

# NETWORKING IN AZURE

# MODULE OVERVIEW

- VIRTUAL NETWORKS
- LOAD BALANCING
- EXTERNAL CONNECTIVITY
- SECURE CONNECTIVITY
- OTHER SERVICES
  - Azure firewall
  - Monitoring (network watcher, Log analytics)

# VIRTUAL NETWORKS

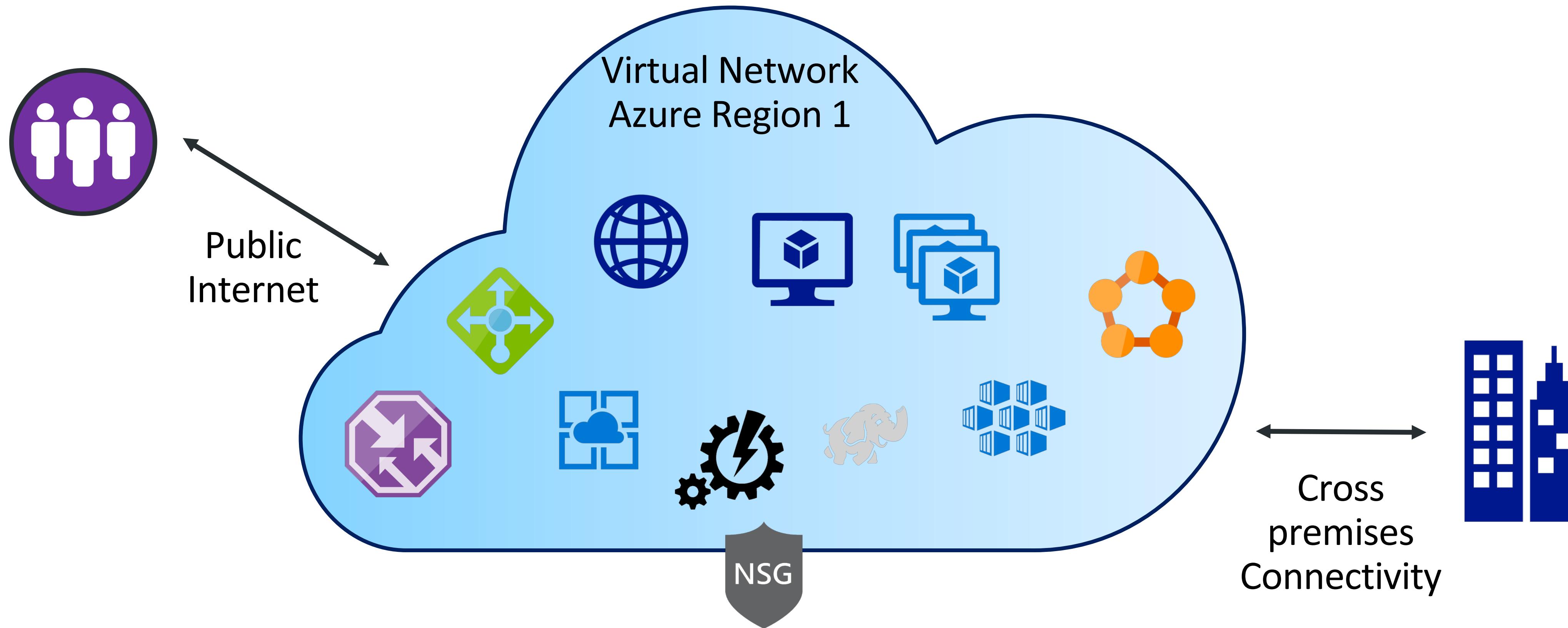
# VIRTUAL NETWORKS

- AZURE VIRTUAL NETWORK (VNET) ARCHITECTURE
- MULTI-REGION VIRTUAL NETWORK ARCHITECTURE
- BASIC CONCEPTS (VNETS, SUBNETS, NICs, PUBLIC IP'S, NSG, ASG)

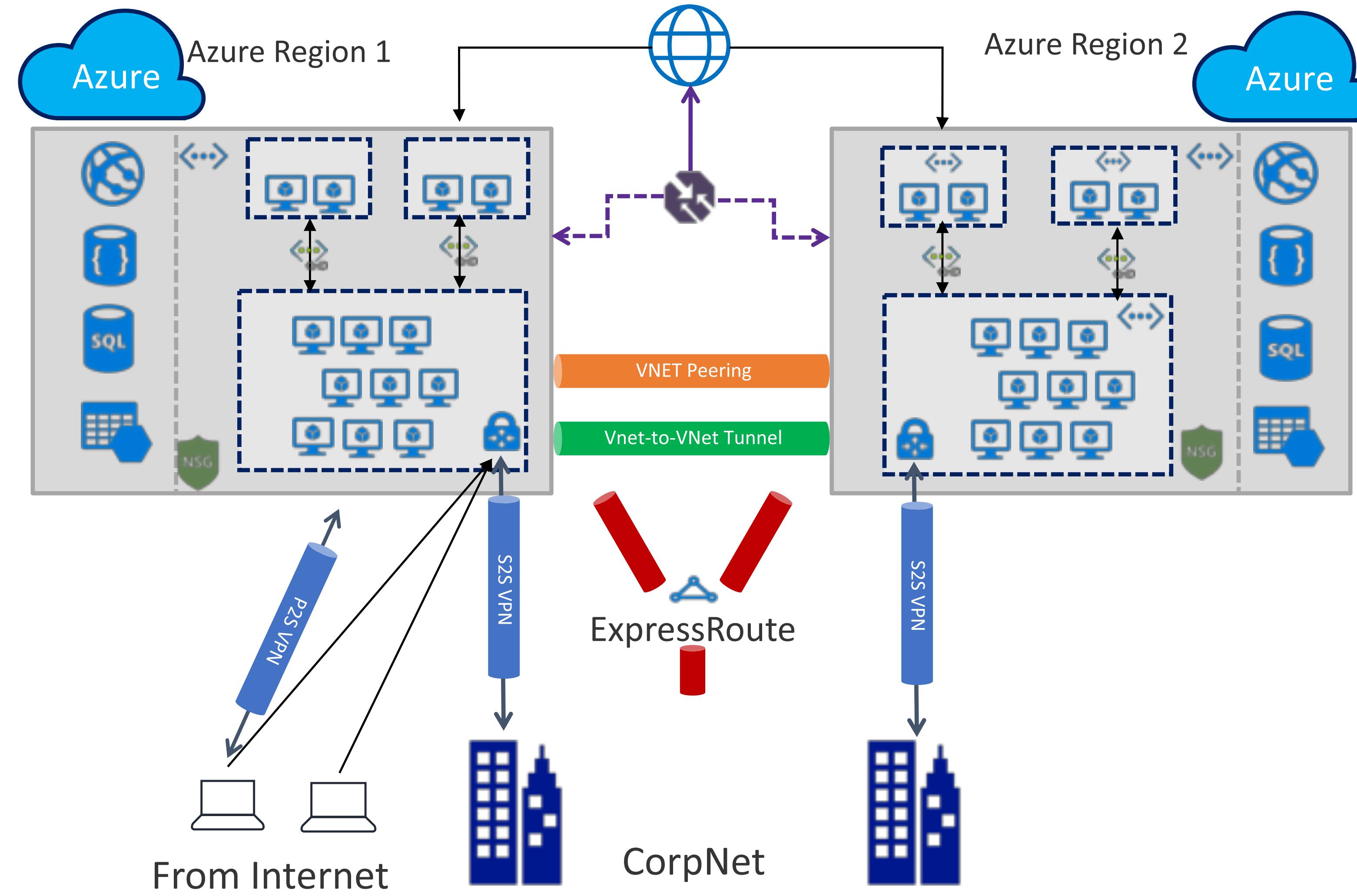
# AZURE NETWORKING BASICS

- VNET, SUBNET, DNS, 168.63.129.16, \*.INTERNAL.CLOUDAPP.NET
- NSG, ASG, SERVICE ENDPOINTS, UDR
- PEERING
- PIP
- LOAD BALANCER, APP GATEWAY / WAF
- NGFW / NVA / APPLIANCE
- **SERVICES:** NETWORK WATCHER, LOG ANALYTICS, SECURITY CENTER

# AZURE VIRTUAL NETWORK (VNET) ARCHITECTURE

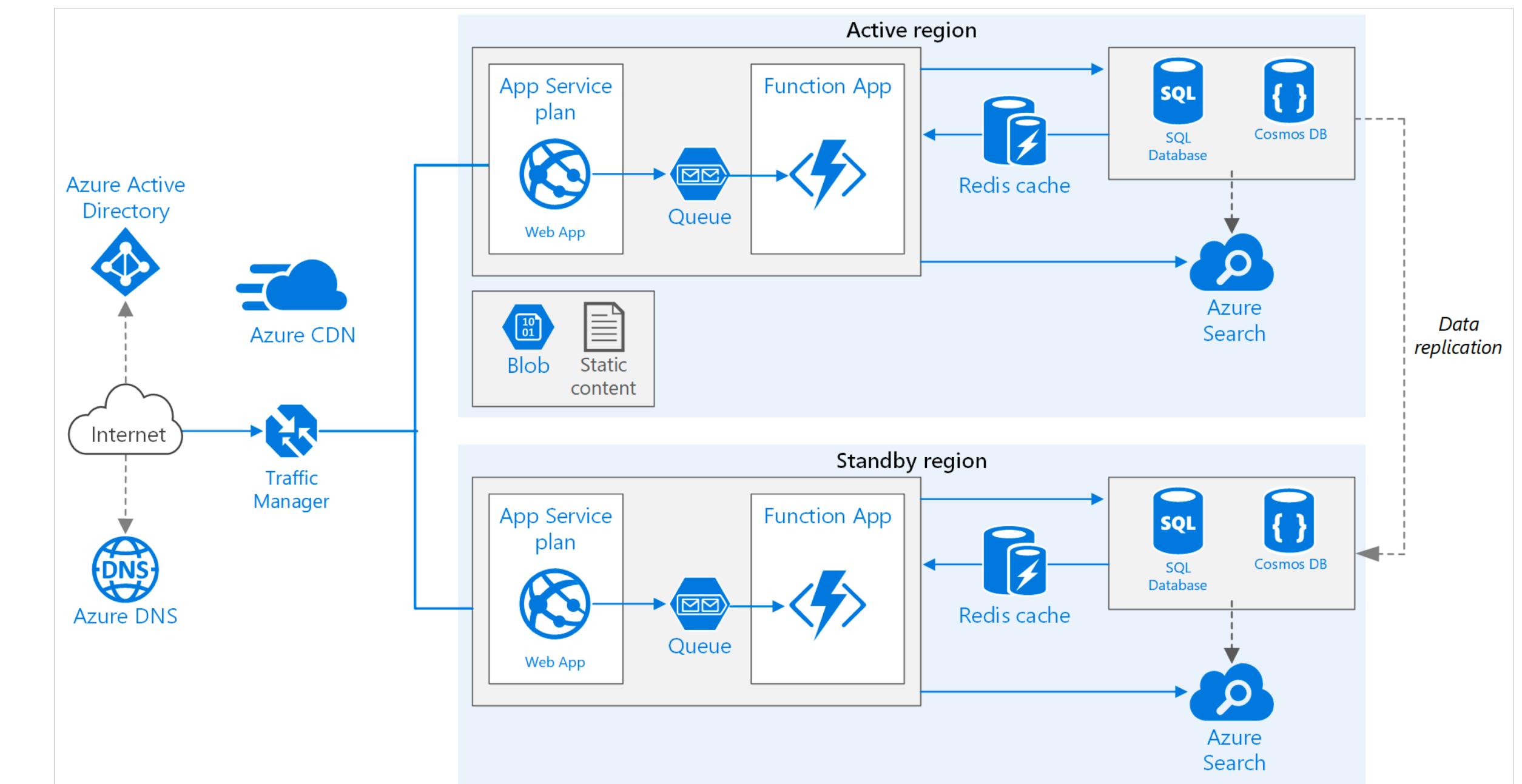


# MULTI-REGION VIRTUAL NETWORK ARCHITECTURE



# MULTI-REGION VIRTUAL NETWORK ARCHITECTURE

- TRAFFIC MANAGER PROVIDES DNS BASED TRAFFIC DISTRIBUTION & FAILOVER ACROSS AZURE REGIONS
- IAAS & PAAS VNET INTER-COMMUNICATION USING SERVICE ENDPOINTS
- ISOLATE VM WORKLOADS IN SUBNETS/VNET
- EXPRESS ROUTE AND/OR S2S VPN FOR CORPNET CONNECTIVITY OR AZURE TO AZURE REGION TRAFFIC
- NSGS/ASGS SECURE THE IN/OUTGOING TRAFFIC ON VNET OR NIC LEVEL



# VNETS & SUBNETS

- DEFINE 1 OR MORE VNETS WITHIN AN AZURE REGION, AND CONFIGURE AN ADDRESS SPACE FOR EACH (MANY RANGES AVAILABLE)
- DEFINE 1 OR MORE SUBNETS WITHIN A VNET, AND CONFIGURE ADDRESS SPACE WITHIN THE VNET RANGE
- VNETS AND SUBNETS ARE USING CIDR NOTATION (X.X.X.X/24, X.X.X.X/16,...) AND CAN USE ALL PRIVATE ADDRESS SPACE
- CONFIGURE NETWORK SECURITY GROUP SETTINGS ON SUBNET LEVEL OR NIC LEVEL
- ATTACH A NIC TO A SUBNET

## SUBNET IP ADDRESSING:

- IP-ADDRESS GETS ALLOCATED TO A NIC DURING PROVISIONING OF THE NIC
- FIRST AVAILABLE IP-ADDRESS IN A SUBNET RANGE IS X.X.X.4 (5 ADDRESS TAKEN BY AZURE)
- AZURE SUBNETS SUPPORT DYNAMIC (=DEFAULT) AND STATIC IP ADDRESSING, PUBLIC IP'S CAN USE IPV6

# PUBLIC & PRIVATE IP-ADDRESSING

## PUBLIC IP-ADDRESSING:

- USED FOR ALL PUBLIC INTERNET-FACING COMMUNICATION
- PRIVATE IP-ADDRESSING:
- USED FOR ALL INTER-VNET COMMUNICATION
- USED FOR ALL COMMUNICATION BETWEEN AN AZURE VNET AND AN ON-PREMISES VNET

The screenshot shows two Azure resource pages. The top page is for a virtual machine named 'vmub1604dev01'. It displays basic details like computer name, operating system, size, and a red box highlights the 'Public IP address' (40.127.192.236) and 'DNS name' (mifurmub01.northeurope.cloudapp.azure.com). The bottom page is for a virtual network named 'vnet01-mng'. It shows the 'Address space' (10.0.0.0/16) and a red box highlights the 'DNS servers' (Azure provided DNS service). Both pages also show connected devices and their network interface details.

