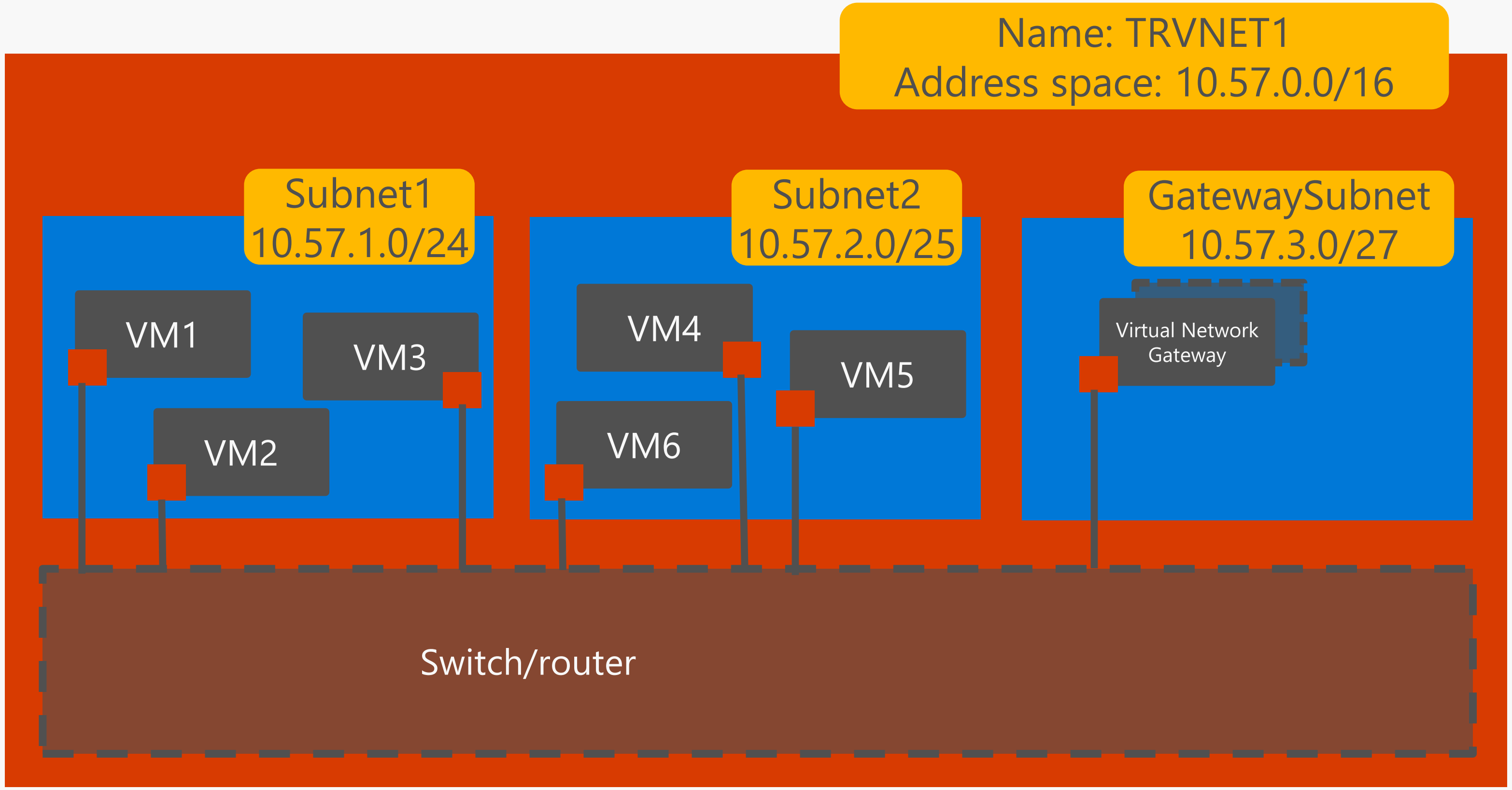


	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,8080 (HTTP)
Allow	AllowAppToOnPrem	AppServers	10.10.128.0/22, 10.20.36.0/20, 192.168.65.0/20, 192.168.10.0/24	22, (SSH) 21, (FTP) 3389, (RDP) 3306 (MySQL)
Allow	AllowAppToExternalAPI	AppServers	148.234.0.0/16, 190.22.33.8/30	443 (HTTPS)
Allow	AllowDBServerToStorage	DatabaseServers	Storage	Any
Deny	DenyAll	Any	Any	Any

Cross-premises connectivity

Virtual Network Gateway

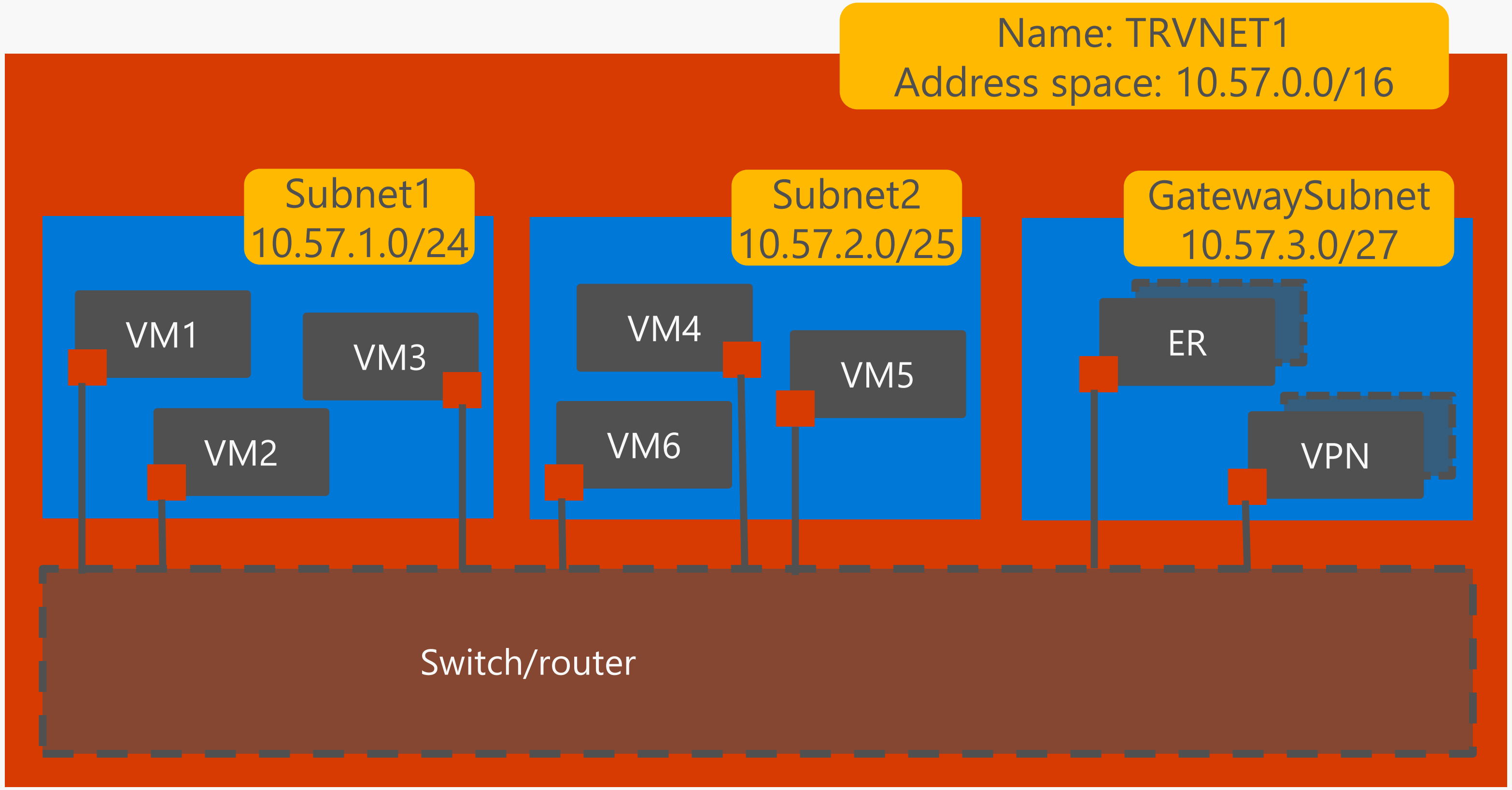
Virtual layer-3 device that routes traffic to remote networks



- Virtual device attached to an Azure VNet (similar to VMs)
- Always provisioned in a reserved subnet named «GatewaySubnet»
- Highly available service
- The «GatewaySubnet» is part of the VNet's address space (/27 or bigger)
- Each Gateway is associated to a public IP address

Virtual Network Gateway

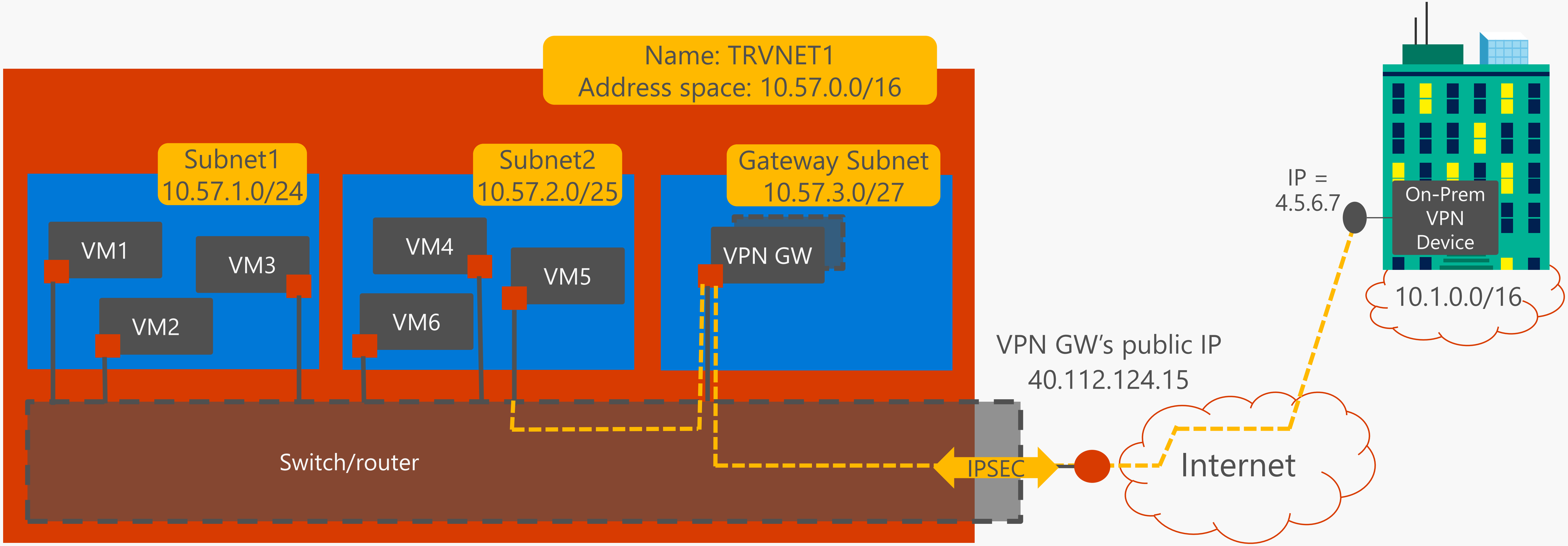
Gateway types: «Vpn» or «ExpressRoute»



