# NETWORKING IN AZURE

# MODULE OVERVIEW

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

# VIRTUAL NETWORKS

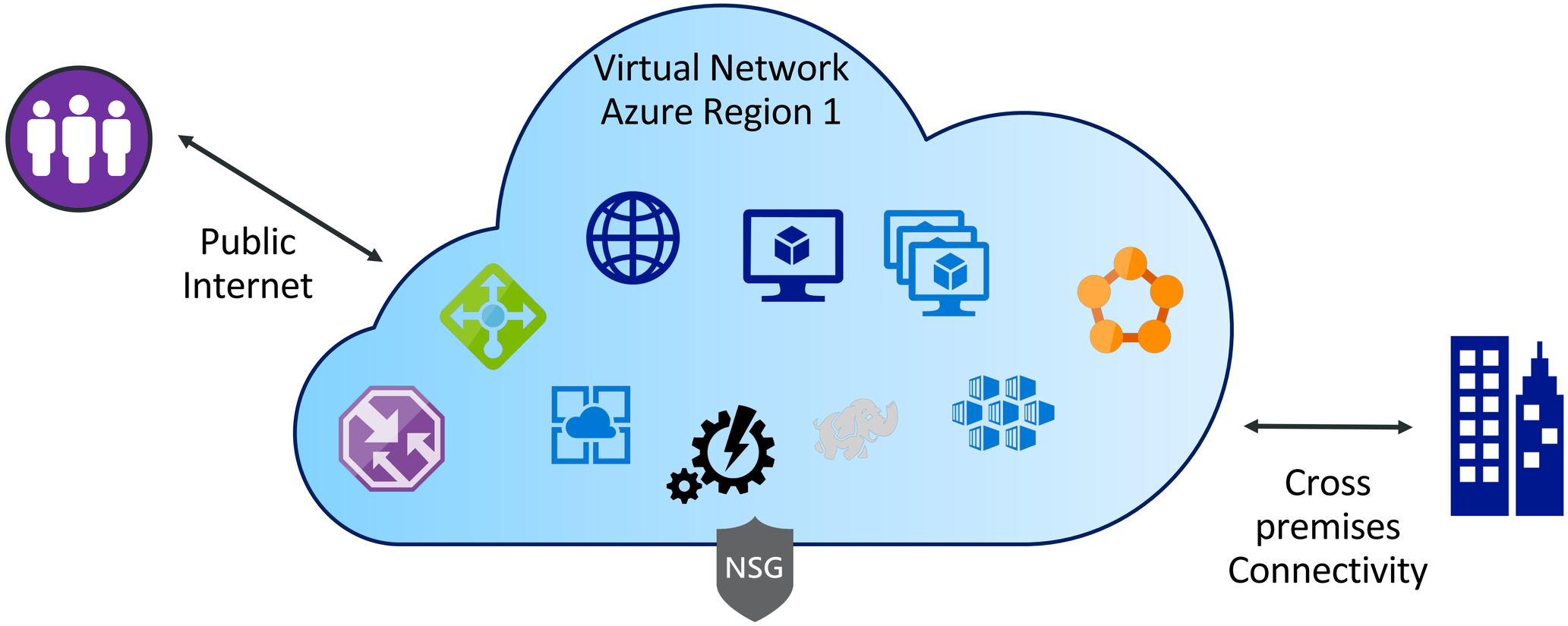
# VIRTUAL NETWORKS

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

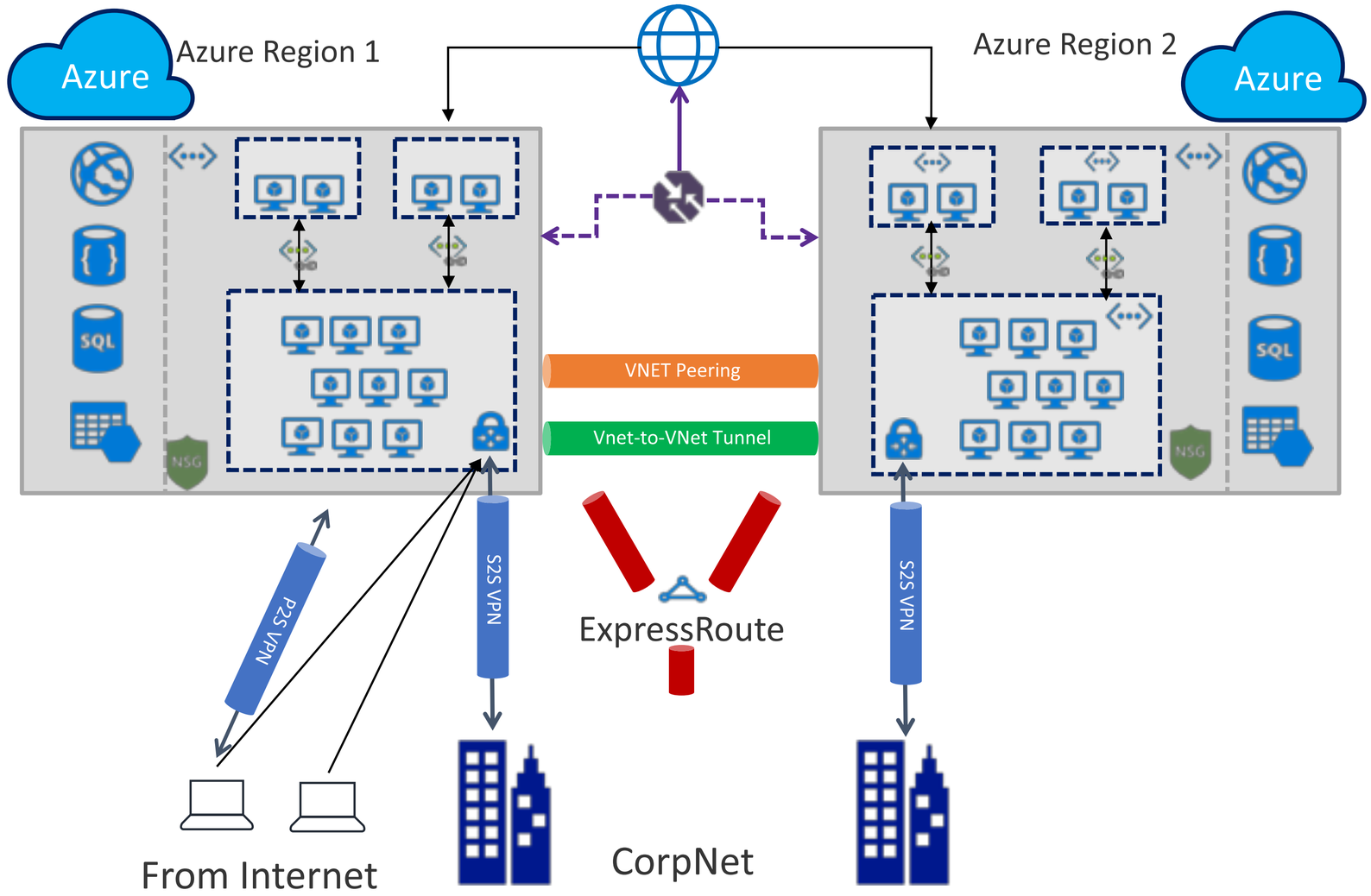
# AZURE NETWORKING BASICS

- 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