**Virtual Machine Details:**

- Computer name: vmub1604dev01
- Operating system: Linux
- Size: Standard A0 (1 vcpus, 0.75 GB memory)
- Public IP address: 40.127.192.236
- DNS name: mifurmub01.northeurope.cloudapp.azure.com

**Virtual Network Details:**

- Address space: 10.0.0.0/16
- DNS servers: Azure provided DNS service

DEVICE	TYPE	IP ADDRESS	SUBNET
vmwin2k16r2dev01NIC01	Network interface	10.0.1.4	backend-subnet
vmub1804dev01NIC01	Network interface	10.0.1.5	backend-subnet
vmwin2k8r2dev01NIC01	Network interface	10.0.1.6	backend-subnet
vmwin2k16dev01NIC01	Network interface	10.0.1.7	backend-subnet
vmub1604dev01NIC01	Network interface	10.0.0.4	wfe-subnet

# AZURE DNS RESOLVING

- DNS SERVER SETTINGS ARE CONFIGURED ON VNET/NIC

LEVEL

- USE AZURE DNS (DEFAULT) OR USE YOUR CUSTOM DNS

CONFIGURATION:

- AZURE DNS APPLIANCE (FROM AZURE MARKETPLACE)

- AZURE VM (E.G. WINDOWS ADDS WITH DNS)

- ON-PREMISES DNS SOLUTION (REQUIRES

CONNECTIVITY)

- PUBLIC DNS NAMES (AVAILABLE FOR VMS AND APP

SERVICES) MUST BE UNIQUE ACROSS AZURE REGIONS:

<HOST.REGION.CLOUDAPP.AZURE.COM>

```
mifurm@vmub1604dev01:~$ nslookup www.wp.pl
Server:          168.63.129.16
Address:         168.63.129.16#53
```

```
Non-authoritative answer:
Name:   www.wp.pl
Address: 212.77.98.9
```

```
mifurm@vmub1804dev01:~$ curl -H Metadata:true "http://169.254.169.254/metadata/instance?api-version=2017-08-01"
{"compute":{"location":"northeurope","name":"vmub1804dev01","offer":"UbuntuServer","osType":"Linux","placementGroupId":"","platformFaultDomain":"0","platformUpdateDomain":"0","publisher":"Canonical","resourceGroupName":"mntworkshop2-rg","sku":"16.04-LTS","subscriptionId":"c0eace6b-deca-4861-8042-b4e807cef056","tags":"","version":"16.04.201811010","vmId":"ab56ef17-6376-4a99-830e-2a421da03dd3","vmSize":"Standard_A0"},"network": {"interface": [{"ipv4": {"privateIpAddress": "10.0.1.5", "publicIpAddress": ""}}, {"subnet": [{"address": "10.0.1.0", "prefix": "24"}]}, {"ipv6": {"ipAddress": [], "macAddress": "000D3ABA8DA7"}]}]}
mifurm@vmub1804dev01:~$ curl -H Metacurl 'https://api.ipify.org?format=json'
{"ip": "168.63.77.6"}mifurm@vmub1804dev01:~$
```

# VIRTUAL NETWORKS SUMMARY

- AZURE VIRTUAL NETWORK (VNET) ARCHITECTURE
- MULTI-REGION VIRTUAL NETWORK ARCHITECTURE
- BASIC CONCEPTS (VNETS, SUBNETS, NICs, PUBLIC IP'S, NSG, ASG)

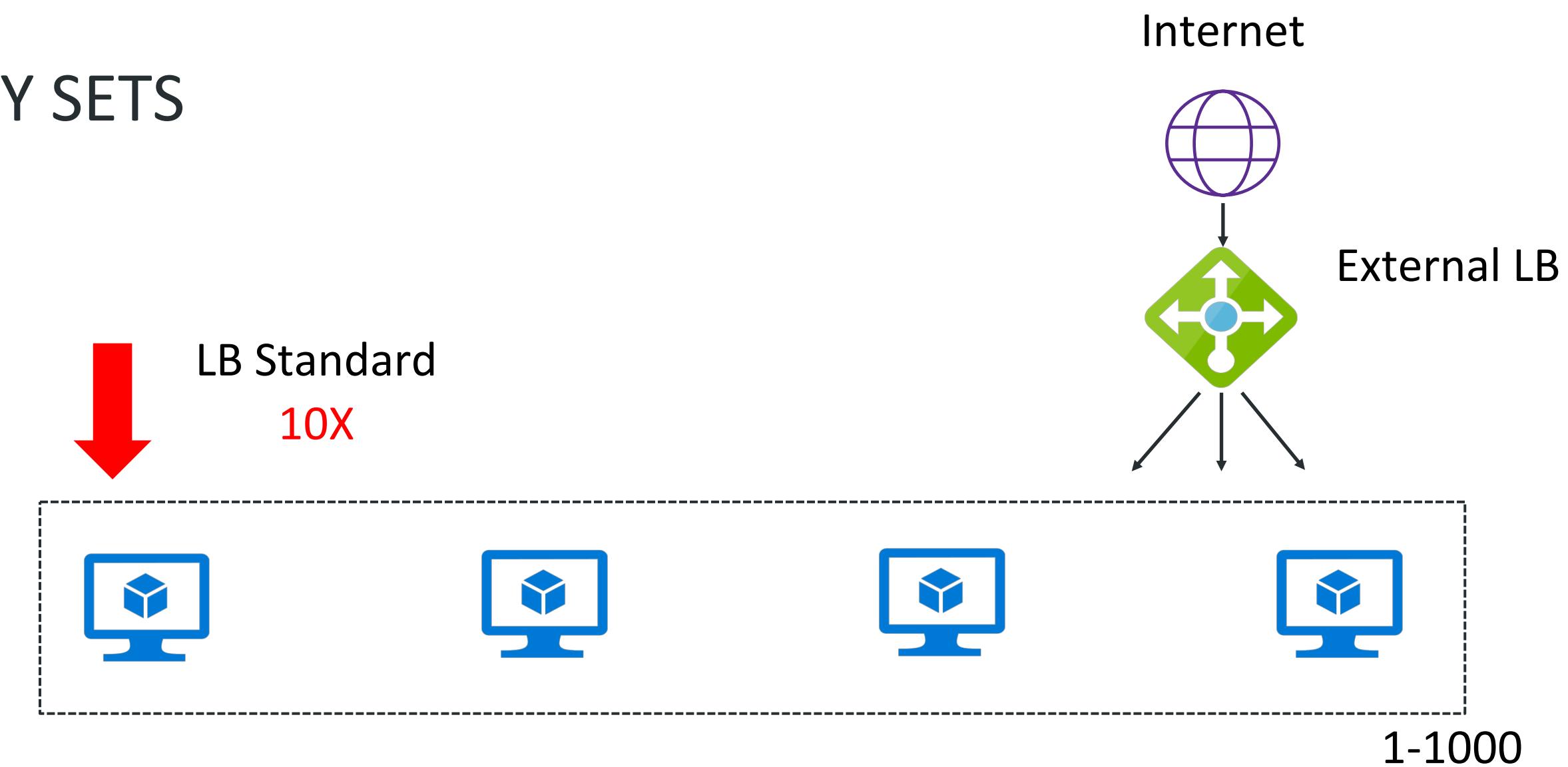
# LOAD BALANCING

# LOAD BALANCING SOLUTIONS

- AZURE LOAD BALANCER (LAYER 4)
- AZURE APPLICATION GATEWAY (LAYER 7)
- AZURE MARKETPLACE LOAD BALANCING APPLIANCE (LAYER 7)
- AZURE TRAFFIC MANAGER (DNS-BASED)

# AZURE LOAD BALANCER – BASIC SKU

- LOAD BALANCER WITH A PUBLIC IP-ADDRESS, SENDING TRAFFIC ALONG TO THE BACK-END POOL SERVERS
- TCP, UDP TRAFFIC
- AZURE PLATFORM MANAGEMENT
- SUPPORT FOR AVAILABILITY SETS



# AZURE LOAD BALANCER – BASIC SKU

- LOAD BALANCER CAN BE USED IN MANY SCENARIOS
- DON'T REQUIRE MANAGEMENT OR DEEP CONFIGURATION
- CAN BE USED BY CLUSTERS IN AZURE (WFC OR ALWAYS ON)
- AZURE DOES NOT SUPPORT NLB (USES MULTICAST)



## Basic

Up to 100 backend instances

Non-zonal frontend

Availability Set (single)

Basic NAT and Probe health status

-

NSG optional

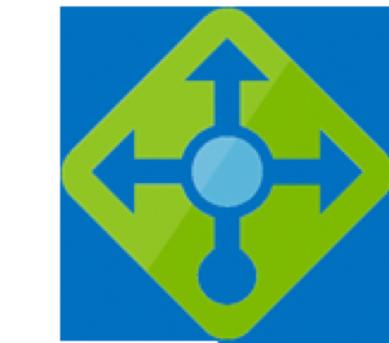
Free

# AZURE LOAD BALANCER – STANDARD SKU

YOU CAN USE LOAD BALANCER STANDARD FOR TCP & UDP

## SCENARIOS WITH:

- LARGER SCALE
- GREATER FLEXIBILITY
- HA PORTS
- NEW METRICS
- AVAILABILITY ZONES



### Standard

Up to 1000 backend instances

Zone-redundant frontend  
Zonal frontend

Availability Sets not required  
and Availability Zones

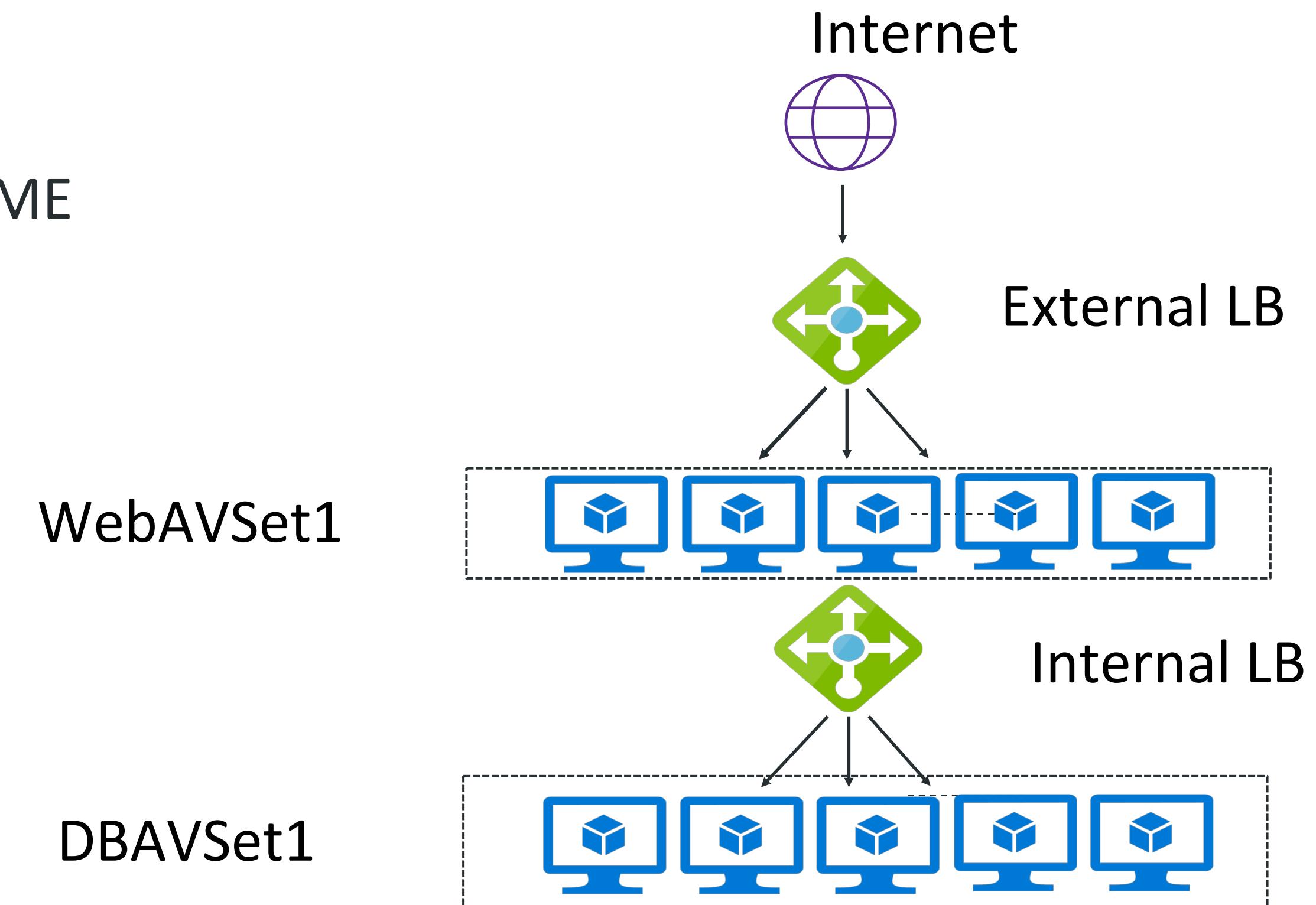
Integrated Frontend and  
Backend health metrics