- Vpn gateways: route traffic to remote networks over internet-based IPSec tunnels
- ExpressRoute gateways: route traffic to on-prem networks over dedicated connectivity
- Can coexist in the same VNet

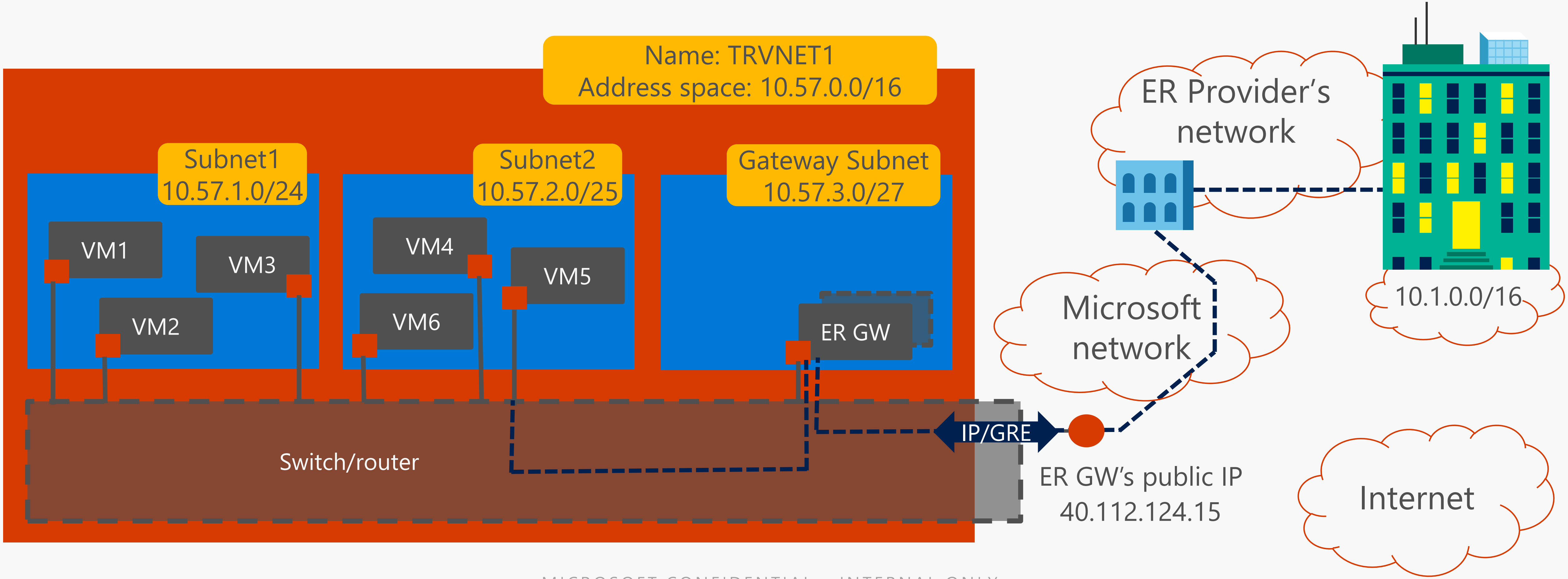
Site2site connectivity

Internet-based IPSec VPNs

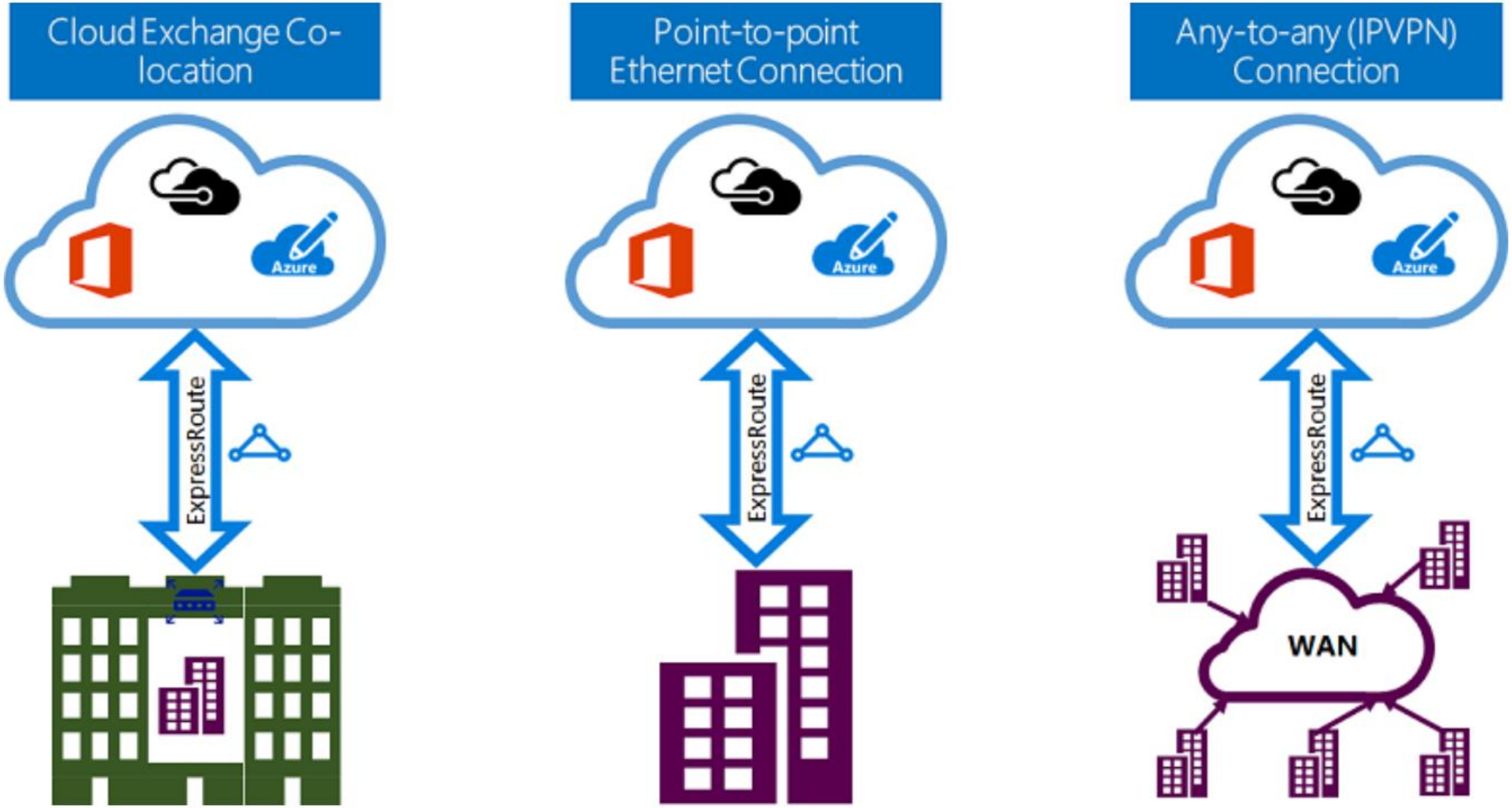


ExpressRoute

Dedicated connectivity to on-prem networks



ExpressRoute Connectivity Options



Cloud Exchange Co-location

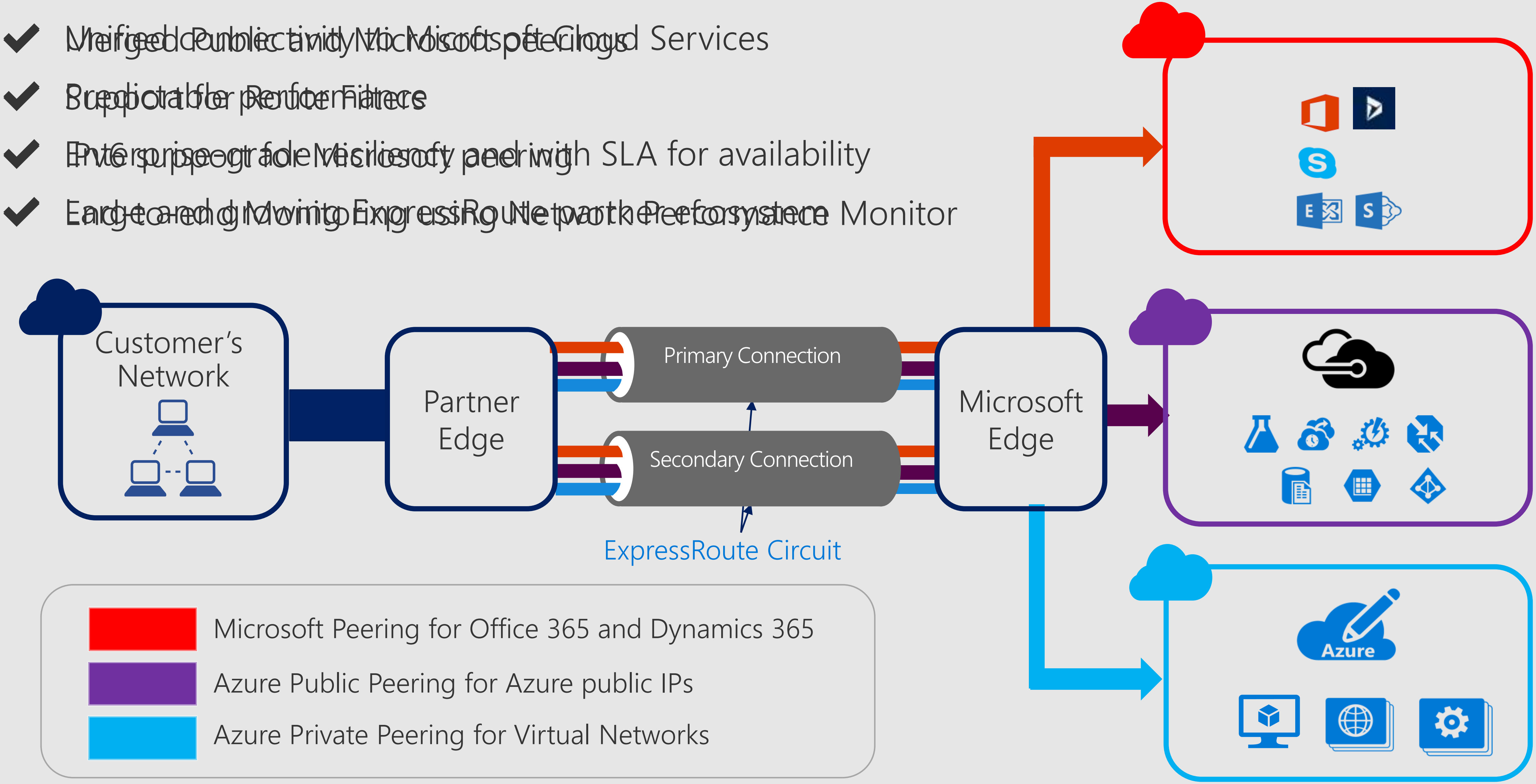
Point-to-point Ethernet Connection

Any-to-any (IPVPN) Connection

ExpressRoute

New

- ✓ Unified Connectivity to Microsoft Cloud Services
- ✓ Merged Public and Microsoft peerings
- ✓ Predictable Performance
- ✓ Support for Route Filters
- ✓ Enterprise-grade resiliency and with SLA for availability
- ✓ IPv6 support for Microsoft peering
- ✓ End-to-end Monitoring using Network Performance Monitor
- ✓ Large and growing ExpressRoute partner ecosystem