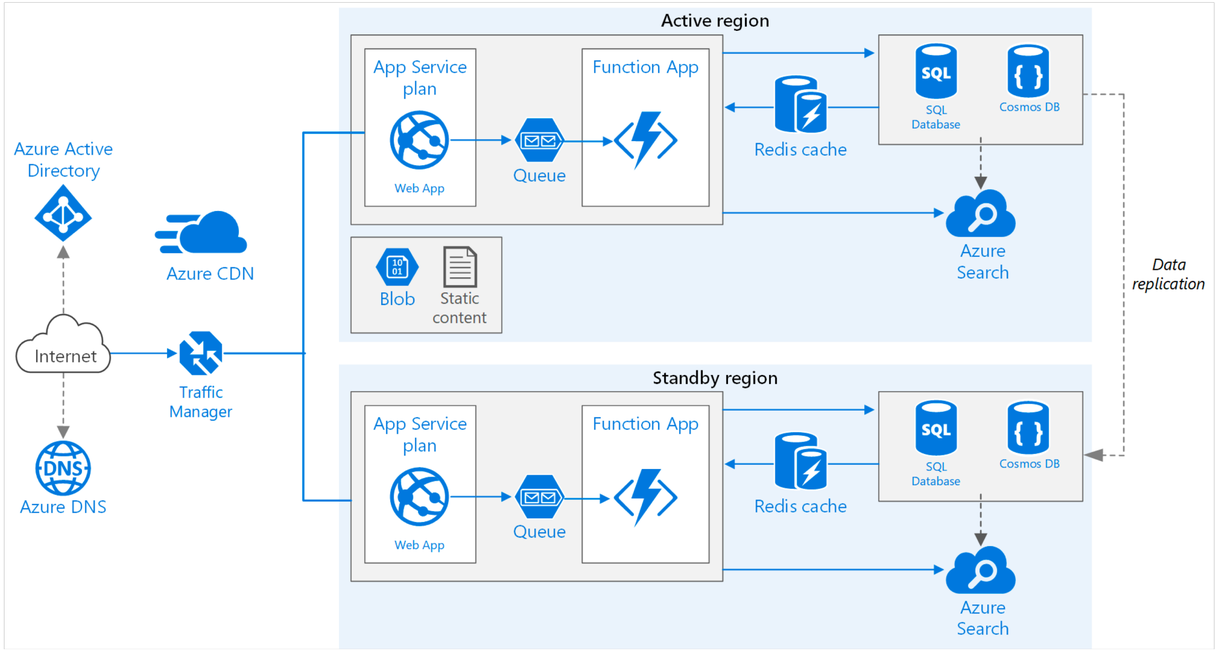


# MULTI-REGION VIRTUAL NETWORK ARCHITECTURE



# 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

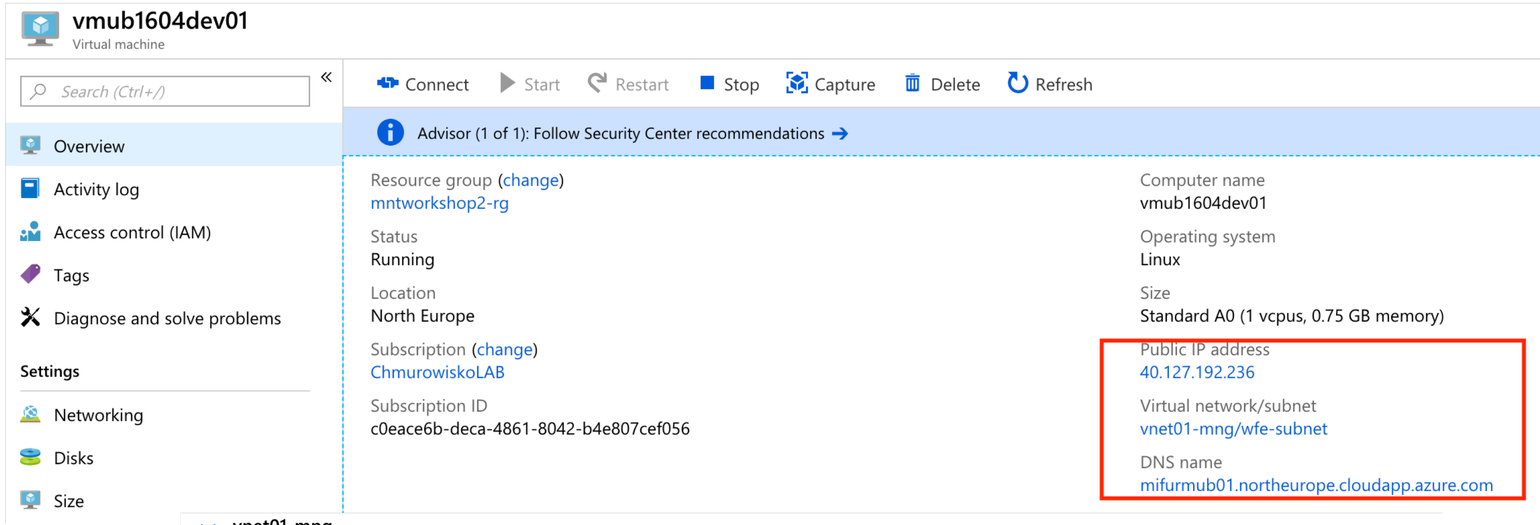
**SUBNET IP ADDRESSING:**

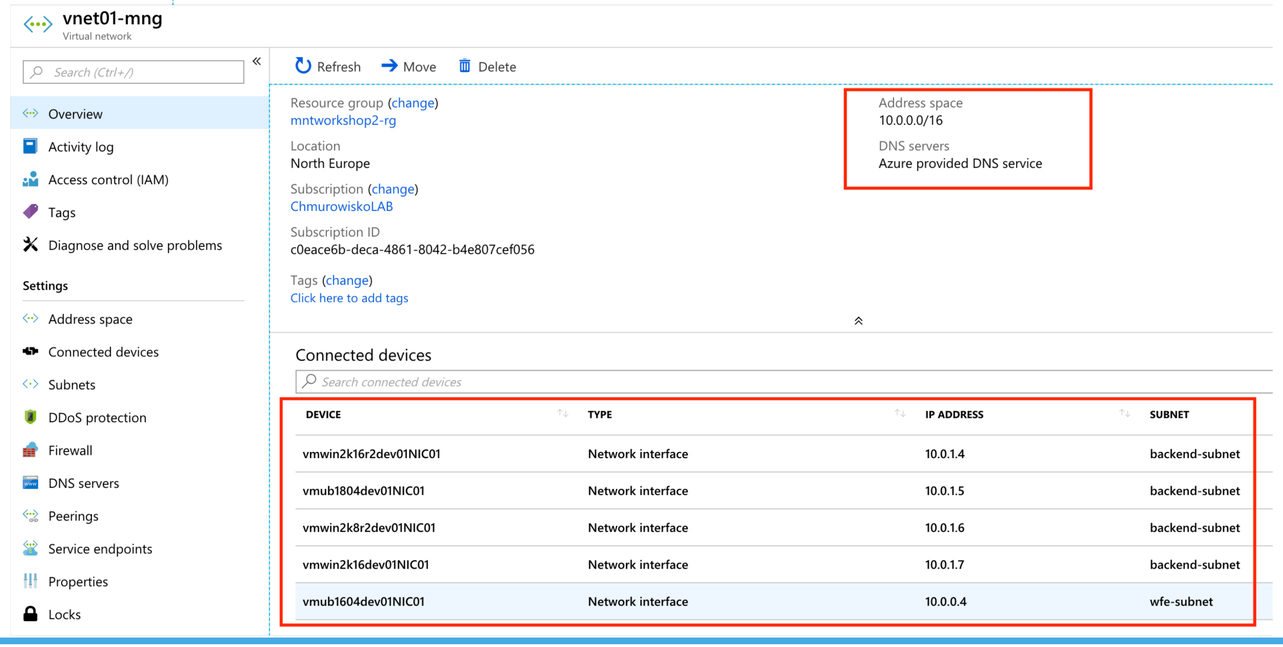
- IP-ADDRESS GETS ALLOCATED TO A NIC DURING PROVISIONING OF THE NIC