Supports HA Ports

NSG required

# INTERNAL LOAD BALANCER

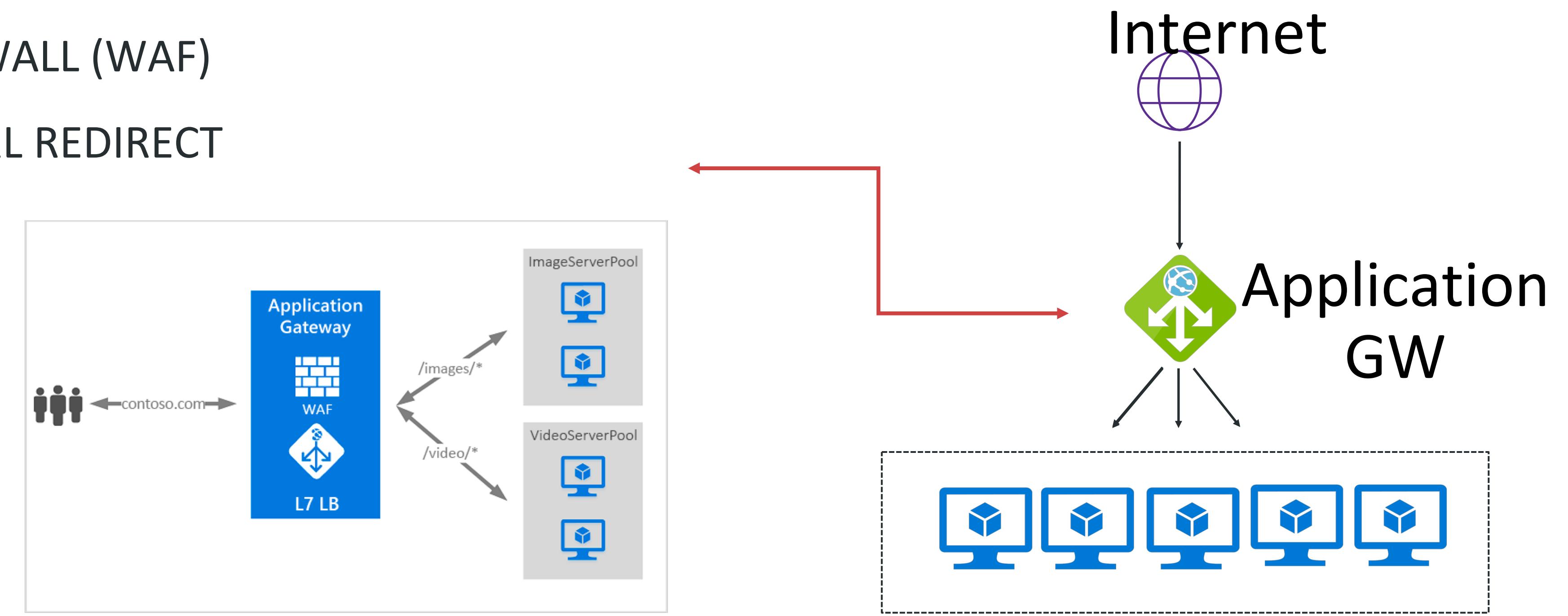
- LOAD BALANCER WITH A PRIVATE IP-ADDRESS, SENDING TRAFFIC ALONG TO THE BACK-END POOL SERVERS
- TCP, UDP TRAFFIC
- CANNOT BE PUBLIC / PRIVATE AT THE SAME TIME



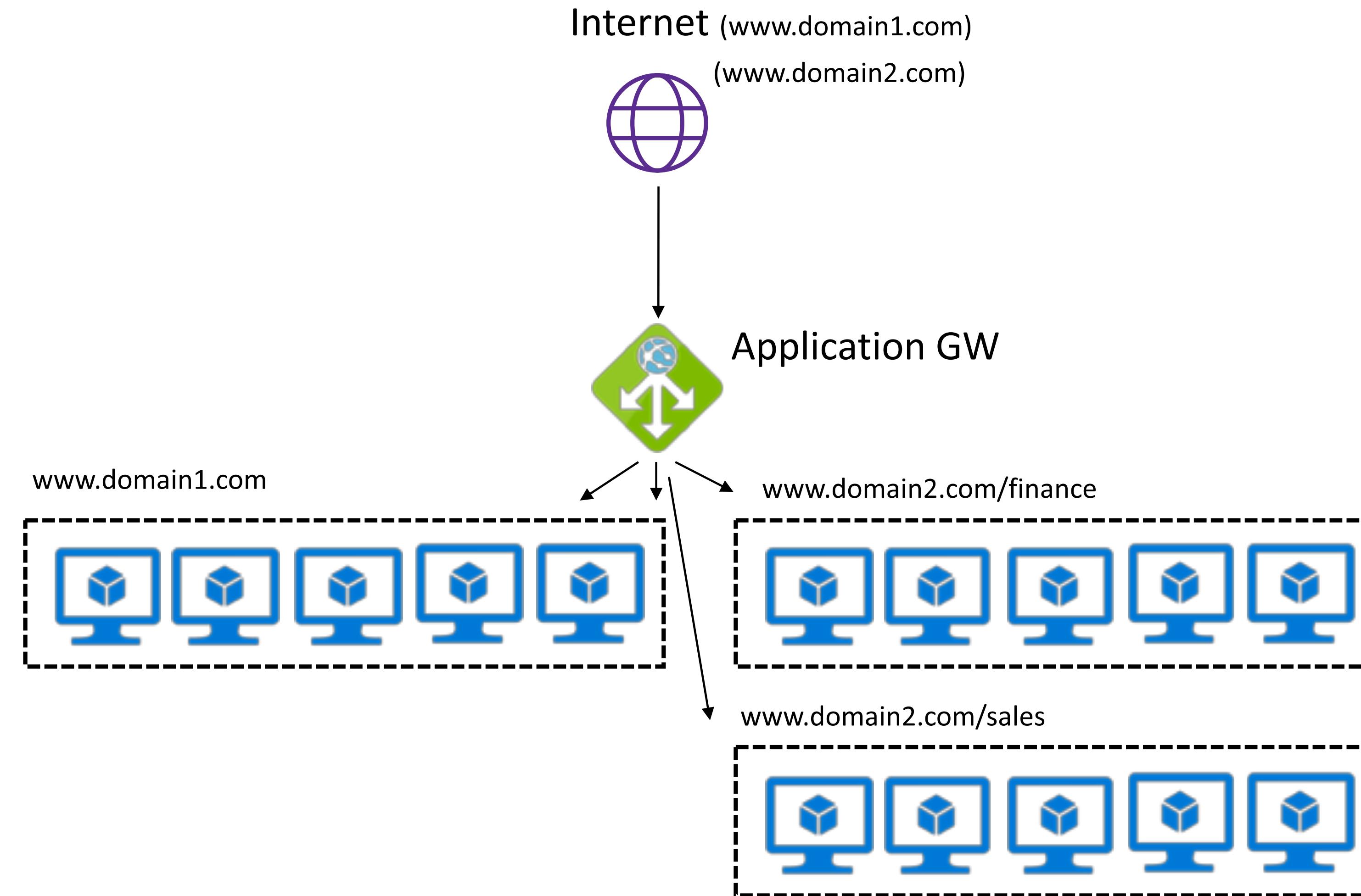
# AZURE APPLICATION GATEWAY

LOAD BALANCER WITH A PUBLIC IP-ADDRESS, SENDING TRAFFIC ALONG TO THE BACK-END POOL SERVERS

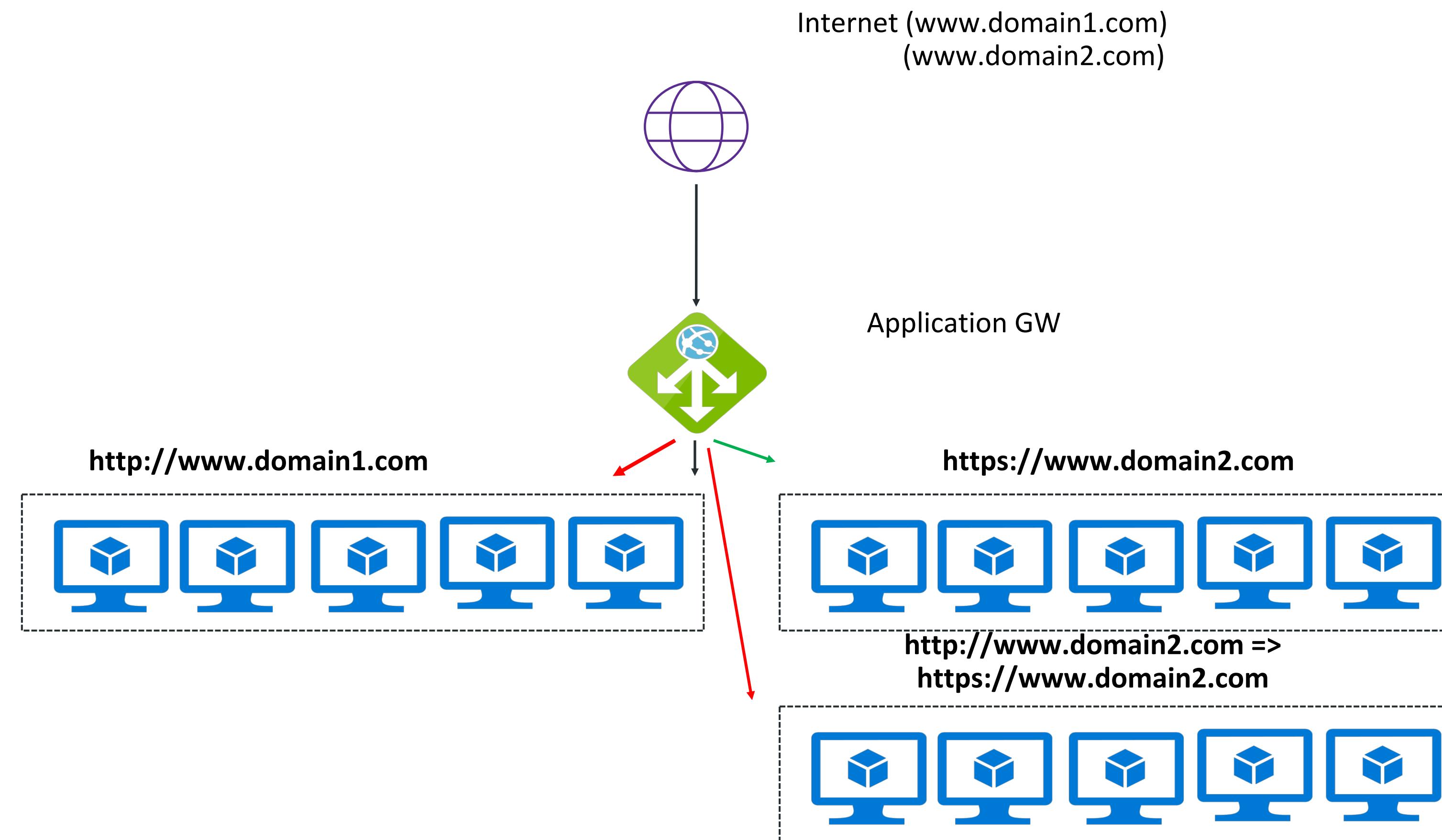
- HTTP/HTTPS ONLY
- SSL OFFLOADING & END2END SSL POSSIBLE
- COOKIE AFFINITY
- WEB APPLICATION FIREWALL (WAF)
- URL BASED ROUTING, URL REDIRECT
- HTTP HEADER ANALYZE