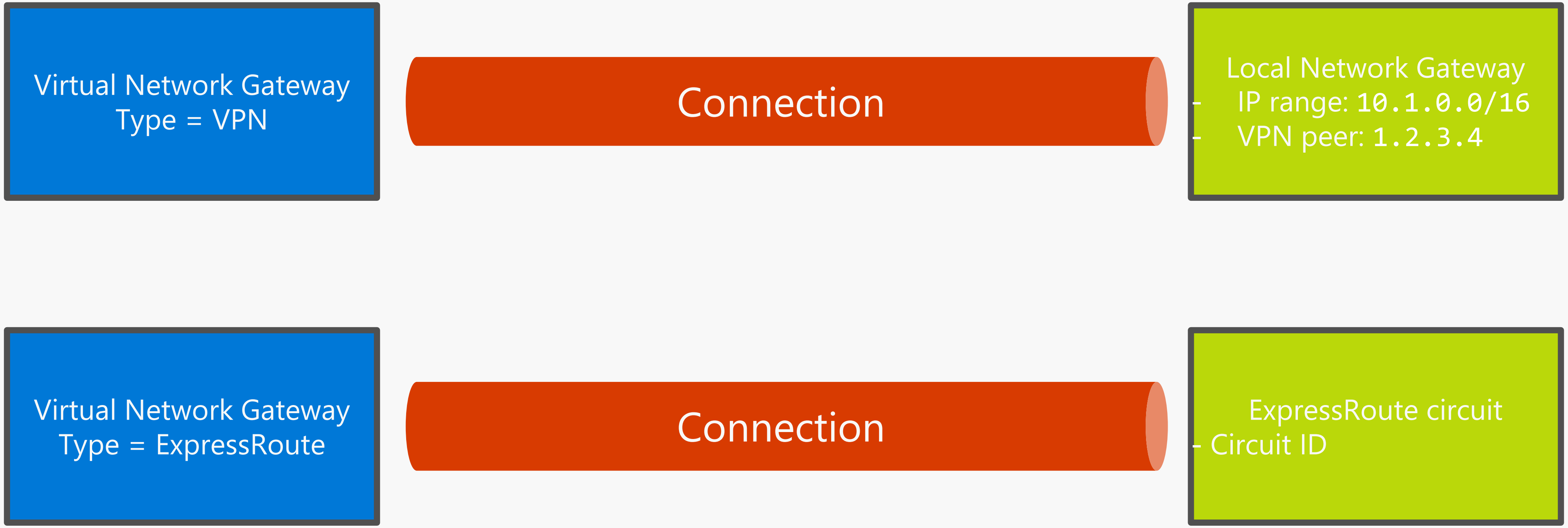
🟥 Microsoft Peering for Office 365 and Dynamics 365

🟪 Azure Public Peering for Azure public IPs

🟦 Azure Private Peering for Virtual Networks

Configuring cross-premises connectivity (ARM)

IPSec and ER connections share the same model



Virtual Network Gateway
Type = VPN

Connection

Local Network Gateway
- IP range: `10.1.0.0/16`
- VPN peer: `1.2.3.4`

Local Network Gateways describe an on-prem network

Virtual Network Gateway
Type = ExpressRoute

Connection

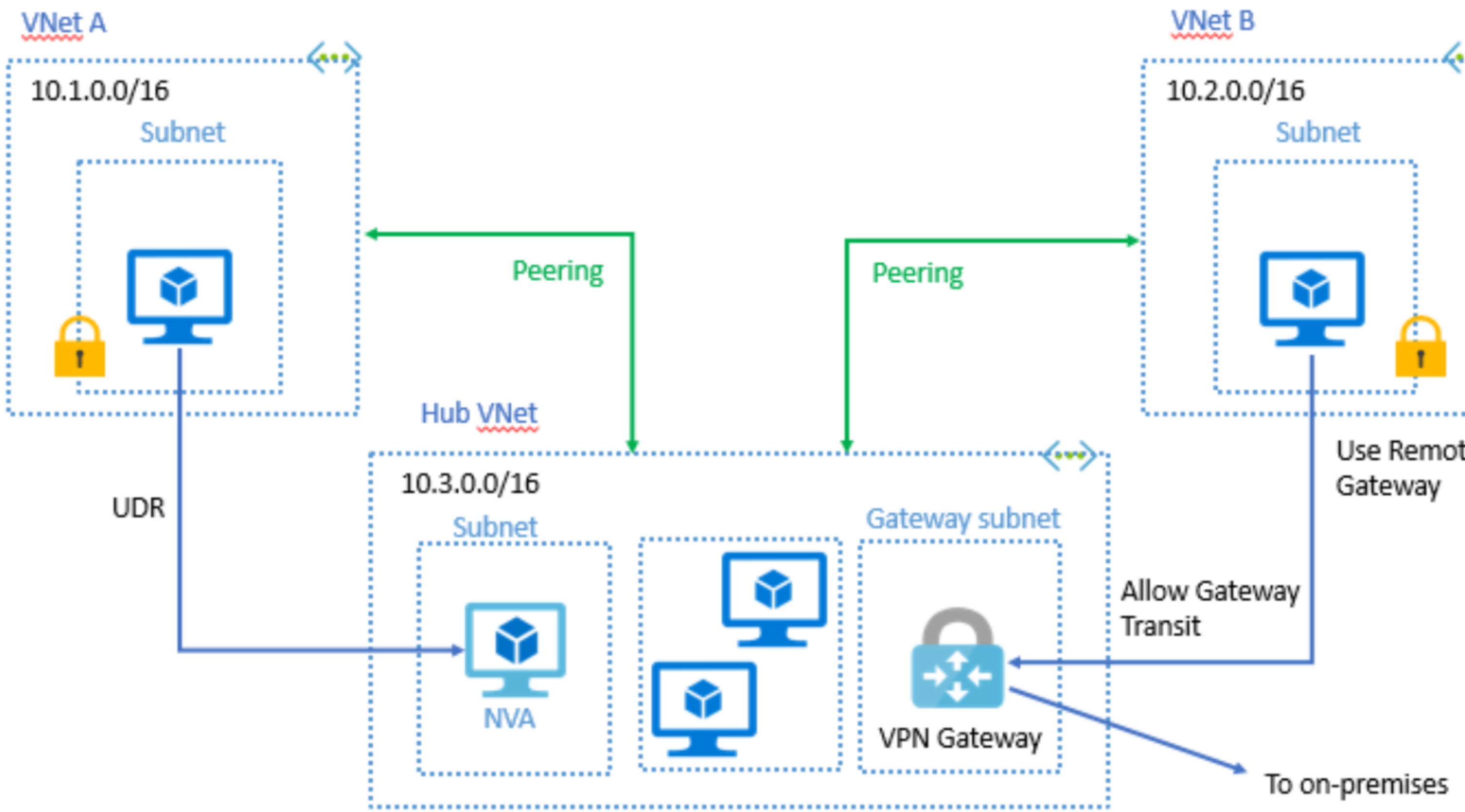
ExpressRoute circuit
- Circuit ID

Reference to a physical connection to an on-prem network

Connecting VNets

VNet Peering

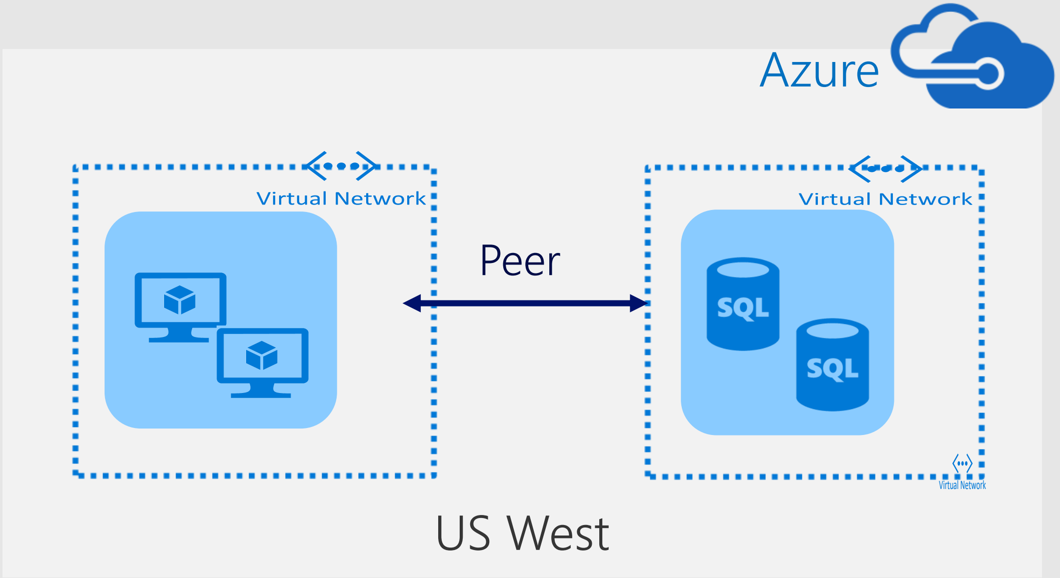
- Extend your Azure virtual network to other Azure virtual networks over the Microsoft backbone infrastructure



Roadmap

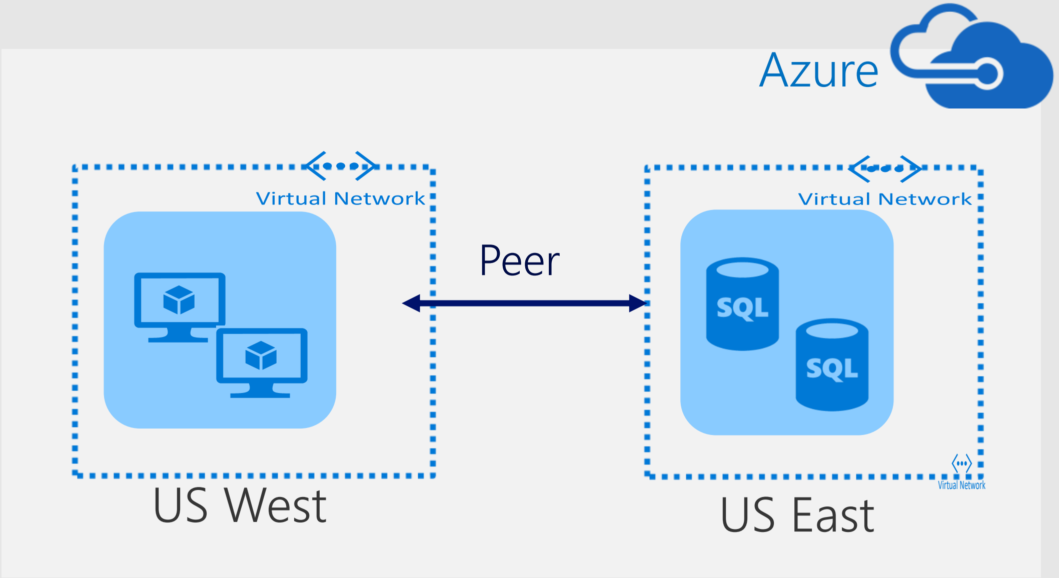
VNet peering

In-region VNet Peering



- Large private networks in Azure through peered Vnets
- Enables hub and spoke architectures in Azure

Global VNet Peering

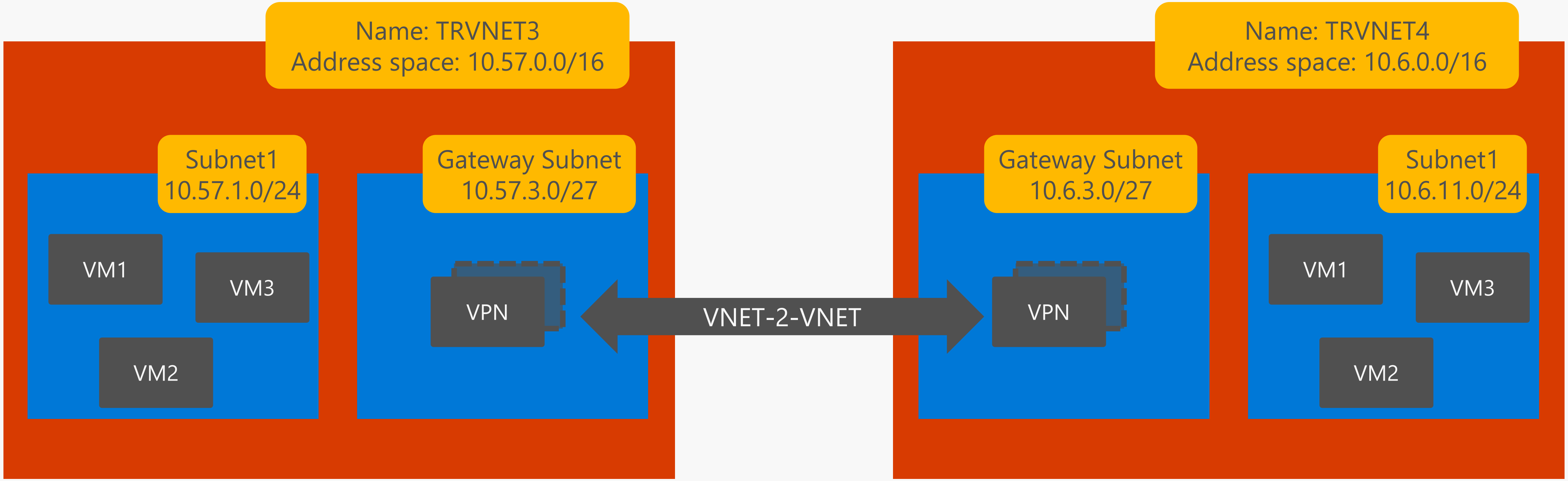


- Global private networks in Azure through peered VNets
- Private: no internet, through Backbone
- High bandwidth cross-region connectivity

MICROSOFT CONFIDENTIAL – INTERNAL ONLY

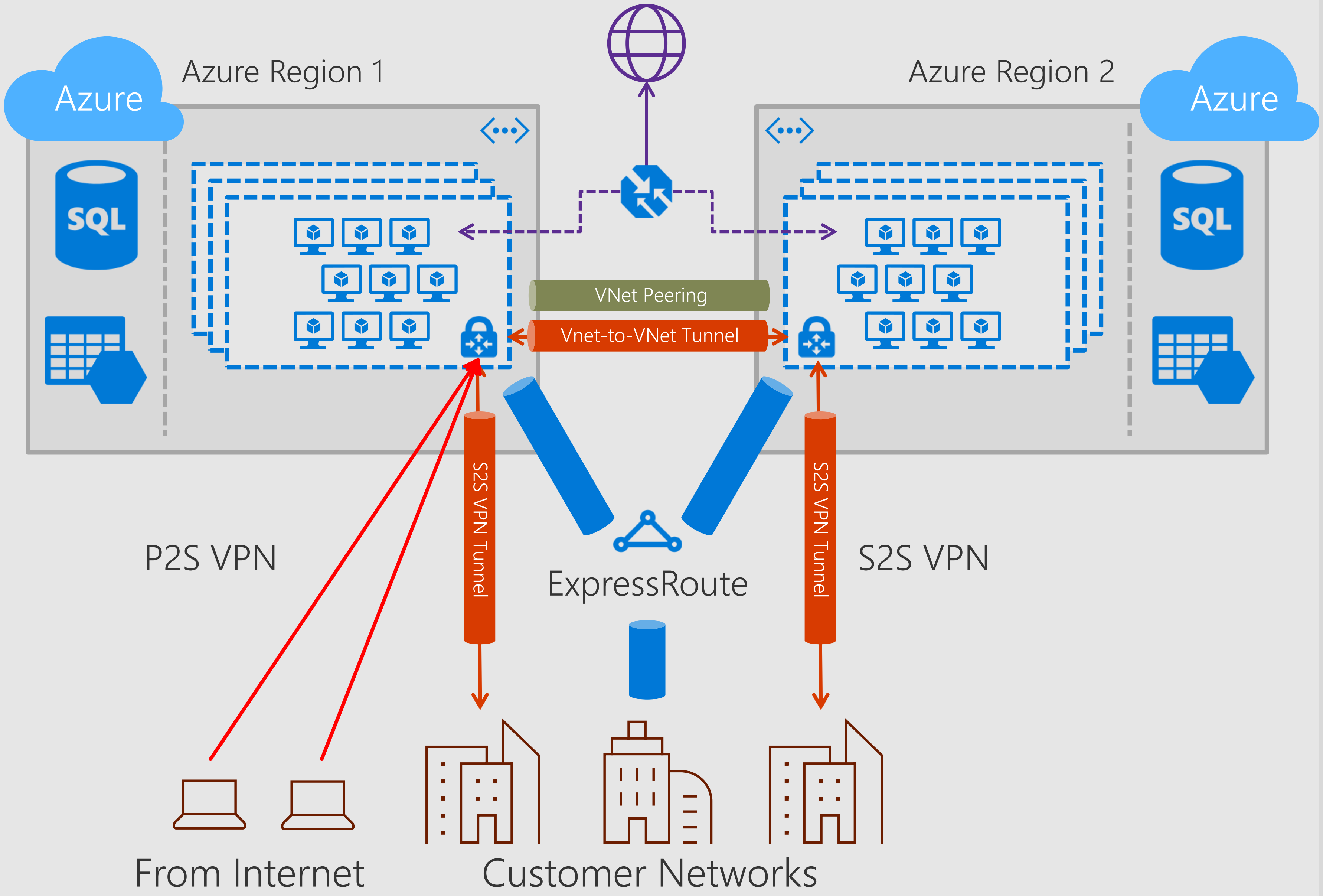
VNET-2-VNET connectivity

VNETs can be connected with each other via IPSec tunnels



MICROSOFT CONFIDENTIAL – INTERNAL ONLY

Connecting VNETs & Cross-Premises Connectivity



New

ExpressRoute

- IPv6 support for Office 365 and Azure PaaS
- Azure services through Microsoft peering
- End-to-end monitoring using Network Performance Monitor

VPN

- New VPN SKUs—6X perf. Improvement
- Monitoring—Azure monitor and Resource Health check
- Apply custom IPsec/IKE policy for compliance
- Download VPN device scripts for seamless configurations