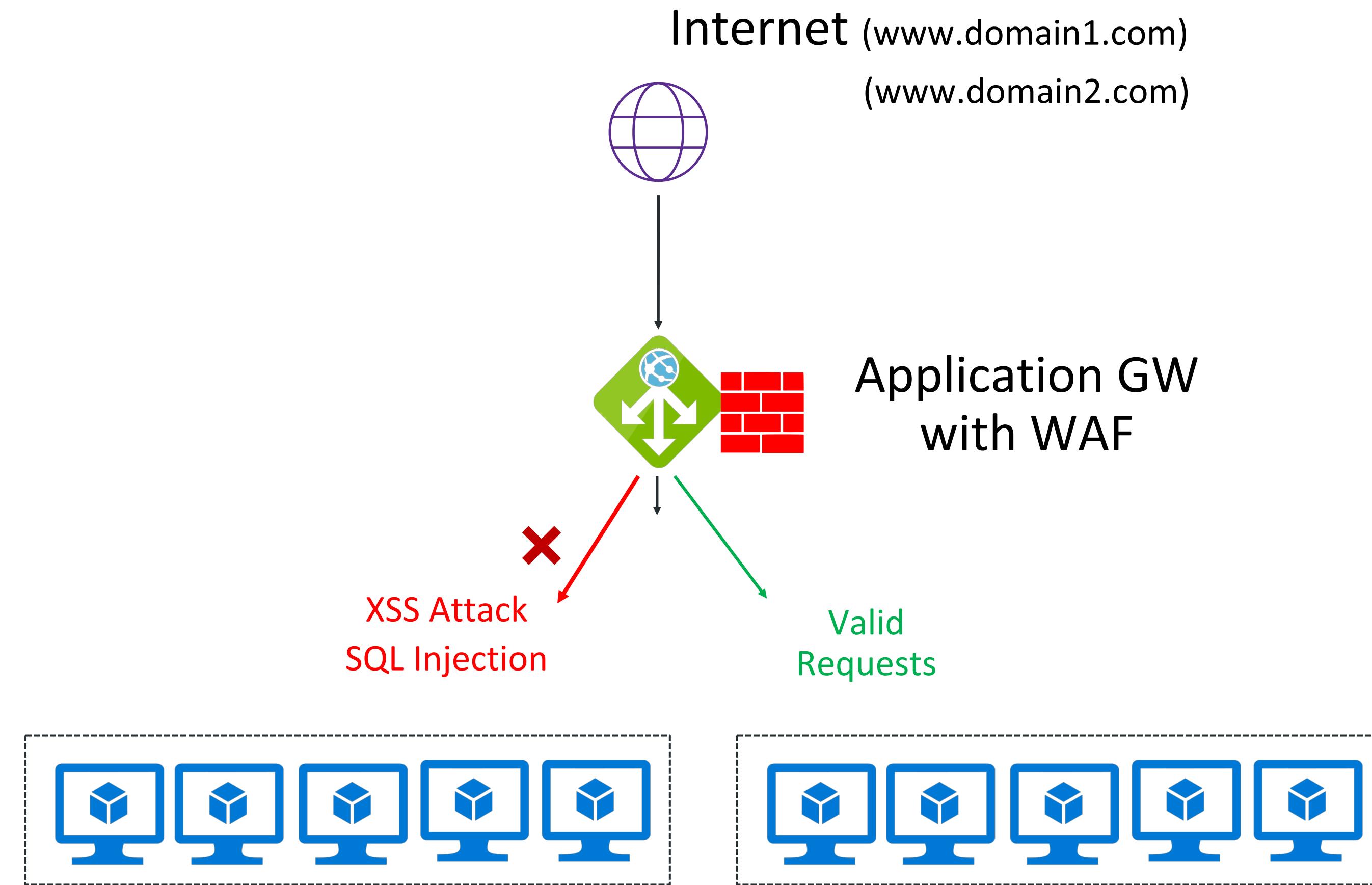
# AZURE APPLICATION GATEWAY



# AZURE APPLICATION GATEWAY – SSL TERMINATION



# AZURE APPLICATION GATEWAY – WAF



# AZURE APPLICATION GATEWAY – PRECONFIGURED WAF RULES (OWSPA 3.0 / 2.0 )

The screenshot shows the Azure Application Gateway configuration interface. On the left, a sidebar lists various settings like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Web application firewall (selected), Backend pools, HTTP settings, Frontend IP configurations, Listeners, Rules (selected), Health probes, Properties, Locks, and Automation script. Below these are sections for Monitoring and Metrics. The main pane displays the configuration for the selected Web application firewall. It includes fields for Firewall status (Enabled), Firewall mode (Prevention), Rule set (OWASP 3.0), and Advanced rule configuration (checked). A search bar labeled "Search rules" is present. A table lists 15 pre-configured rules, each with an enable checkbox and a description:

ENAB...	NAME	DESCRIPTION
<input checked="" type="checkbox"/>	▶ REQUEST-910-IP-REPUTATION	
<input checked="" type="checkbox"/>	▶ REQUEST-911-METHOD-ENFORCEMENT	
<input checked="" type="checkbox"/>	▶ REQUEST-912-DOS-PROTECTION	
<input checked="" type="checkbox"/>	▶ REQUEST-913-SCANNER-DETECTION	
<input checked="" type="checkbox"/>	▶ REQUEST-920-PROTOCOL-ENFORCEMENT	
<input type="checkbox"/>	▶ REQUEST-921-PROTOCOL-ATTACK	
<input checked="" type="checkbox"/>	▶ REQUEST-930-APPLICATION-ATTACK-LFI	
<input checked="" type="checkbox"/>	▶ REQUEST-931-APPLICATION-ATTACK-RFI	
<input checked="" type="checkbox"/>	▶ REQUEST-932-APPLICATION-ATTACK-RCE	
<input checked="" type="checkbox"/>	▶ REQUEST-933-APPLICATION-ATTACK-PHP	
<input checked="" type="checkbox"/>	▶ REQUEST-941-APPLICATION-ATTACK-XSS	
<input checked="" type="checkbox"/>	▶ REQUEST-942-APPLICATION-ATTACK-SQLI	
<input checked="" type="checkbox"/>	▶ REQUEST-943-APPLICATION-ATTACK-SESSIO...	

# AZURE APPLICATION GATEWAY – MARKET PLACE

- PRECONFIGURED VENDOR VM APPLIANCES, SUPPORTED BY AZURE
- BYOL OR PAY-PER-USE
- CAN BE AN ALTERNATIVE FOR AZURE PLATFORM PROVIDED OPTIONS

Appliances	
	VM-Series Next Generation Firewall (BYOL) Palo Alto Networks, Inc.
	Cisco ASAv - BYOL 4 NIC Cisco Systems, Inc.
	F5 WAF Solution for ASC F5 Networks
	Riverbed SteelCentral ApplInternals APM Riverbed Technology
	Barracuda NextGen Firewall F-Series (BYOL) Barracuda Networks, Inc.
	FortiGate NGFW High Availability (HA) Fortinet
	FortiGate NGFW Single VM Fortinet
	Fortinet Web Application Firewall - FortiWeb Fortinet
	A10 vThunder ADC BYOL A10 Networks
	BYOL Load Balancer, ADC & WAF - Trial & Perpetual KEMP Technologies Inc
	Cisco CSR 1000v - XE 16.4 Deployment with 2 NICs Cisco Systems, Inc.

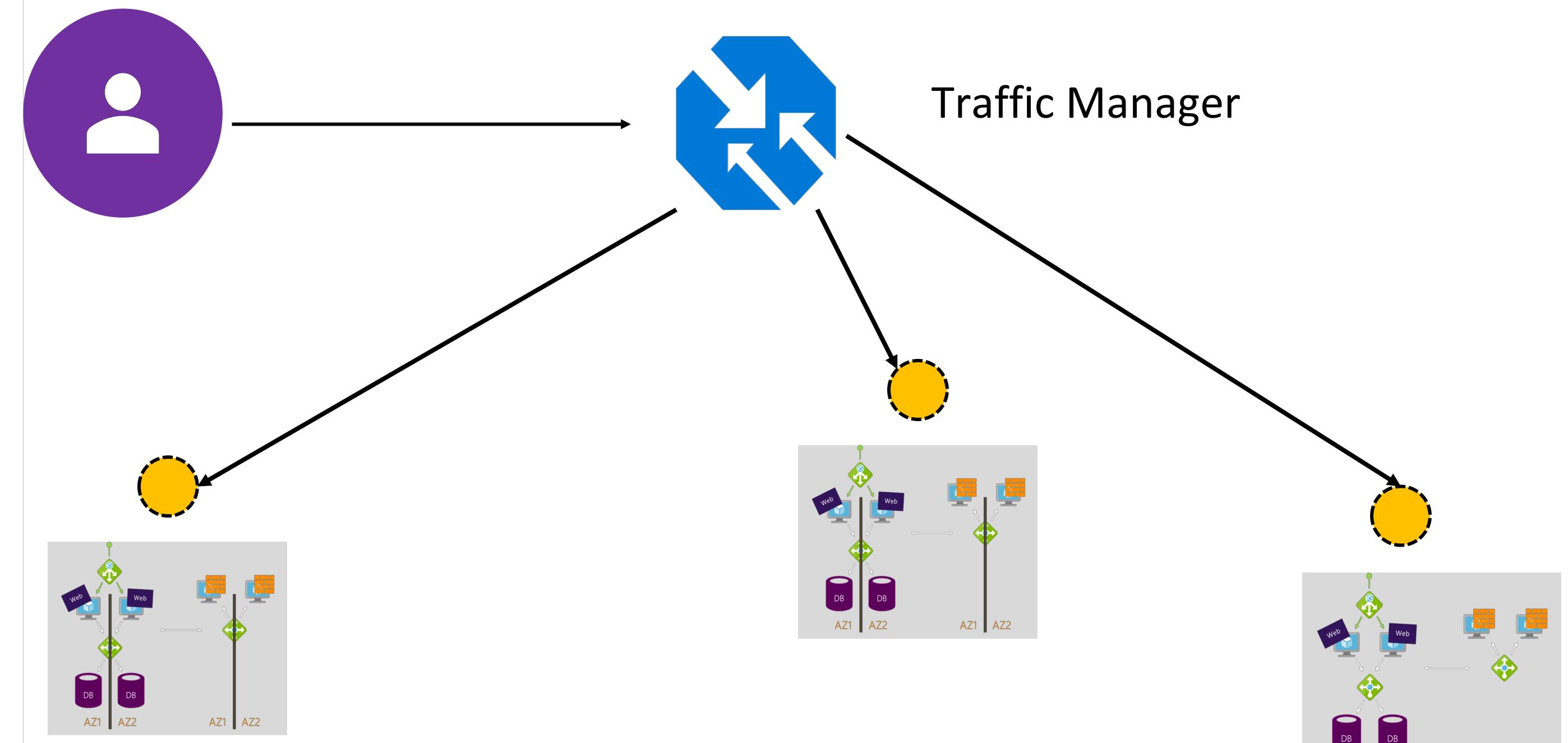
# AZURE TRAFFIC MANAGER

- GLOBAL RESILIENCY AND PERFORMANCE, BASED ON DNS

## 6 LOAD BALANCING OPTIONS:

- PRIORITY, WEIGHTED, GEOGRAPHICAL, PERFORMANCE, MULTI VALUE, SUBNET

- **Priority**: Select **Priority** when you want to use a primary service endpoint for all traffic, and provide backups in case the primary or the backup endpoints are unavailable.
- **Weighted**: Select **Weighted** when you want to distribute traffic across a set of endpoints, either evenly or according to weights, which you define.
- **Performance**: Select **Performance** when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint in terms of the lowest network latency.
- **Geographic**: Select **Geographic** so that users are directed to specific endpoints (Azure, External, or Nested) based on which geographic location their DNS query originates from. This empowers Traffic Manager customers to enable scenarios where knowing a user's geographic region and routing them based on that is important. Examples include complying with data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.
- **Multivalue**: Select **MultiValue** for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, all healthy endpoints are returned.
- **Subnet**: Select **Subnet** traffic-routing method to map sets of end-user IP address ranges to a specific endpoint within a Traffic Manager profile. When a request is received, the endpoint returned will be the one mapped for that request's source IP address.



# LOAD BALANCING SOLUTIONS - SUMMARY

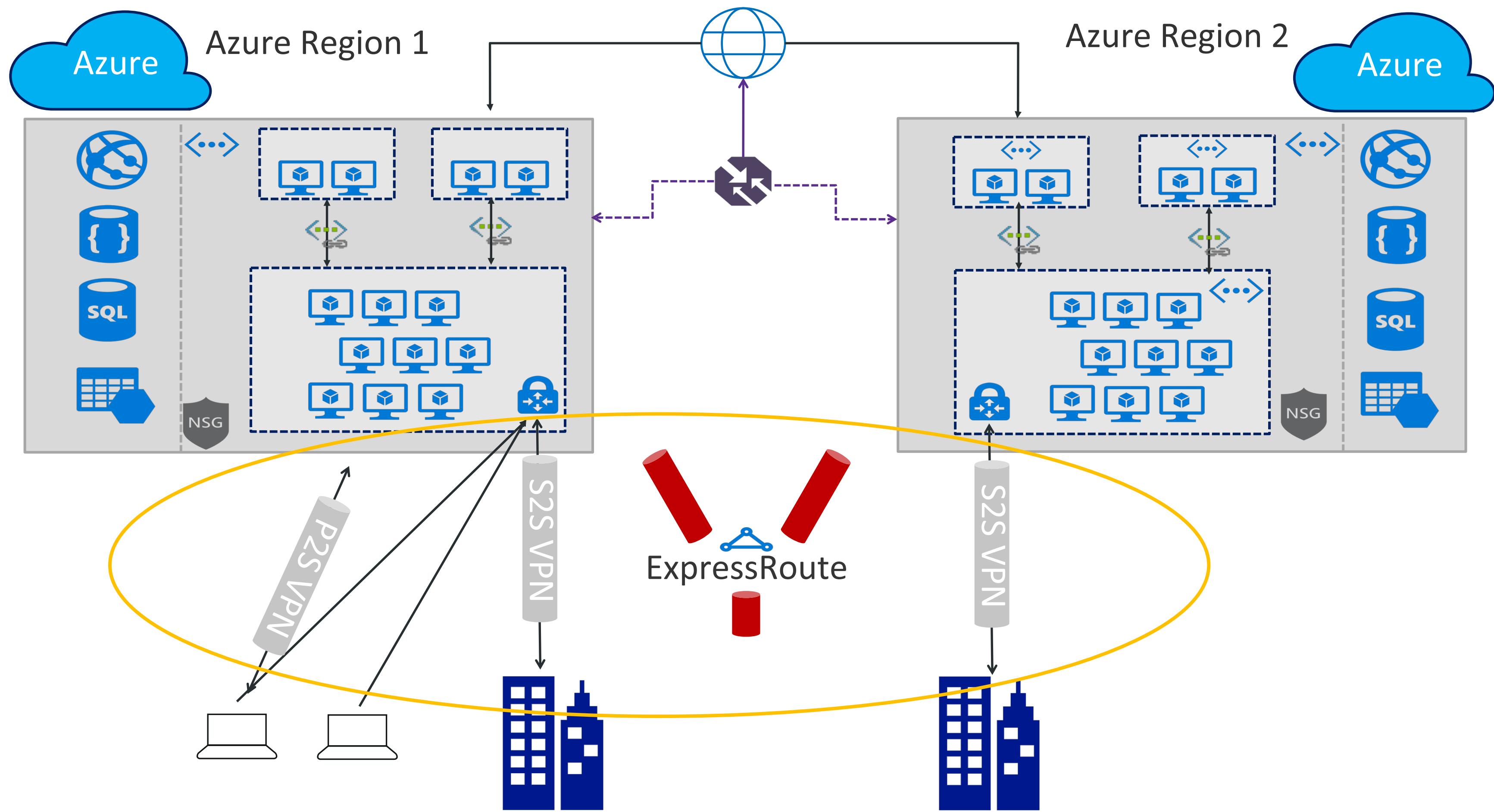
- AZURE LOAD BALANCER (LAYER 4)
- AZURE APPLICATION GATEWAY (LAYER 7)
- AZURE MARKETPLACE LOAD BALANCING APPLIANCE (LAYER 7)
- AZURE TRAFFIC MANAGER (DNS-BASED)