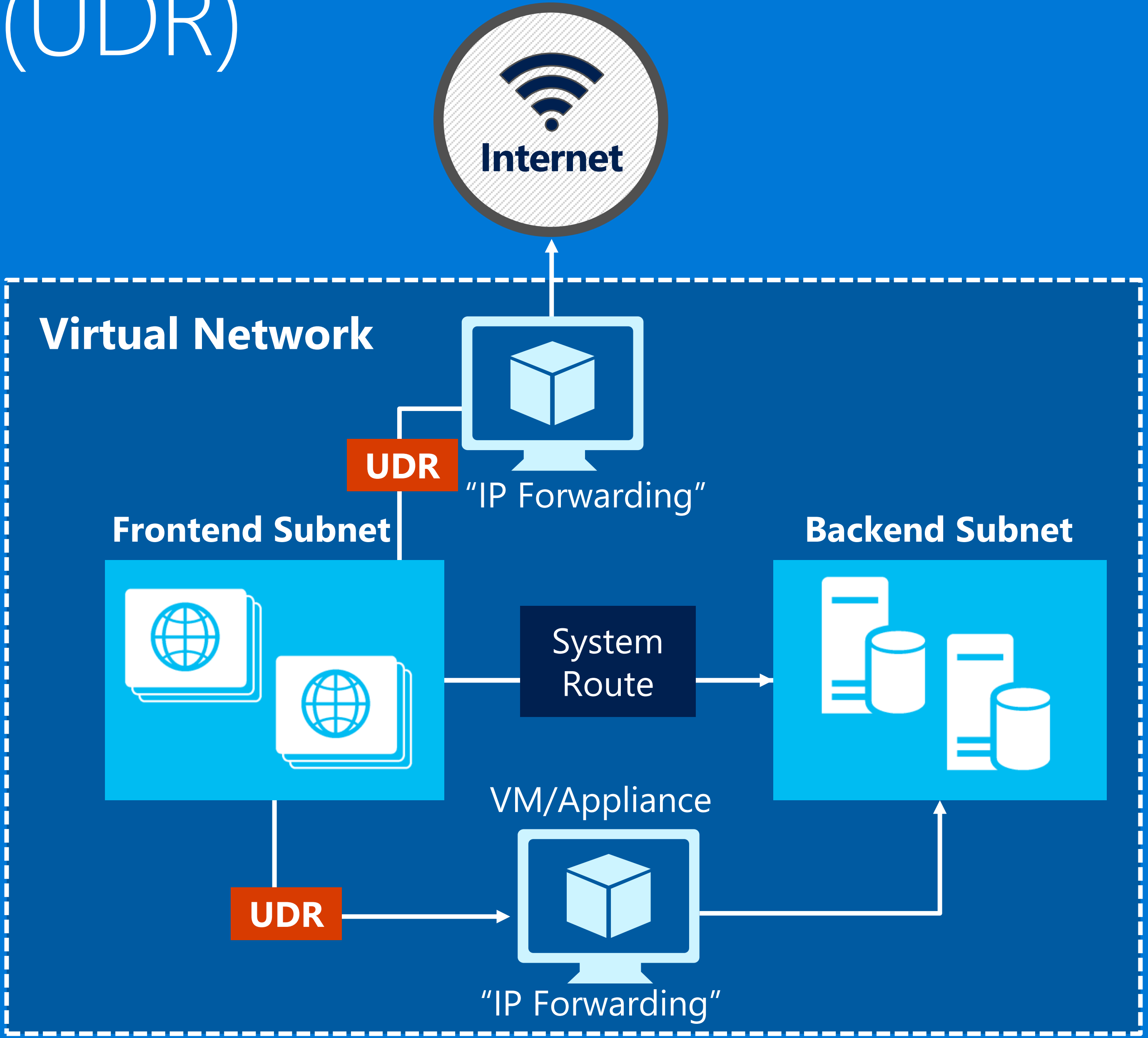
Point-to-site connectivity

- Support for macOS clients
- AD authentication for clients

Routing in Azure VNets

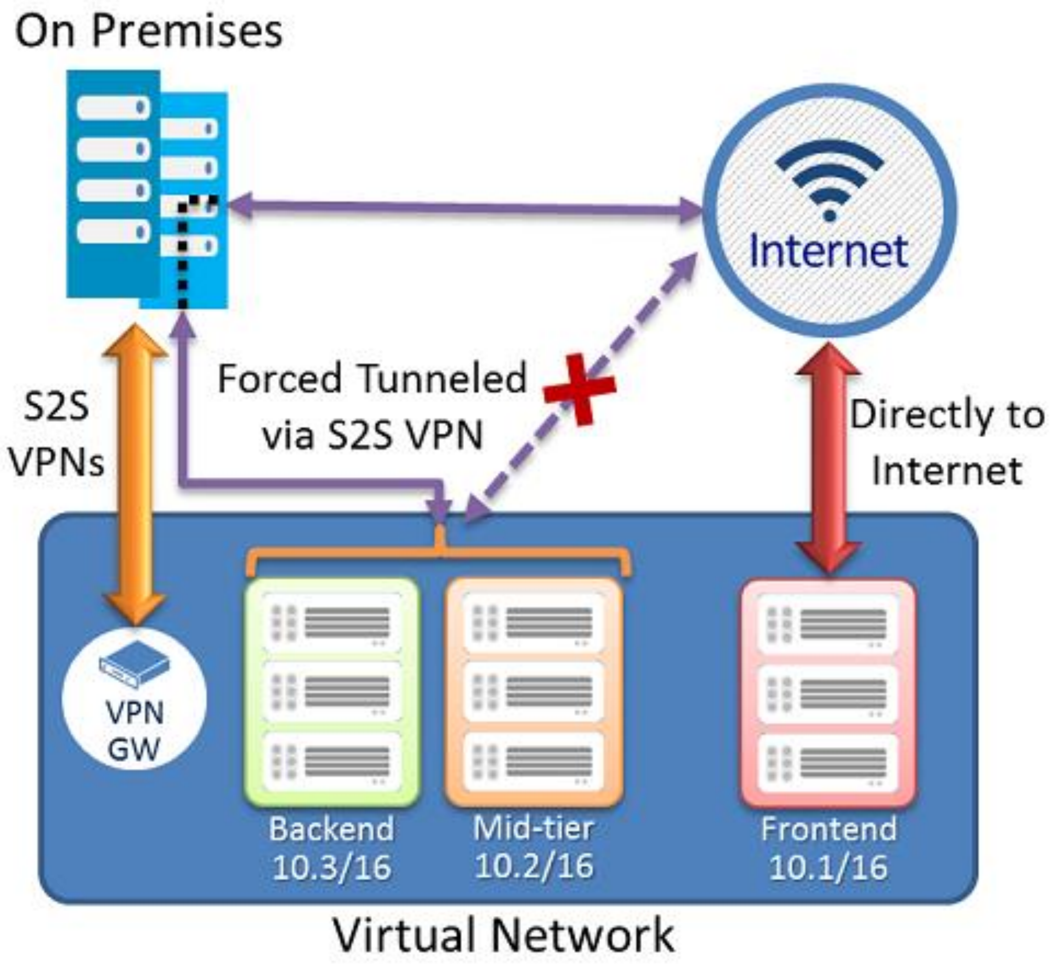
User Defined Routes (UDR)

- Control traffic flow in your network with custom routes
- Attach route tables to subnets
- Specify next hop for any address prefix
- Set 0/0 route to force tunnel all traffic to on-premises or appliance



Forced Tunneling

- Force all traffic from a subnet to a VNet gateway
- Allows scenario for inspection and auditing of traffic
- Can create a routing table to create a default route, then associate routing table to VNet subnets

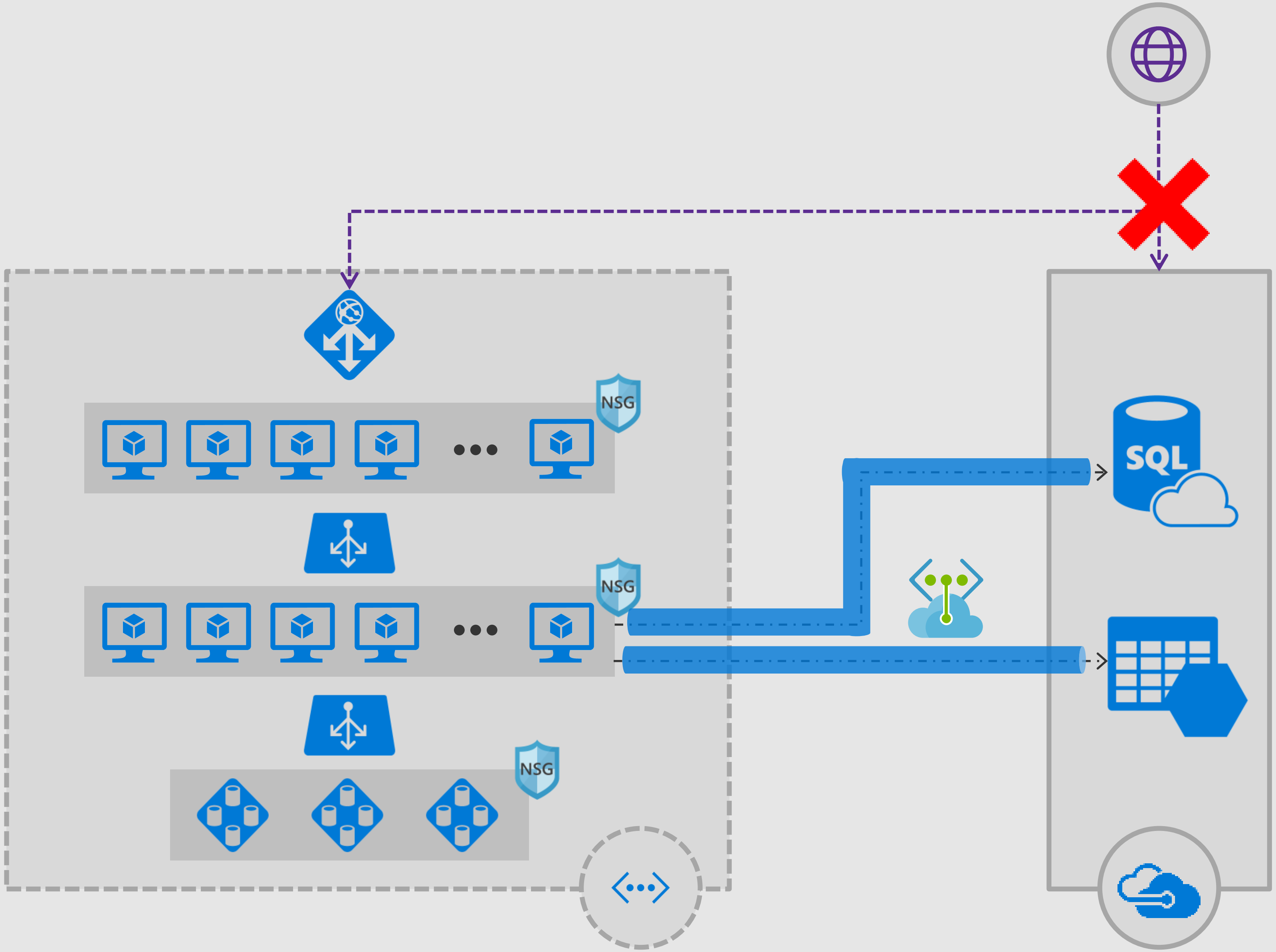


Additional Networking Services / Capabilities / Tools

Microsoft

VNet Service Endpoints

New



Challenges

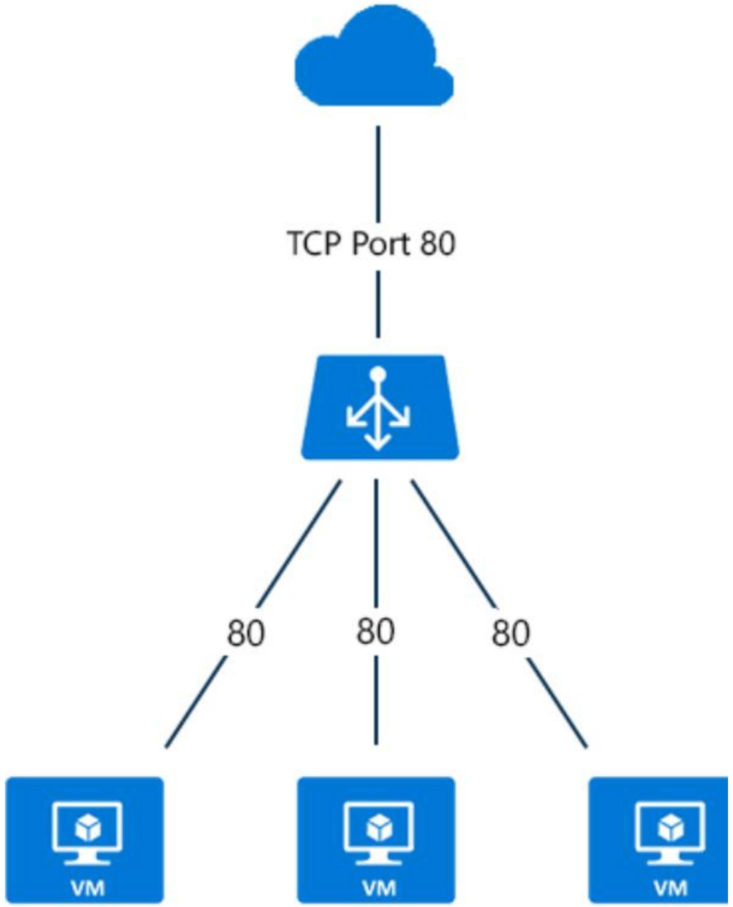
- PaaS services accessible through internet
- Customers may require their services endpoints to be only accessed from their VNets

Solution—VNet Service Endpoints

- PaaS services only accessible from a VNet
- Available now for Storage and SQL DB
- Will roll out to other PaaS services in the future

Azure Public Load Balancer

- Public Load Balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the virtual machine and vice versa for the response traffic from the virtual machine
- Load balancing rules allow you to distribute specific types of traffic between multiple virtual machines or services e.g. you can spread the load of web request traffic across multiple web servers
- By default, Azure Load Balancer distributes network traffic equally among multiple virtual machine instances

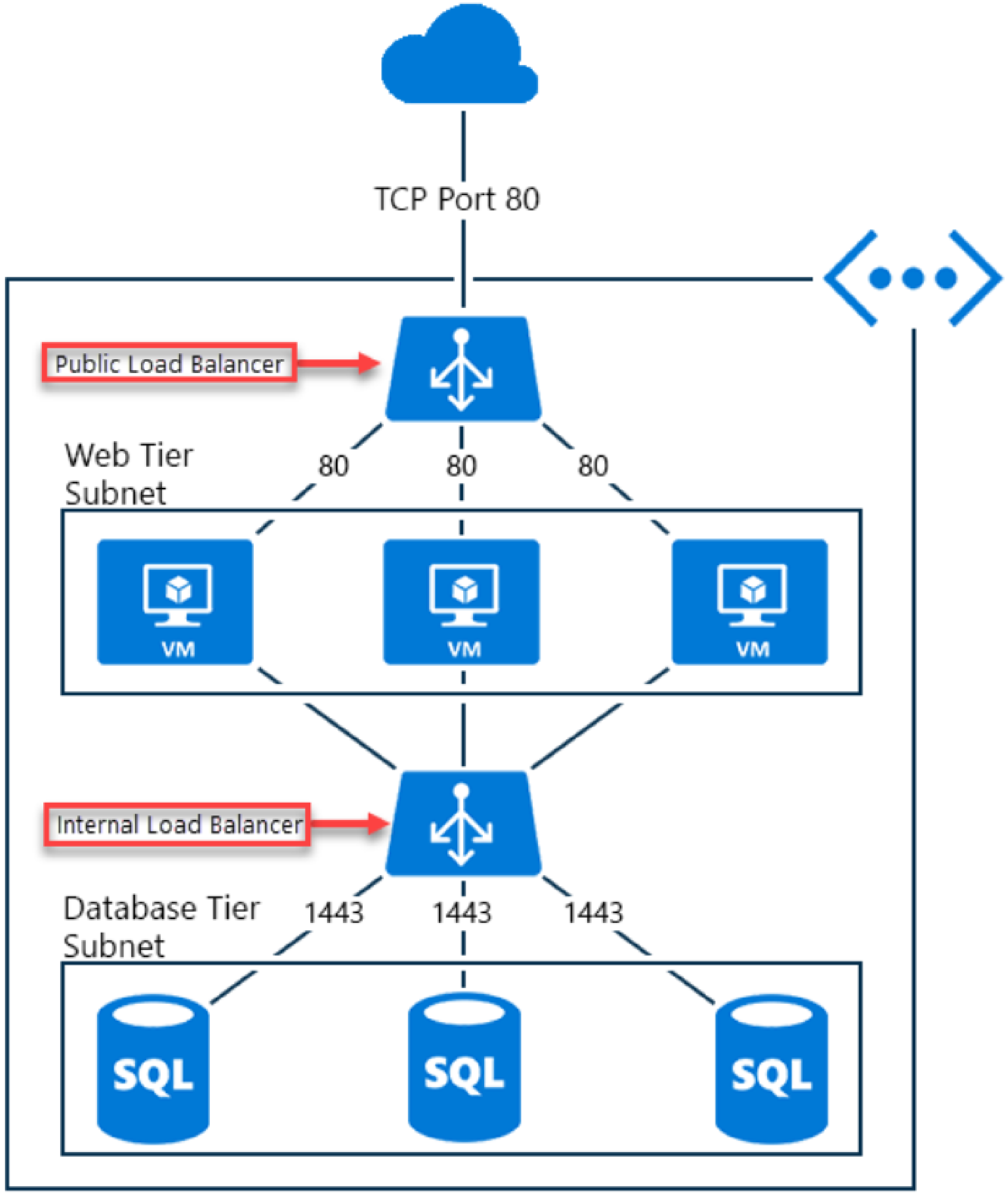


Azure Internal Load Balancer

- Internal Load Balancer only directs traffic to resources that are inside a virtual network or that use a VPN to access Azure infrastructure

- Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint

- Internal line-of-business applications run in Azure and are accessed from within Azure or from on-premises resources



Basic & Standard Load Balancers

	Basic SKU	Standard SKU
Backend Pool Size	Up to 100 instances	Up to 1000 instances
Backend Pool Endpoints	Virtual machines in a single availability set or virtual machine scale set	Any virtual machine in a single virtual network, including blend of virtual machines, availability sets, virtual machine scale sets
Availability Zones	None	Zone-redundant and zonal frontends for inbound and outbound, outbound flows mappings survive zone failure, cross-zone load balancing
Diagnostics	Azure Log Analytics for public Load Balancer only, SNAT exhaustion alert, backend pool health count	Azure Monitor, multi-dimensional metrics including byte and packet counters, health probe status, connection attempts (TCP SYN), outbound connection health (SNAT successful and failed flows), active data plane measurements
HA Ports	None	Internal Load Balancer
Secure by Default	Default open, network security group optional	Default closed for public IP and Load Balancer endpoints and a network security group must be used to explicitly whitelist for traffic to flow

Azure DNS Services

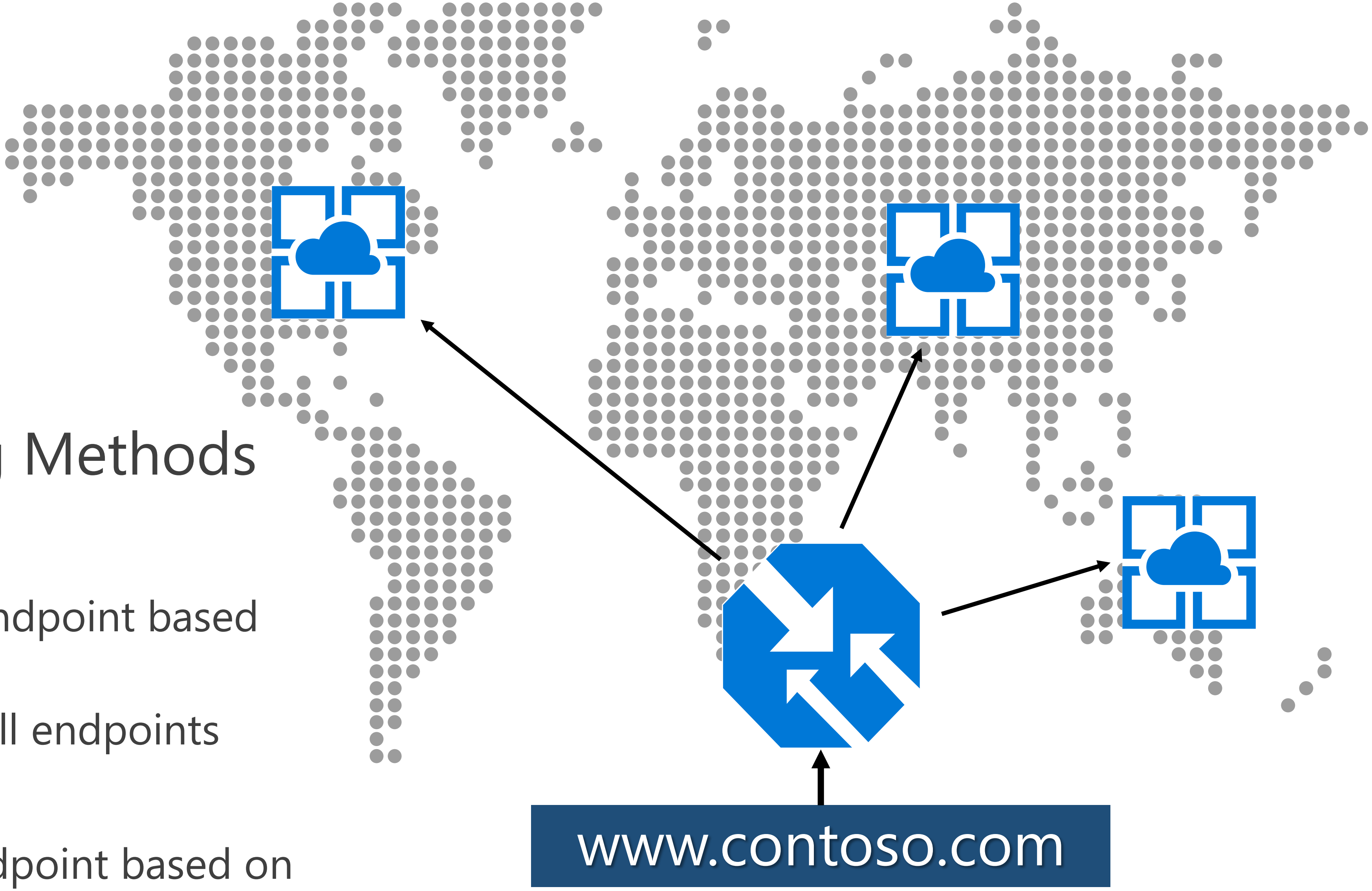
Azure DNS

Host your DNS domains in Azure
Integrate your Web and Domain hosting

Traffic Manager

Globally route user traffic with flexible policies
Enable best-of-class end to end user experience

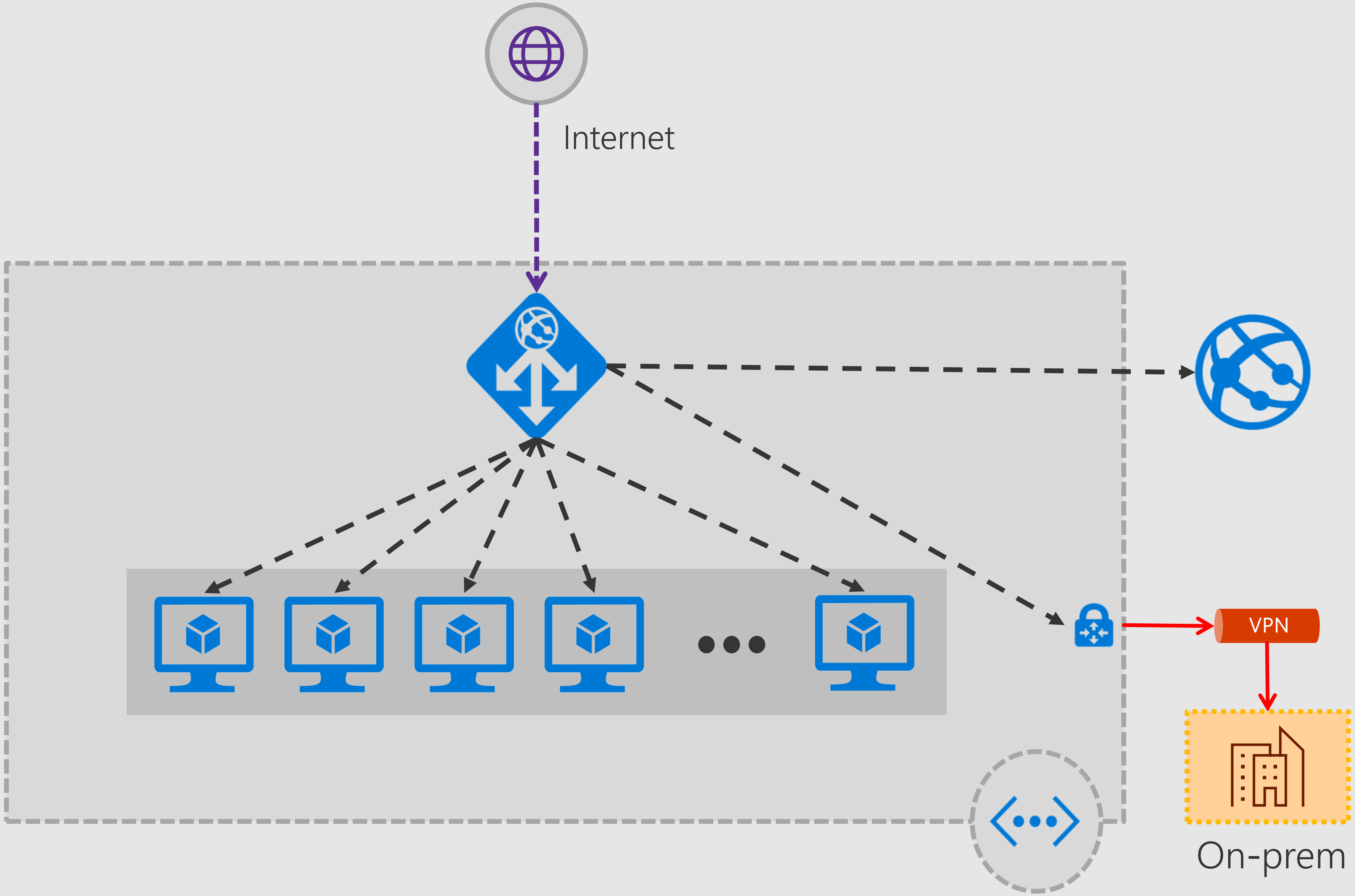
Traffic Manager



Traffic Manager Routing Methods

- **Performance** – The "closest" endpoint based on network latency
- **Weighted** – Distribute across all endpoints
- **Priority** – A single endpoint
- **Geographic** – The "closest" endpoint based on geographic location