# EXTERNAL CONNECTIVITY

# EXTERNAL CONNECTIVITY

- ON-PREM TO AZURE CONNECTIVITY
- VNET PEERING WITH LOCAL AND GLOBAL VNET
- MULTI-REGION CONNECTIVITY
- SERVICE ENDPOINTS

# ON-PREM TO AZURE – POSSIBLE SCENARIOS



# ON-PREM TO AZURE – CONNECTIVITY OPTIONS

Connectivity	Benefits
ExpressRoute	<ul style="list-style-type: none"><li>■ ExpressRoute as primary cross-premises connectivity</li><li>■ Multiple circuits for redundancy &amp; better routing</li><li>■ ExpressRoute-VPN co-existence for highly available, redundant paths</li><li>■ Access to PaaS or SaaS offerings</li><li>■ Dedicated ports and dedicated NAT IP's on the datacenter site</li></ul>
Site-to-Site VPN	<ul style="list-style-type: none"><li>■ S2S VPN over Internet for remote branch locations</li><li>■ BGP &amp; active-active configuration for HA and transit</li><li>■ Easy to deploy and cheap to maintain, fast to provision</li><li>■ Very broad support for devices available</li></ul>
Point-to-Site VPN	<ul style="list-style-type: none"><li>■ P2S VPN for mobile users &amp; developers to connect from anywhere with macOS &amp; Windows</li><li>■ AD/radius authentication for enterprise grade security</li><li>■ Possibility to require authentication with Azure AD</li></ul>

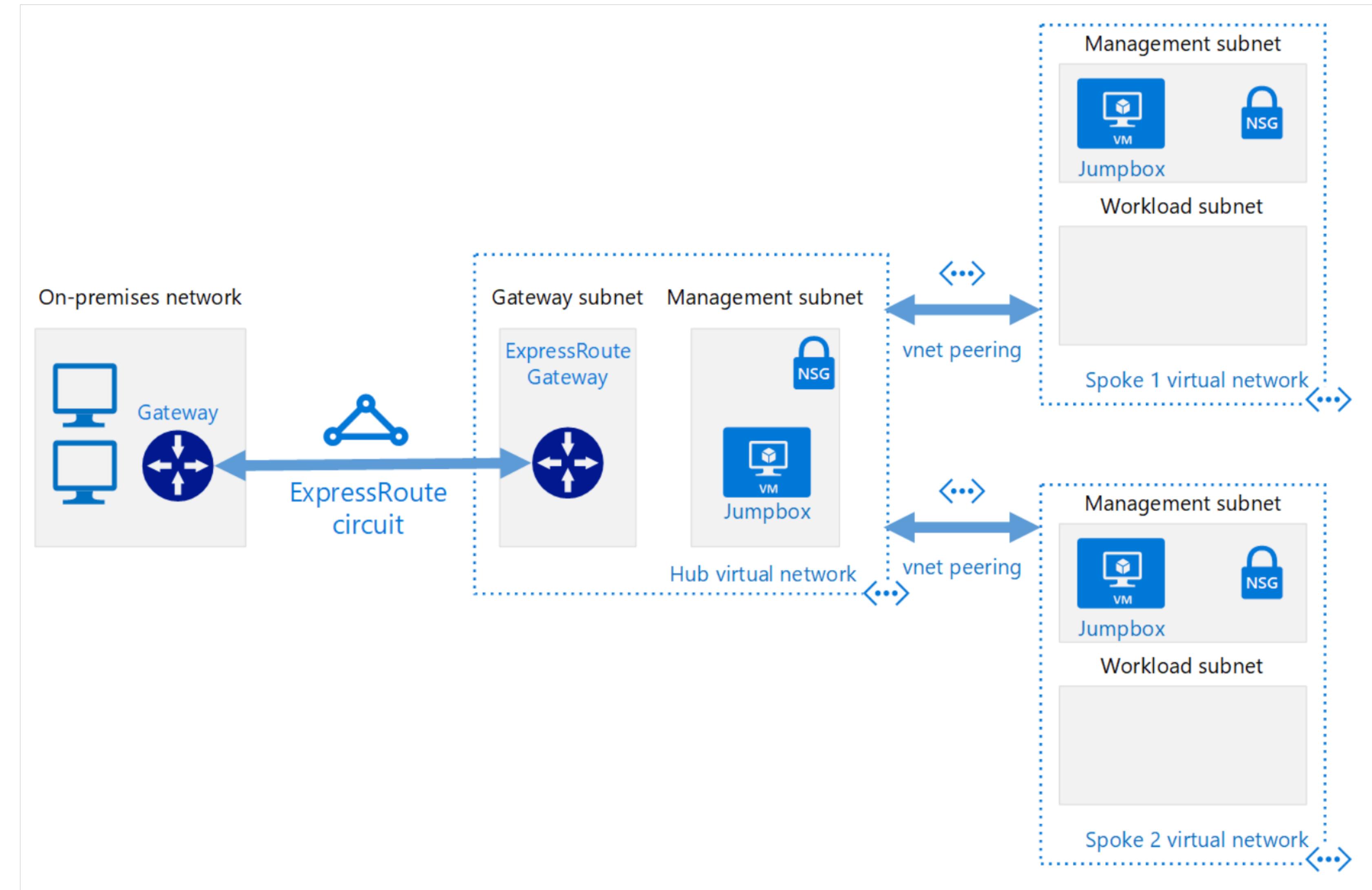
# HIGH-PERF VPN GATEWAYS

## SCENARIOS:

- HIGH THROUGHPUT, HYBRID WORKLOAD OVER VPN TUNNELS
- FAILOVER FROM EXPRESSROUTE CIRCUITS TO S2S VPN TUNNELS
- P2S FOR DEV/TEST CONNECTIVITY FROM ANYWHERE

SKU	S2S/VNet-to-VNet Tunnels	P2S Connections	P2S IKEv2 Connections	Aggregate Throughput Benchmark	BGP
Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported
VpnGw1	Max. 30*	Max. 128	Max. 250	650 Mbps	Supported
VpnGw2	Max. 30*	Max. 128	Max. 500	1 Gbps	Supported
VpnGw3	Max. 30*	Max. 128	Max. 1000	1.25 Gbps	Supported

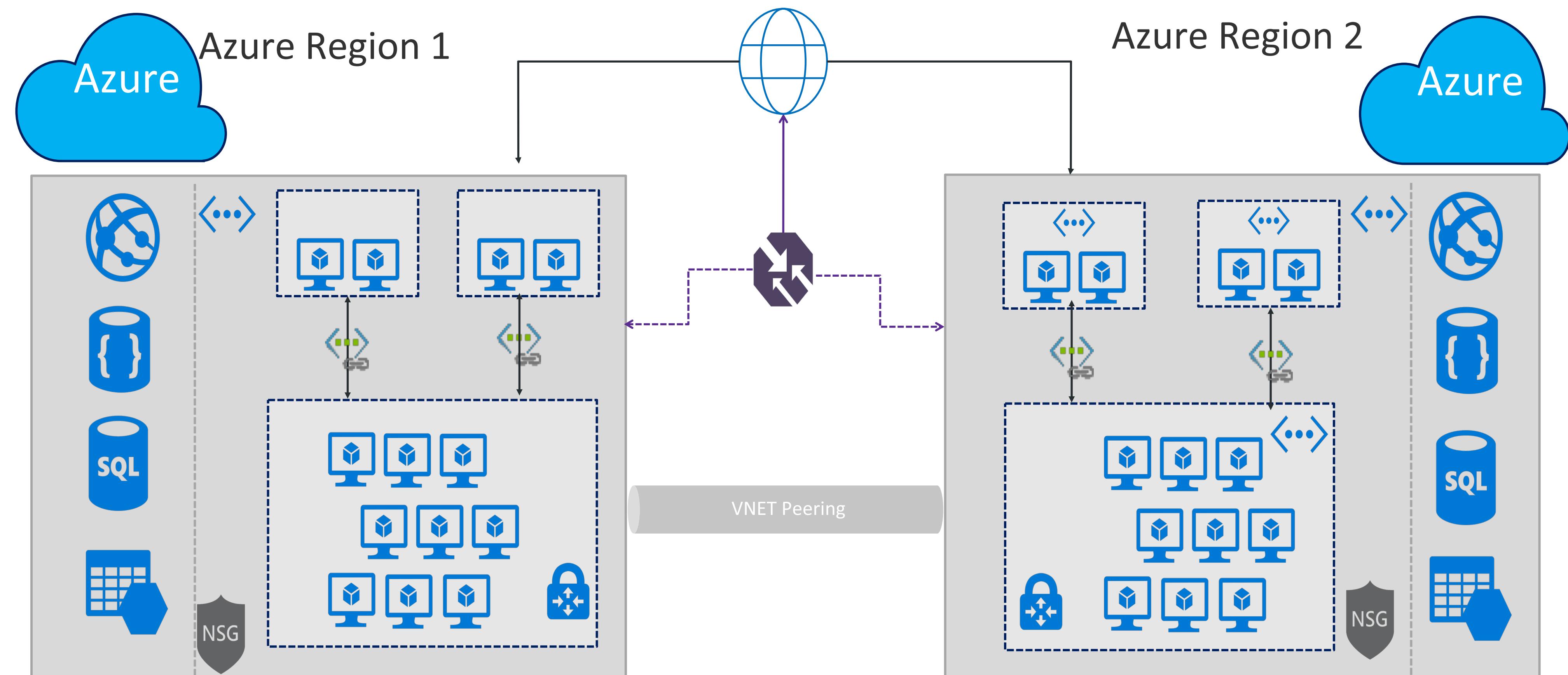
# VPN GATEWAYS ARCHITECTURE



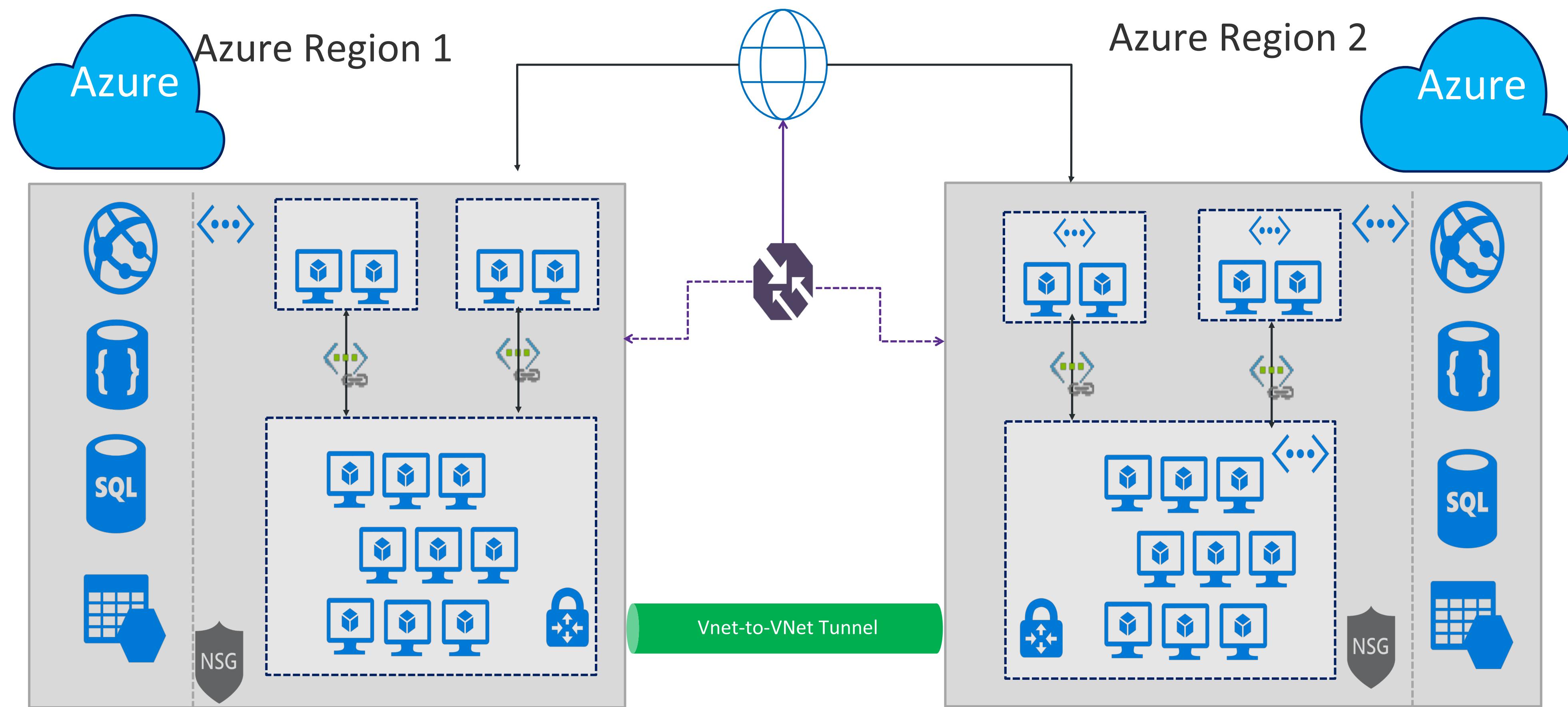
## VNET PEERING

- VNET PEERING ALLOWS YOU TO INTERCONNECT 2 AZURE VNETS, AS IF THEY ARE 1 LARGE VNET  
(DEFAULT ROUTING AVAILABLE WITH FULL SPEED AND LOW LATENCY, WORK IN BACKBONE)
- VNET PEERING IS POSSIBLE WITHIN THE SAME AZURE REGION, OR ACROSS AZURE REGIONS  
(USING MS BACKBONE, NO PUBLIC INTERNET INVOLVED)
- VNET PEERING IS SUPPORTED TO INTERCONNECT AN AZURE CLASSIC VNET WITH AN ARM VNET  
(E.G., FOR MIGRATING WORKLOADS)
- VNET GLOBAL PEERING VS. VNET PEERING HAS SOME IMPACT ON ACCESSING LOCAL LOAD  
BALANCERS
- PREVIOUSLY ONLY VPN GATEWAY CONNECTION BETWEEN REGIONS AND VNETS WAS POSSIBLE

# VNET PEERING



# VNET PEERING



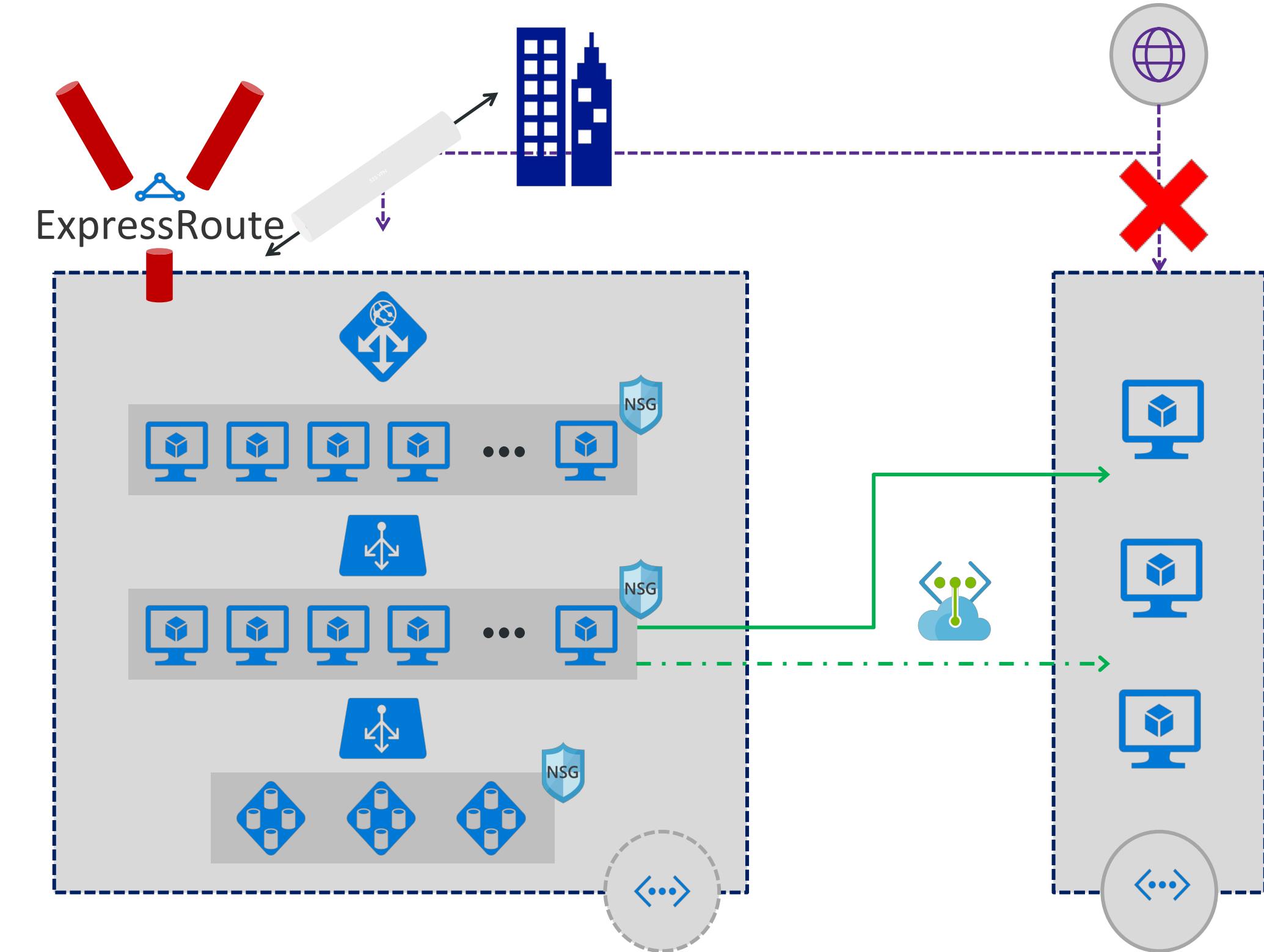
# FORCED TUNNELING

## CHALLENGES:

- IAAS SERVICES ACCESSIBLE THROUGH INTERNET
- CUSTOMERS MAY REQUIRE THEIR VMS TO BE ONLY ACCESSED FROM ON-PREMISES VNET

## SOLUTION—FORCED TUNNELING:

- IAAS SERVICES ONLY ACCESSIBLE FROM A VNET
- SITE-TO-SITE VPN
- OR EXPRESSROUTE



# SERVICE ENDPOINTS

## CHALLENGES:

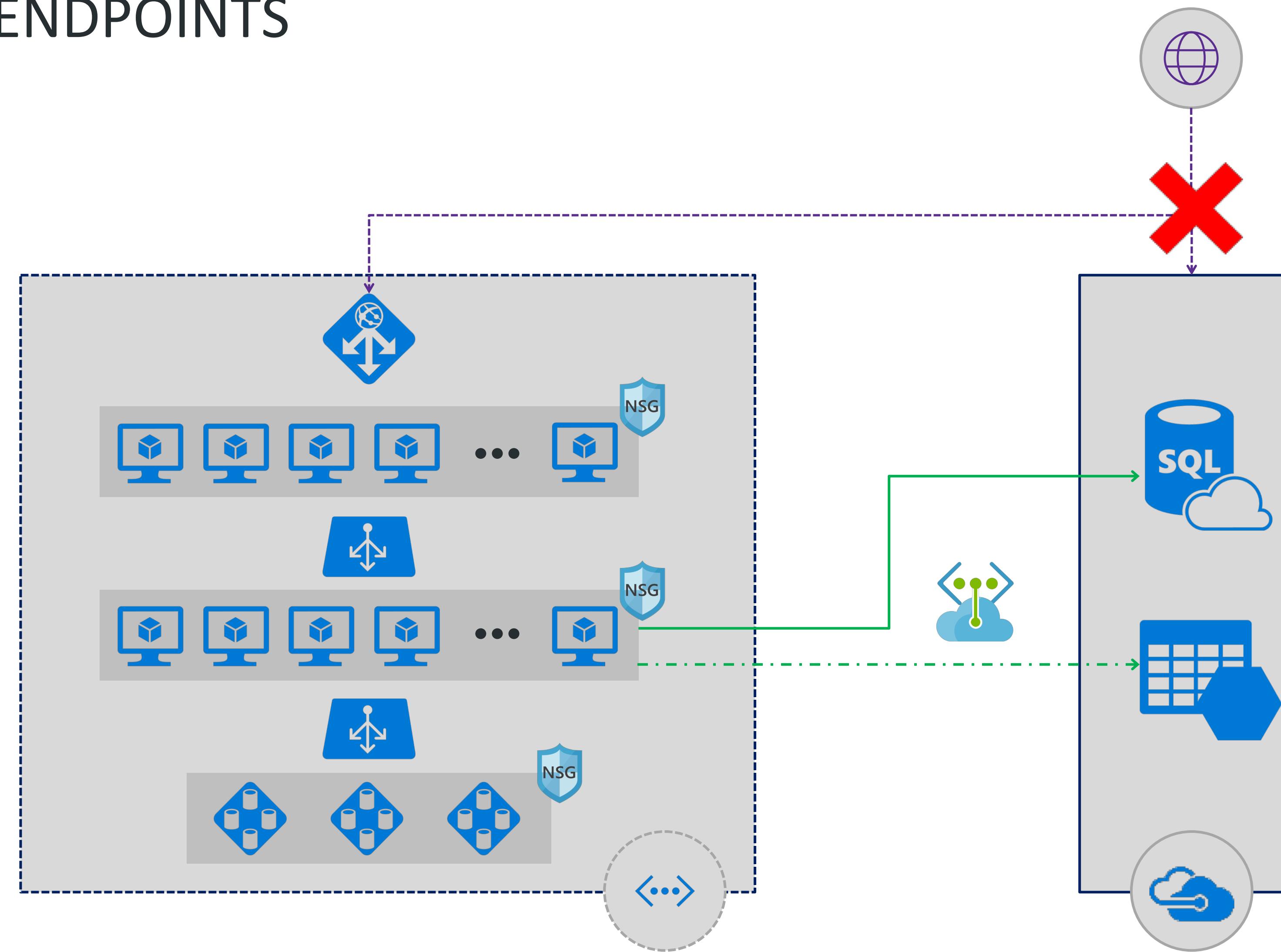
- PAAS SERVICES ACCESSIBLE THROUGH INTERNET
- CUSTOMERS MAY REQUIRE THEIR SERVICES ENDPOINTS TO BE ONLY ACCESSED FROM THEIR VNETS

## SOLUTION—VNET SERVICE ENDPOINTS:

- PAAS SERVICES ONLY ACCESSIBLE FROM A VNET
- AVAILABLE NOW FOR STORAGE, SQL DB, COSMOS DB AND MANY MORE
- WILL ROLL OUT TO OTHER PAAS SERVICES IN THE FUTURE

SERVICE	SUBNET	STATUS	LOCATIONS
Microsoft.Sql	1	Succeeded	North Europe
Microsoft.Storage	AzureFirewallSubnet	Succeeded	North Europe, West Europe

# SERVICE ENDPOINTS



# SERVICE ENDPOINTS

**mifurmsa - Firewalls and virtual networks**  
Storage account

Search (Ctrl+/  
Save Discard Refresh

Allow access from  
 All networks  Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks  
Secure your storage account with virtual networks. + Add existing virtual network + Add new virtual network

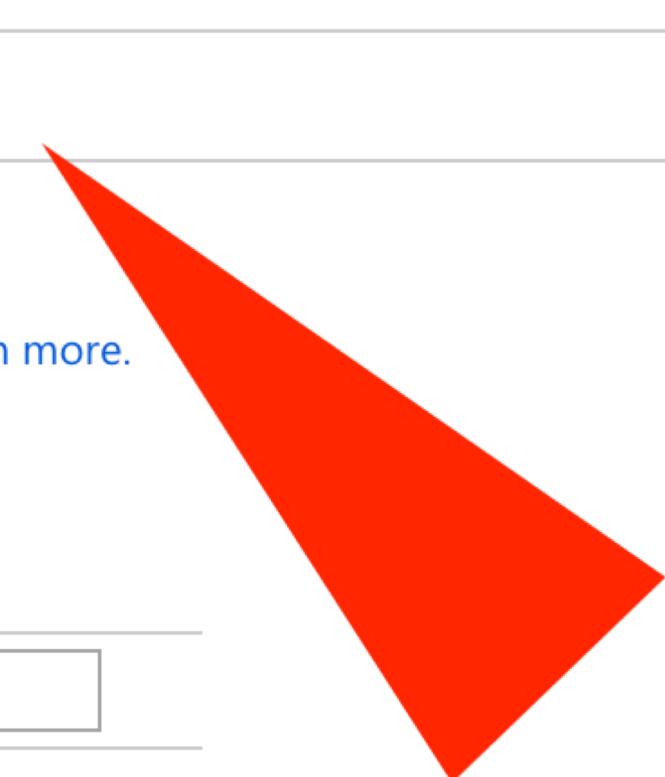
VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
vnet01	1	10.4.0.0/16		mntworkshop2-rg	ChmurowiskoLAB

Firewall  
Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)

Add your client IP address ('217.8.177.132') i

ADDRESS RANGE  
IP address or CIDR

Exceptions  
 Allow trusted Microsoft services to access this storage account i  
 Allow read access to storage logging from any network



# EXTERNAL CONNECTIVITY - SUMMARY

- ON-PREM TO AZURE CONNECTIVITY
- VNET PEERING WITH LOCAL AND GLOBAL VNET
- MULTI-REGION CONNECTIVITY
- SERVICE ENDPOINTS

# SECURING CONNECTIVITY

# SECURING CONNECTIVITY

- NETWORK SECURITY GROUPS
- APPLICATION SECURITY GROUPS
- SERVICE TAGS

# NETWORK SECURITY GROUPS

A NETWORK SECURITY GROUP (NSG) IS A TOP LEVEL OBJECT THAT IS ASSOCIATED TO YOUR SUBSCRIPTION:

- IT CAN BE USED TO CONTROL TRAFFIC TO ONE OR MORE VIRTUAL MACHINE (VM) INSTANCES IN YOUR VIRTUAL NETWORK
- AN NSG CONTAINS ACCESS CONTROL RULES THAT ALLOW OR DENY TRAFFIC TO AND FROM VM INSTANCES
- THE RULES OF AN NSG CAN BE CHANGED AT ANY TIME, AND CHANGES ARE APPLIED TO ALL ASSOCIATED INSTANCES
- NSG ARE ATTACHED ON SUBNET OR NIC LEVEL
- MAXIMUM NUMBER OF 4000 RULES CAN BE ASSIGNED, DEFAULT RULES CANNOT BE CHANGED

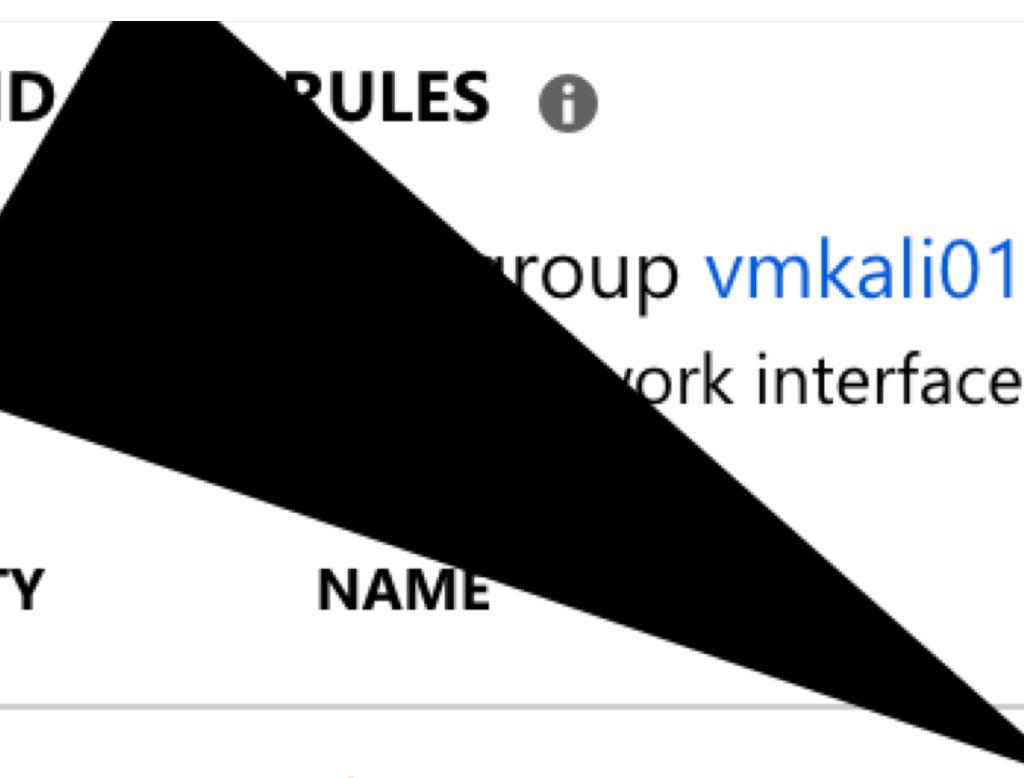
**BE CAREFULL – NSG'S ARE STATEFULL ☺ ONCE CONNECTION HAS BEEN ESTABLISHED, IT WILL NOT BE DROPPED**

# NETWORK SECURITY GROUPS – INBOUND RULES

**INBOUND RULES** ⓘ

Network security group [vmkali01-nsg](#) (attached to network interface: [vmkali01725](#))

Add inbound port rule



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
300	⚠ SSH	22	TCP	Any	Any	<span>Allow</span>	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<span>Allow</span>	...
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBal...	Any	<span>Allow</span>	...
65500	DenyAllInBound	Any	Any	Any	Any	<span>Deny</span>	...

# NETWORK SECURITY GROUPS – OUTBOUND RULES

## OUTBOUND PORT RULES

 Network security group [vmkali01-nsg](#) (attached to network interface: [vmkali01725](#))  
Impacts 0 subnets, 1 network interfaces

[Add outbound port rule](#)

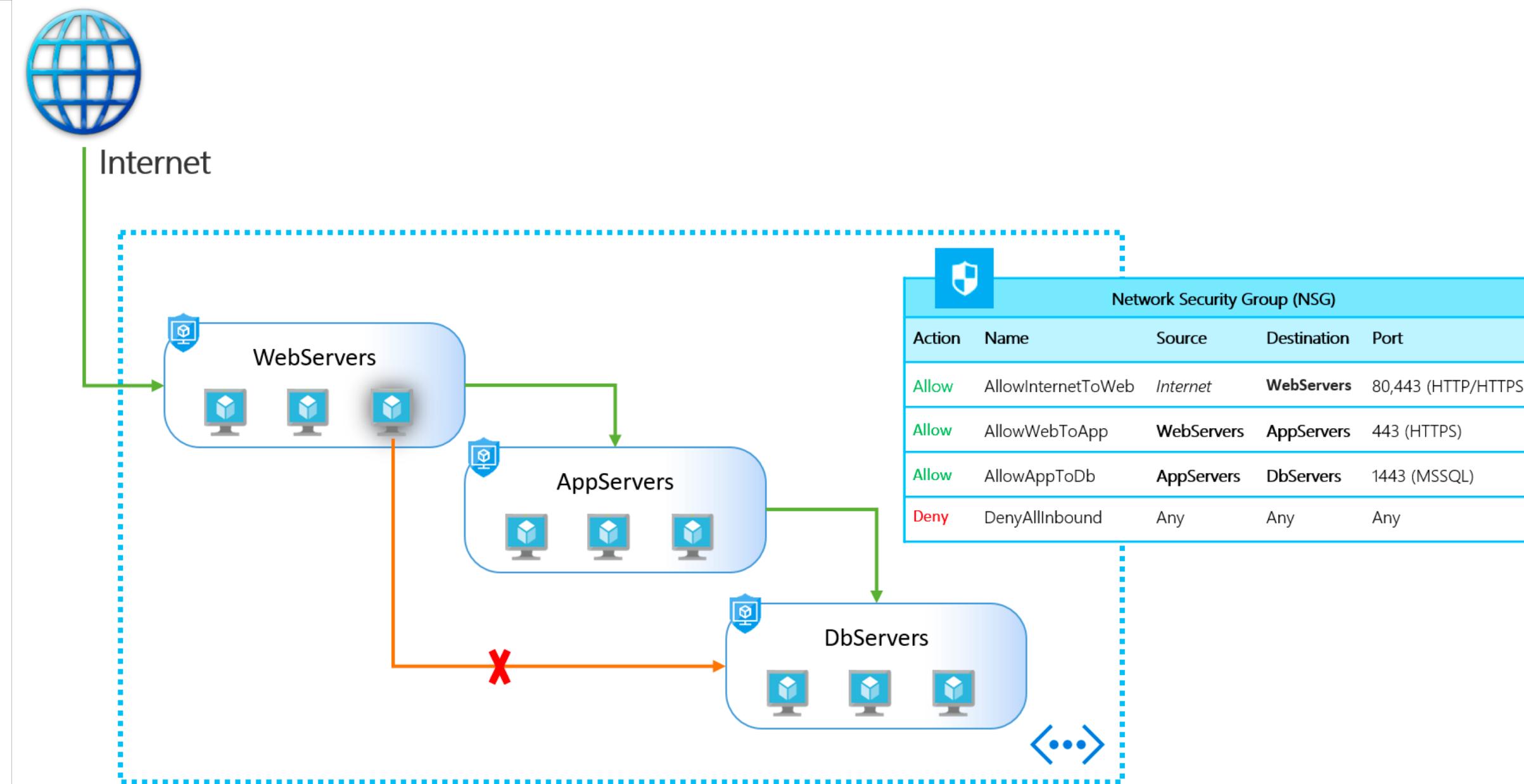
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow	<a href="#">...</a>
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow	<a href="#">...</a>
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny	<a href="#">...</a>

# APPLICATION SECURITY GROUPS

**APPLICATION SECURITY GROUPS** ⓘ

 asgwfeappsec  Configure the application security groups

4096      denyall      Any      Any       asgwfeapp...     asgwfeapp...     Deny      ...



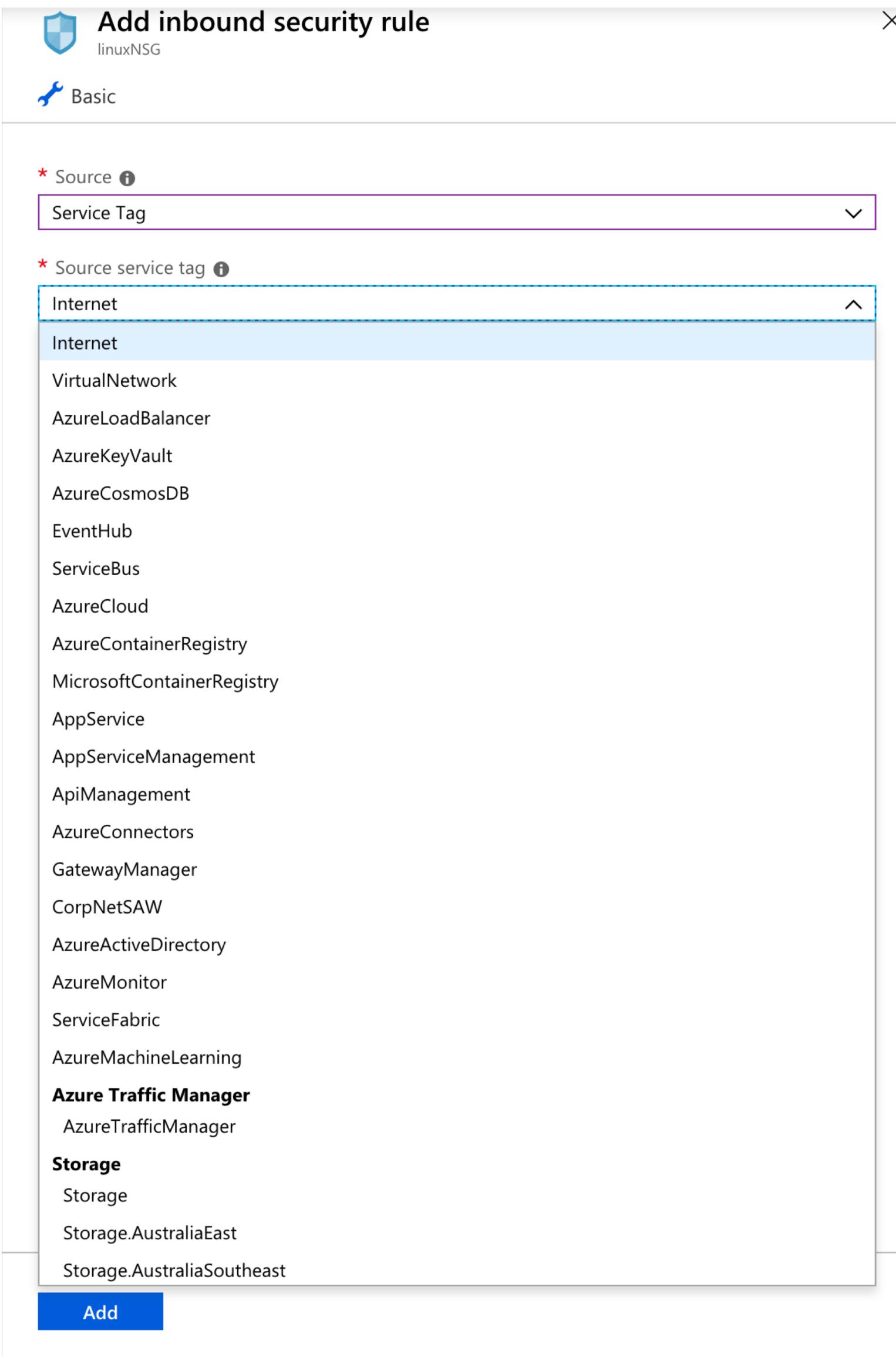
The diagram illustrates a network architecture with three server groups: WebServers, AppServers, and DbServers. The Internet connects to the WebServers group. The WebServers group connects to the AppServers group. The AppServers group connects to the DbServers group. A red 'X' on the connection line between the AppServers and DbServers groups indicates a Deny rule. To the right of the diagram, a table titled 'Network Security Group (NSG)' shows the configuration:

Action	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,443 (HTTP/HTTPS)
Allow	AllowWebToApp	WebServers	AppServers	443 (HTTPS)
Allow	AllowAppToDb	AppServers	DbServers	1443 (MSSQL)
Deny	DenyAllInbound	Any	Any	Any

SZKOŁA CHMURY

Chmurowisko

# SERVICE TAGS



# SECURING CONNECTIVITY - SUMMARY

- NETWORK SECURITY GROUPS
- APPLICATION SECURITY GROUPS
- SERVICE TAGS

## OTHER SERVICES

## OTHER SERVICES

- AZURE FIREWALL
- AZURE NETWORK WATCHER
- AZURE DDOS

# AZURE FIREWALL

The screenshot shows the Azure Firewall interface. On the left, a sidebar menu lists various options: Overview (selected), Activity log, Access control (IAM), Tags, Settings, Rules (selected), Properties, Locks, and Automation script.

**Overview Page:**

- Resource group: mntworkshop2-rg
- Location: North Europe
- Subscription: ChmurowiskoLAB
- Subscription ID: c0eace6b-deca-4861-8042-b4e807cef056
- Virtual network/subnet: vnet01/AzureFirewallSubnet
- Private IP address: 10.4.0.4
- Public IP address: azureFirewalls-ip2
- Provisioning state: Failed

**Rules Page:**

- Overview (selected)
- Activity log
- Access control (IAM)
- Tags
- Settings
- Rules (selected)
- Properties
- Locks
- Automation script

The main content area displays the NAT rule collection:

- NAT rule collection:** Selected tab.
- Network rule collection:**
- Application rule collection:**

**Add NAT rule collection**

PRIORITY	NAME	ACTION	RULES
100	rdp	Dnat	▶ 1 rule.