Application Gateway and WAF



New

Application Gateway

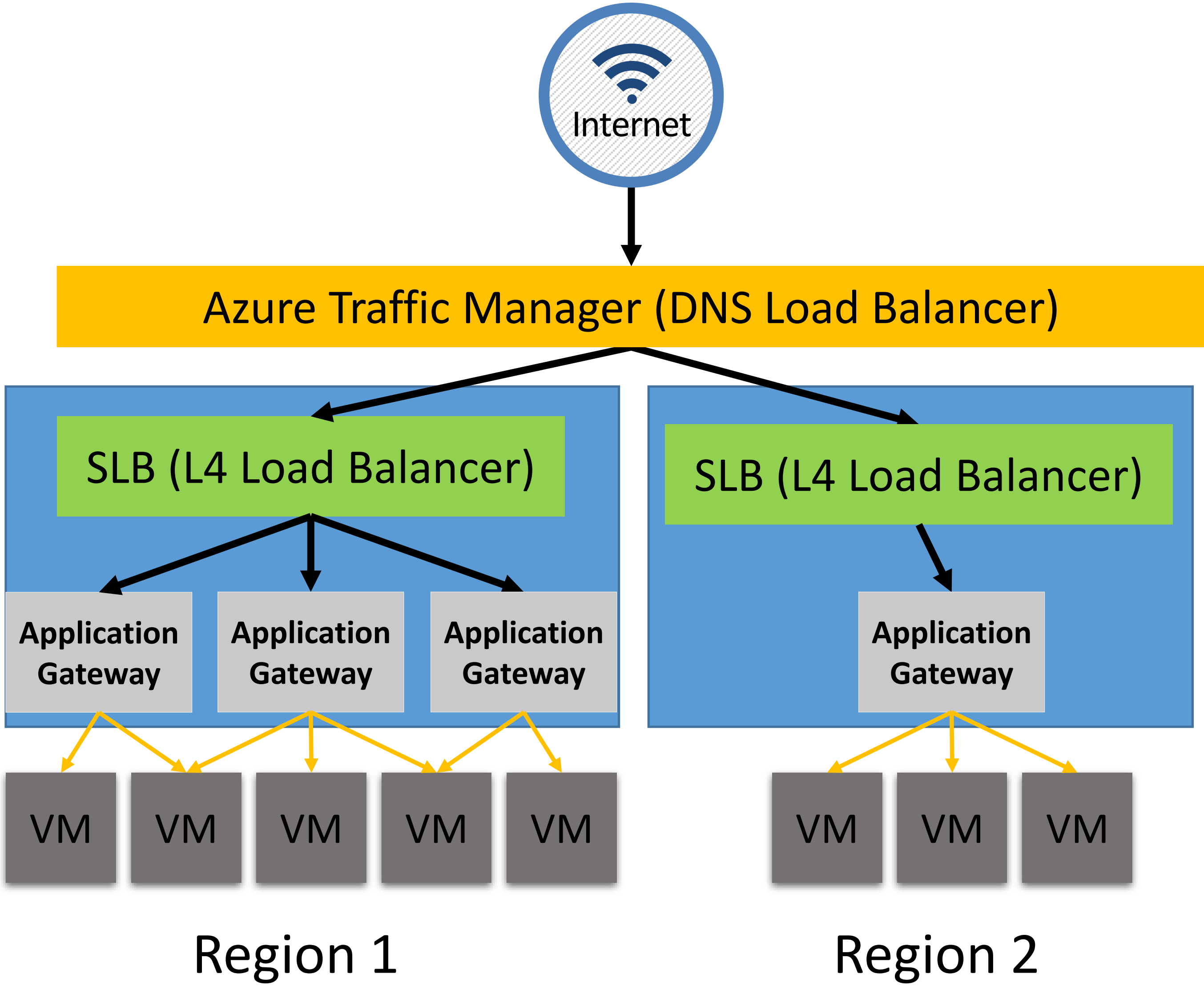
- SSL Policy—control TLS protocol version and cipher suite
- Redirection support at Gateway
- Support multi-tenant backend—Azure Web Apps
- Enhanced probing

WAF

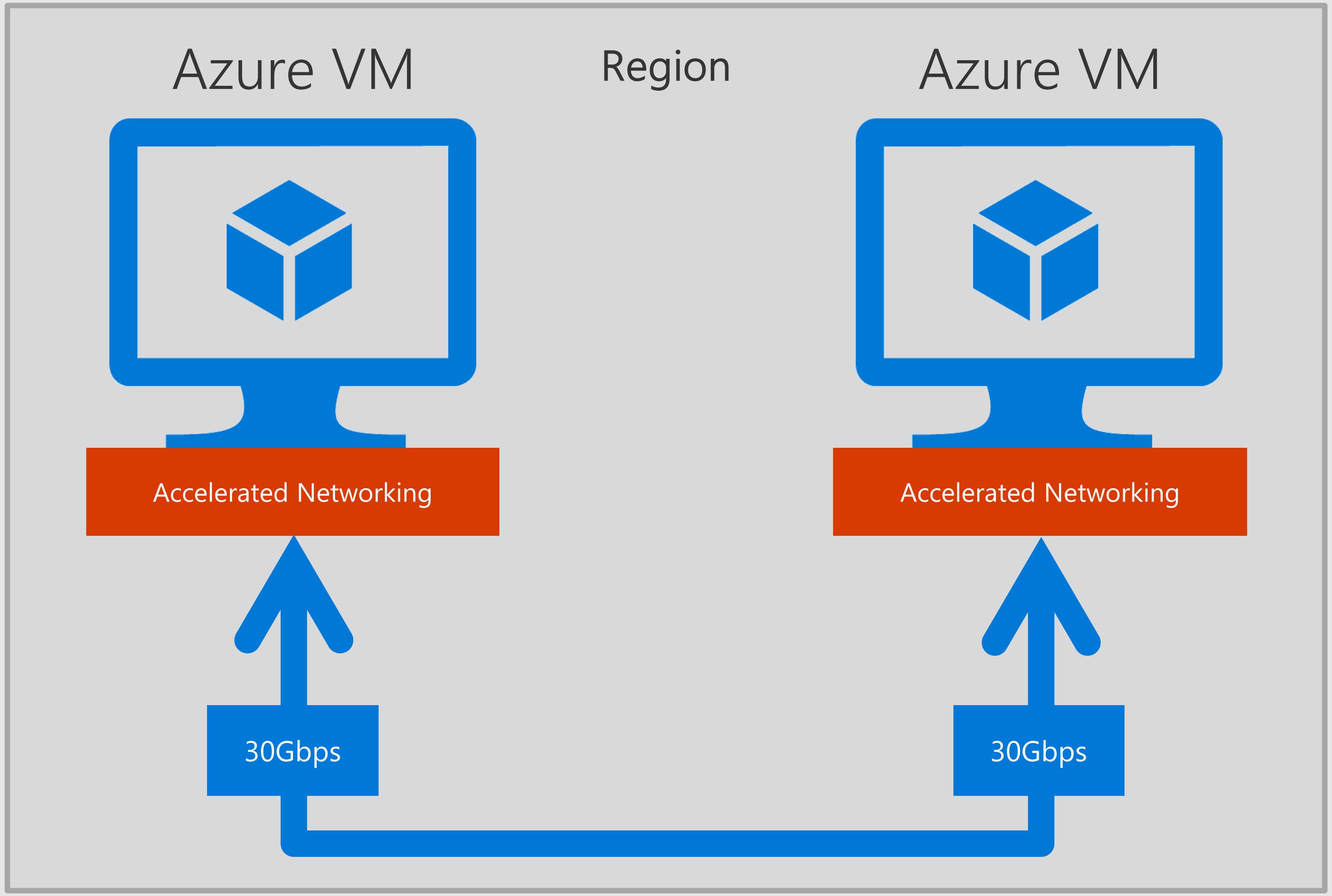
- Support OWASP ModSecurity CRS 3.0
- Enable/Disable Rules or Rule Groups
- WAF logs Integrated with Azure Monitor
- WAF integrated with Azure Security Center

Application Gateway – LB Hierarchy

Azure Service	What	Example
Traffic Manager	Cross-region redirection & availability	http://news.com ➔ apac.news.com ➔ emea.news.com ➔ us.news.com
SLB	In-region scalability & availability	emea.news.com ➔ AppGw1 ➔ AppGw2 ➔ AppGw2
Application Gateway	URL/content-based routing & load balancing	news.com/topnews news.com/sports news.com/images
VMs	Web Servers	



Accelerated Networking



New

30 Gbps

VM to VM bandwidth!

Accelerated Networking

Support expanded to 4 core VMs

No additional cost

New

Network Watcher

Topology

- Visualize your network

Packet Capture

- Initiate packet capture from portal or programmatically
- Captures stored in .cap format

IP Flow Verify

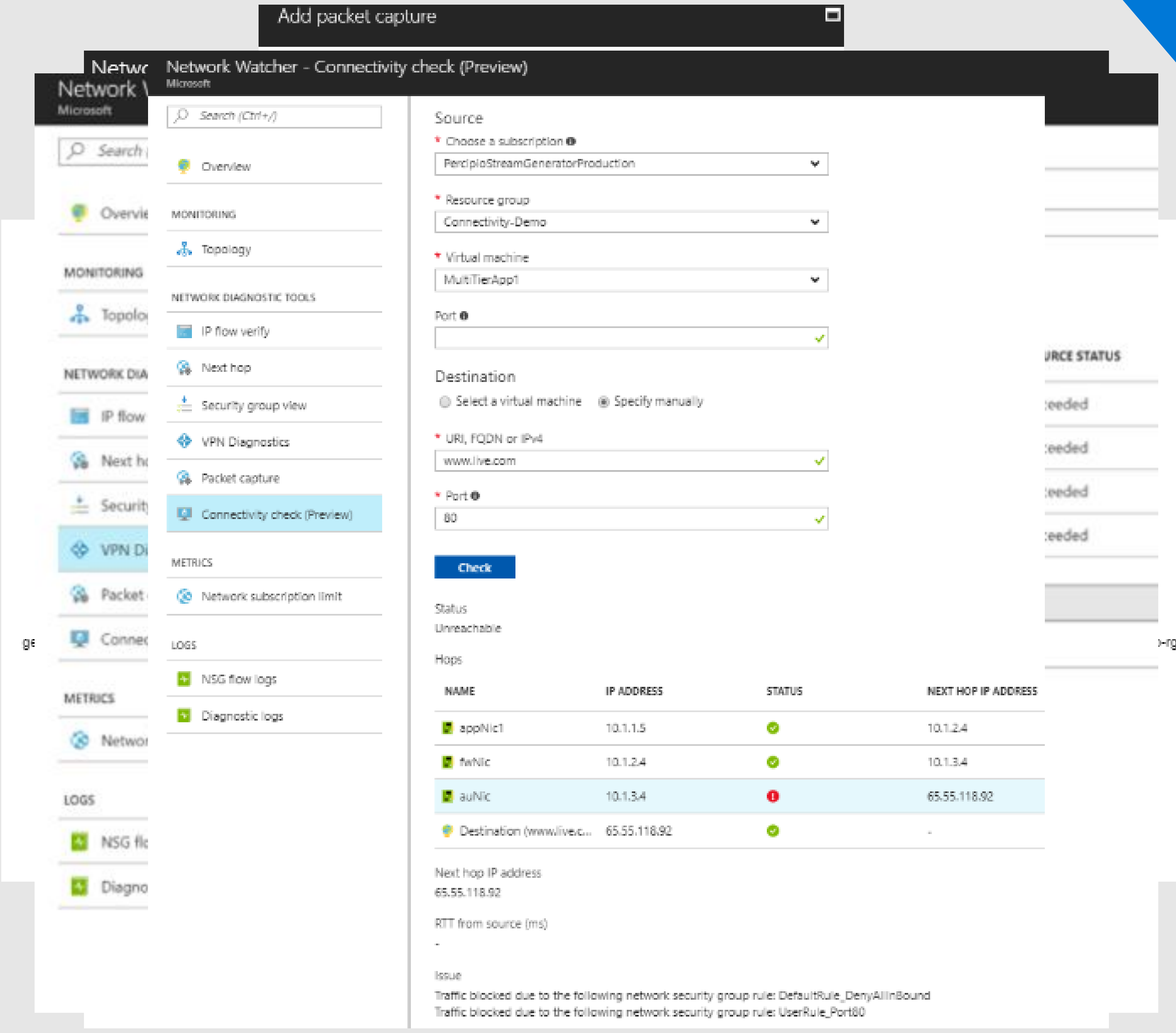
- Identify configured NSG rules blocking traffic

VPN Diagnostics

- Troubleshoot VPN Gateway and Connections and identify issues like
  - Preshared Key mismatch
  - Unsupported IKE policies
  - Gateway Unreachable
  - Gateway instance under maintenance

Connectivity

- Diagnose connectivity and latency issues between VM and an Endpoint (VM, FQDN, URI, IPv4 Address)
- Identify configuration issues impacting connectivity



Source

* Choose a subscription: PercipioStreamGeneratorProduction

* Resource group: Connectivity-Demo

* Virtual machine: MultiTierApp1

Port:

Destination

○ Select a virtual machine ● Specify manually

* URI, FQDN or IPv4: www.live.com

* Port: 80

Status

Unreachable

Hops

NAME	IP ADDRESS	STATUS	NEXT HOP IP ADDRESS
appNic1	10.1.1.5	✓	10.1.2.4
fwNic	10.1.2.4	✓	10.1.3.4
auNic	10.1.3.4	!	65.55.118.92
Destination (www.live.c...	65.55.118.92	✓	-

Next hop IP address

65.55.118.92

RTT from source (ms)

-

Issue

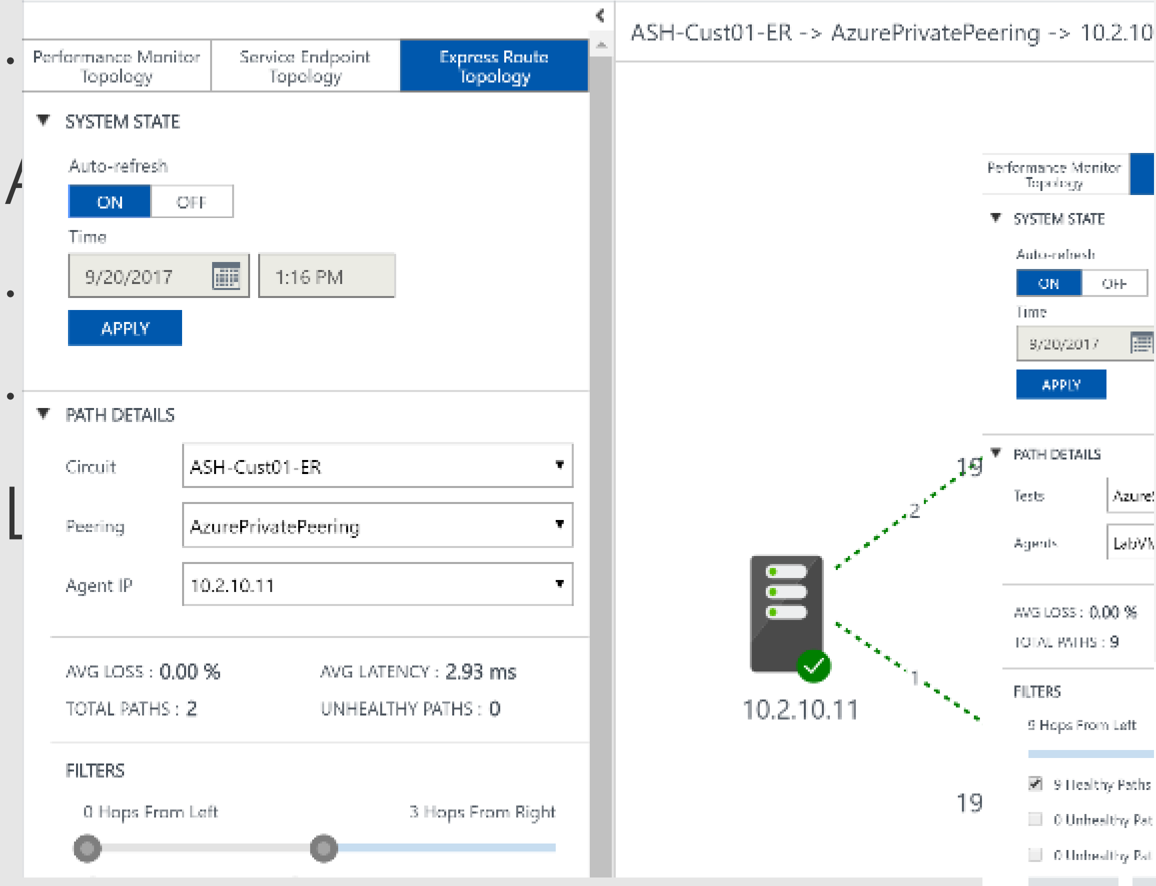
Traffic blocked due to the following network security group rule: DefaultRule_DenyAllInBound
Traffic blocked due to the following network security group rule: UserRule_Port80

Network Performance Monitor for ExpressRoute

New

Continuously monitor

- On-premises to Azure services
- PaaS and SaaS services



Performance Monitor Topology
Service Endpoint Topology
Express Route Topology
ASH-Cust01-ER -> AzurePrivatePeering -> 10.2.10
19
2
1
10.2.10.11
19
Performance Monitor Topology

SYSTEM STATE

Auto-refresh: ON | OFF

Time: 9/20/2017 1:16 PM

APPLY

PATH DETAILS

Circuit: ASH-Cust01-ER

Peering: AzurePrivatePeering

Agent IP: 10.2.10.11

AVG LOSS : 0.00 % AVG LATENCY : 2.93 ms

TOTAL PATHS : 2 UNHEALTHY PATHS : 0

FILTERS

0 Hops From Left 3 Hops From Right

SYSTEM STATE

Auto-refresh: ON | OFF

Time: 9/20/2017

APPLY

PATH DETAILS

Tests: Azure

Agents: LabVM

AVG LOSS : 0.00 %

TOTAL PATHS : 9

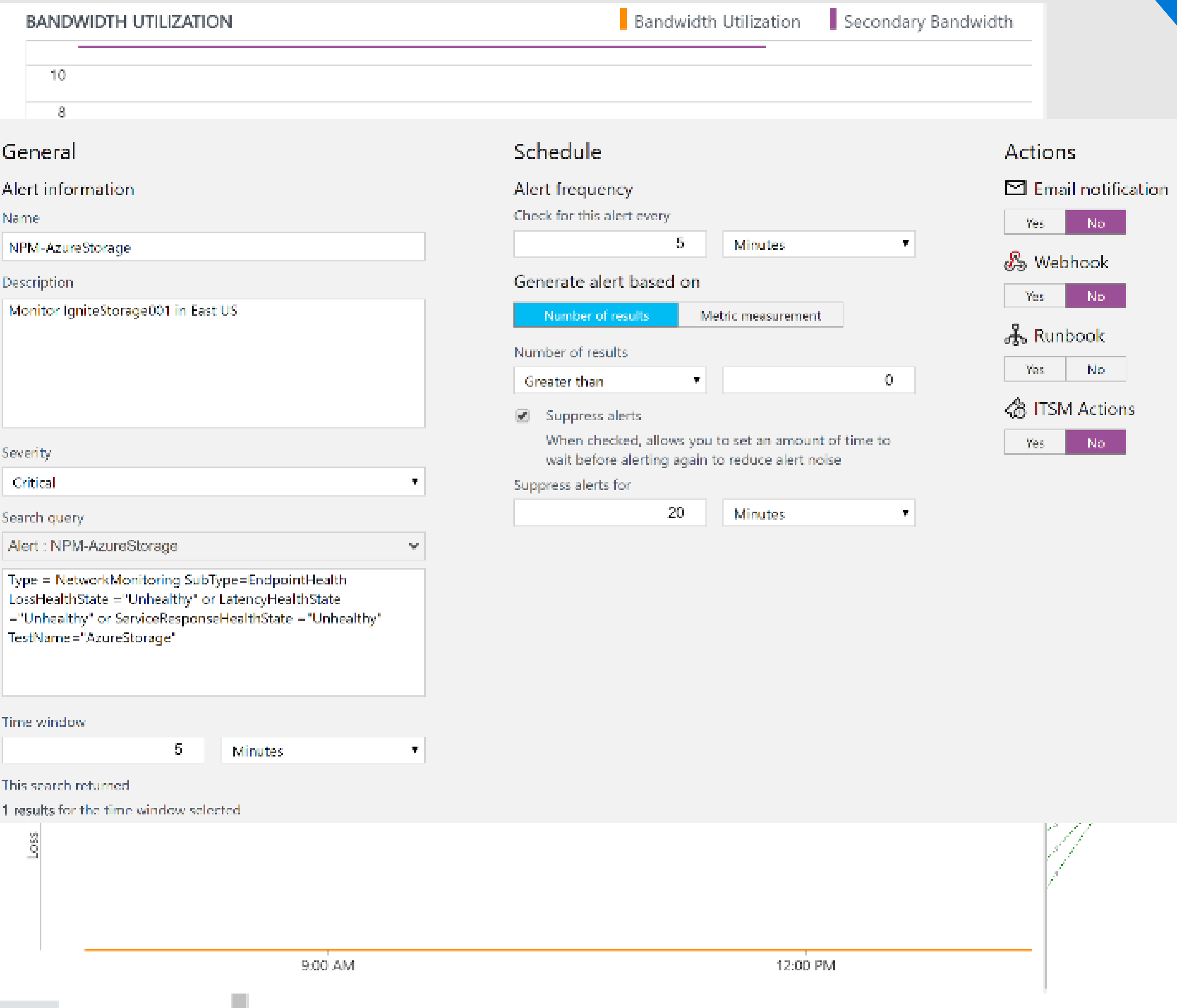
FILTERS

9 Hops From Left

☑ 9 Healthy Paths

□ 0 Unhealthy Pat

□ 0 Unhealthy Pat



General

Alert information

Name: NPM-AzureStorage

Description: Monitor IgniteStorage001 in East US

Severity: Critical

Search query: Alert : NPM-AzureStorage

```
Type = NetworkMonitoring SubType=EndpointHealth
LossHealthState = "Unhealthy" or LatencyHealthState
= "Unhealthy" or ServiceResponseHealthState = "Unhealthy"
TestName="AzureStorage"
```

Time window: 5 Minutes

This search returned

1 results for the time window selected

Schedule

Alert frequency

Check for this alert every: 5 Minutes

Generate alert based on: Number of results | Metric measurement

Number of results: Greater than 0

☑ Suppress alerts

When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Suppress alerts for: 20 Minutes

Actions

Email notification: Yes [✓ No]

Webhook: Yes [✓ No]

Runbook: Yes No

ITSM Actions: Yes [✓ No]

Microsoft

© Copyright Microsoft Corporation. All rights reserved.