# AZURE FIREWALL

NAT rule collection   Network rule collection   Application rule collection

+ Add application rule collection

PRIORITY	NAME	ACTION	RULES	...
100	onet.pl	Allow	▶ 1 rule.	...
300	mifurmsa.blob.core.windows.net	Allow	▶ 1 rule.	...

# AZURE NETWORK WATCHER

Home > Network Watcher

## Network Watcher

Microsoft

- Search (Ctrl+ /)
- Overview
- Monitoring
  - Topology
  - Connection monitor
  - Network Performance Monitor
- Network diagnostic tools
  - IP flow verify
  - Next hop
  - Security group view
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot
- Metrics
  - Usage + quotas
- Logs
  - NSG flow logs
  - Diagnostic logs
  - Traffic Analytics

Network Watcher - Topology

Microsoft

- Search (Ctrl+ /)
- Download topology
- Subscription: ChmurowiskoLAB
- Resource Group: mntworkshop2-rg
- Virtual Network: vnet01-mng
- Overview
- Monitoring
  - Topology
  - Connection monitor
  - Network Performance Monitor
- Network diagnostic tools
  - IP flow verify
  - Next hop
  - Security group view
  - VPN troubleshoot
  - Packet capture
  - Connection troubleshoot
- Metrics
  - Usage + quotas
- Logs
  - NSG flow logs
  - Diagnostic logs

The diagram illustrates the Azure Network Watcher topology for the vnet01-mng virtual network. It shows the following structure:

- Subnets:** wfe-subnet, dns-subnet, backend-subnet.
- VMs:** vmub1604dev01NIC01, vmub1804dev01NIC01, vmwin2k8r2dev01NIC01, vmwin2k16dev01NIC01, vmwin2k16r2dev01NIC01, vmub1604dev01PIP, vmub1604dev01, linuxNSG, backendpool, vmub1804dev01PIP, vmwin2k8r2dev01PIP, winNSG, vmwin2k16dev01PIP, vmwin2k16r2dev01PIP.
- Load Balancer:** lbstd02, LoadBalancerFront...
- Health Probe:** hp.

# AZURE NETWORK WATCHER

Home > Network Watcher

## Network Watcher

Microsoft

Search (Ctrl+ /)

**Overview**

**Monitoring**

- Topology
- Connection monitor
- Network Performance Monitor

**Network diagnostic tools**

- IP flow verify
- Next hop
- Security group view
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

**Metrics**

- Usage + quotas

**Logs**

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

## Network Watcher - Traffic Analytics

Microsoft

Search (Ctrl+/) Refresh Send us your feedback FAQ

\* Log Analytics subscriptions ChmurowiskoLAB oms-rg ChmurowiskoLAB 7 selected \* Time interval Last 30 days

### TRAFFIC VISUALIZATION

View your network traffic flow distribution

Total flows Inbound 1.1M 1M Outbound

**2.11M**

Category	Value
Inbound	152K 949K 998K 10K
Outbound	152K 944K 4.6K 998K 10K

This tabular representation of network traffic flow distribution is "not to scale"

### YOUR ENVIRONMENT

Across Azure regions, virtual networks, resources and subnetworks

**Deployed Azure regions**

**3** of 42 total

Region Type	Count
Active	2
Inactive	1
Traffic Analytics enabled	2
Allowed malicious	2

**TA enabled NSGs\***

**3** of 10

\* enable TA for all NSGs to view richer data

**Talking to Internet**

Ports receiving traffic from Internet 210.46K  
VMs sending traffic to Internet 7

**Virtual networks**

**9** total

Network Type	Count
Active	2
Inactive	7
Allowed malicious	2

**View VNets**

**Virtual subnetworks**

**14** total

Subnet Type	Count
Active	3
Inactive	11
Allowed malicious	3

**View subnets**

Do more Launch Log Search query Documentation

# AZURE NETWORK WATCHER – IP FLOW VERIFY

Home > Network Watcher

## Network Watcher

Microsoft

Search (Ctrl+ /)

Overview

Monitoring

- Topology
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify
- Next hop
- Security group view
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

## Network Watcher - IP flow verify

Microsoft

Search (Ctrl+ /) <

Overview

Monitoring

- Topology
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify
- Next hop
- Security group view
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

Specify a target virtual machine with associated network security groups, then run an inbound or outbound packet to see if access is allowed or denied.

\* Subscription *i*  
ChmurowiskoLAB

Resource group\* *i*  
mntworkshop2-rg

Virtual machine\* *i*  
vm01westus

Network interface\*  
vm01westus387

Packet details

Protocol  
 TCP  UDP

Direction  
 Inbound  Outbound

Local IP address\* *i*  
10.1.1.4 ✓ Local port\* *i*  
80 ✓

Remote IP address\* *i*  
212.77.98.9 ✓ Remote port\* *i*  
80 ✓

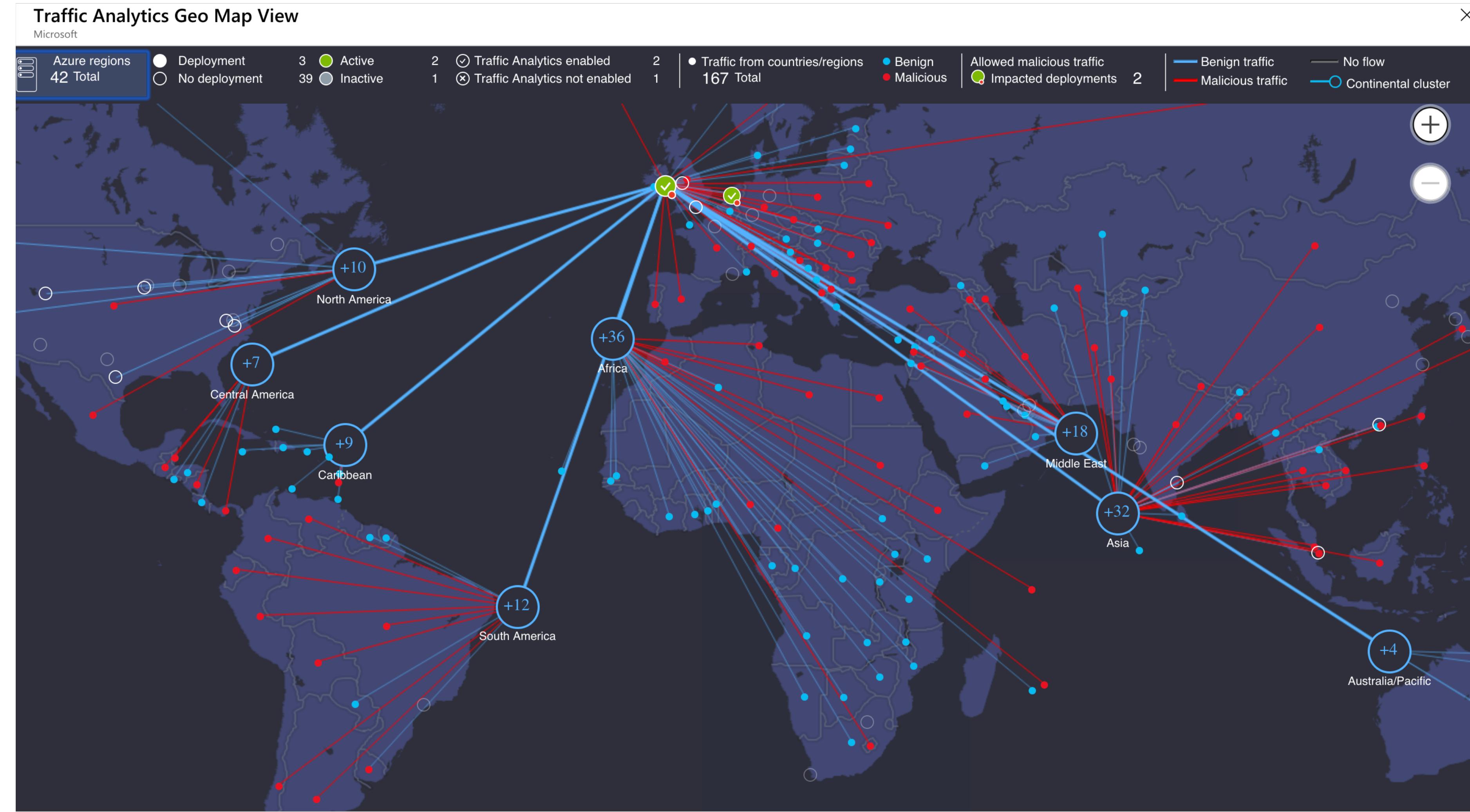
**Check**

Loading...

Access allowed

Security rule  
AllowInternetOutBound

# AZURE NETWORK WATCHER



# AZURE NETWORK WATCHER – TRAFFIC ANALYTICS

**Network Watcher - IP flow verify**  
Microsoft

Search (Ctrl+ /) <>

**Overview**

**Monitoring**

- Topology
- Connection monitor
- Network Performance Monitor

**Network diagnostic tools**

- IP flow verify** (selected)
- Next hop
- Security group view
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

**Metrics**

- Usage + quotas

**Logs**

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

Specify a target virtual machine with associated network security groups, then run an inbound or outbound packet to see if access is allowed or denied.

\* Subscription: ChmurowiskoLAB

Resource group\*: mntworkshop2-rg

Virtual machine\*: vm01westus

Network interface\*: vm01westus387

**Packet details**

Protocol:  TCP  UDP

Direction:  Inbound  Outbound

Local IP address\*: 10.1.1.4 Local port\*: 80

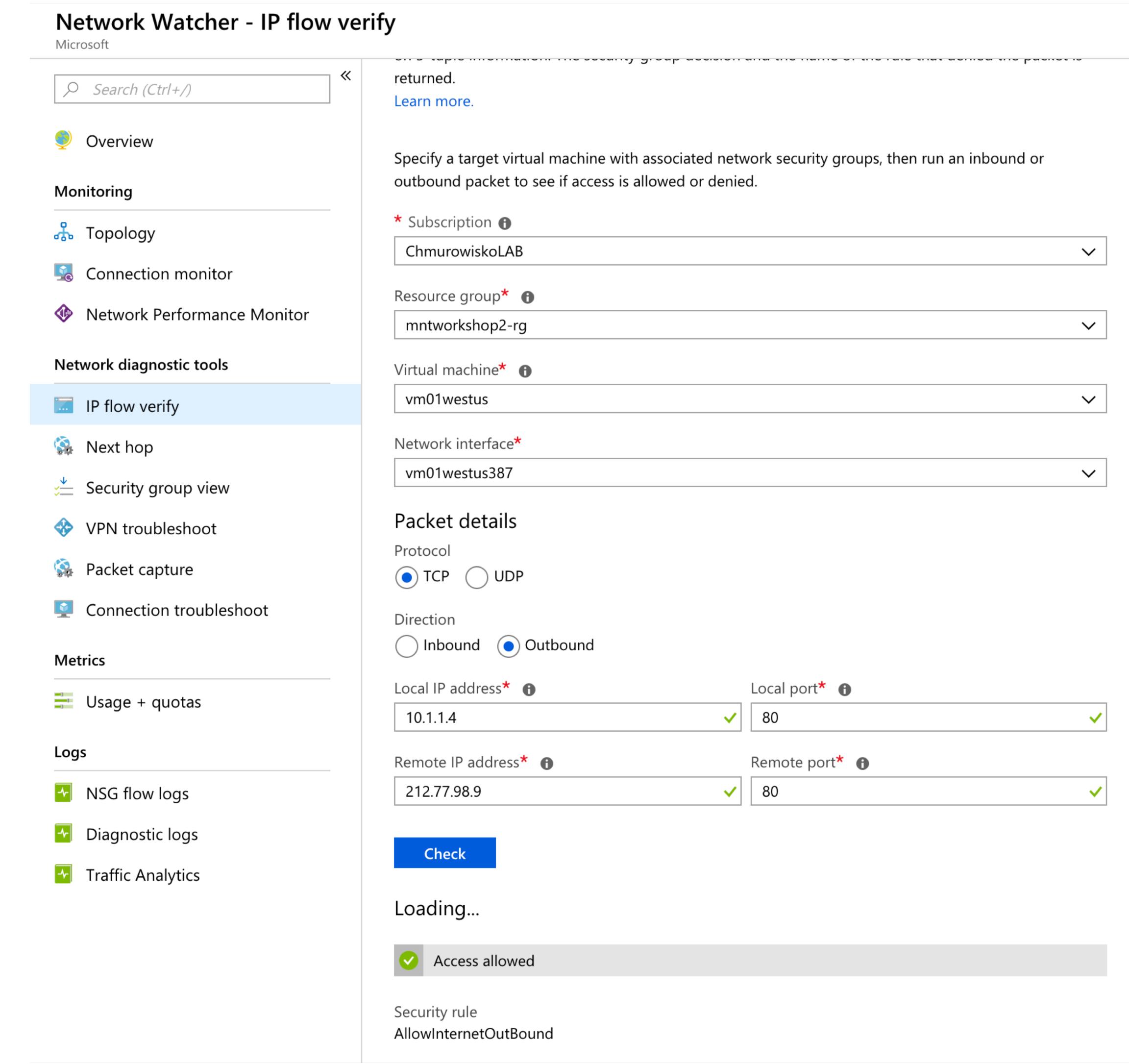
Remote IP address\*: 212.77.98.9 Remote port\*: 80

**Check**

Loading...

**Access allowed**

Security rule: AllowInternetOutBound



## OTHER SERVICES - SUMMARY

- AZURE FIREWALL
- AZURE NETWORK WATCHER
- AZURE DDOS