- FIRST AVAILABLE IP-ADDRESS IN A SUBNET RANGE IS X.X.X.4 (5 ADDRESS TAKEN BY AZURE)
- AZURE SUBNETS SUPPORT DYNAMIC (=DEFAULT) AND STATIC IP ADDRESSING, PUBLIC IP’S CAN USE IPV6

# 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



# 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)

```
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":{"ipAddress":[{"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:~$
```

- PUBLIC DNS NAMES (AVAILABLE FOR VMS AND APP SERVICES) MUST BE UNIQUE ACROSS AZURE REGIONS: <HOST.REGION.CLOUDAPP.AZURE.COM>

# VIRTUAL NETWORKS SUMMARY

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

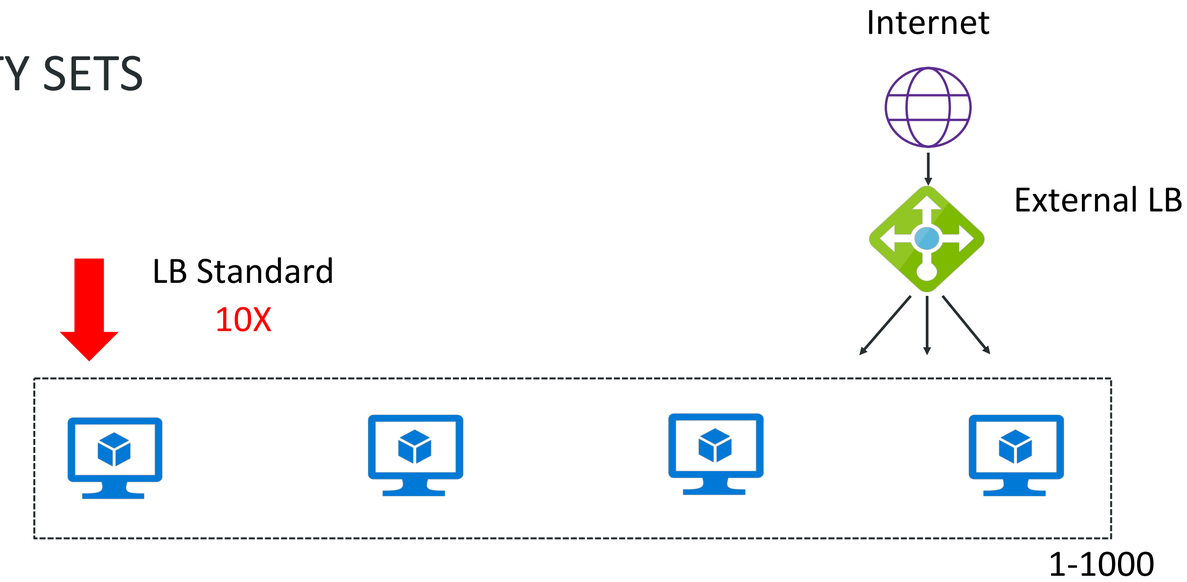
# LOAD BALANCING

# 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**

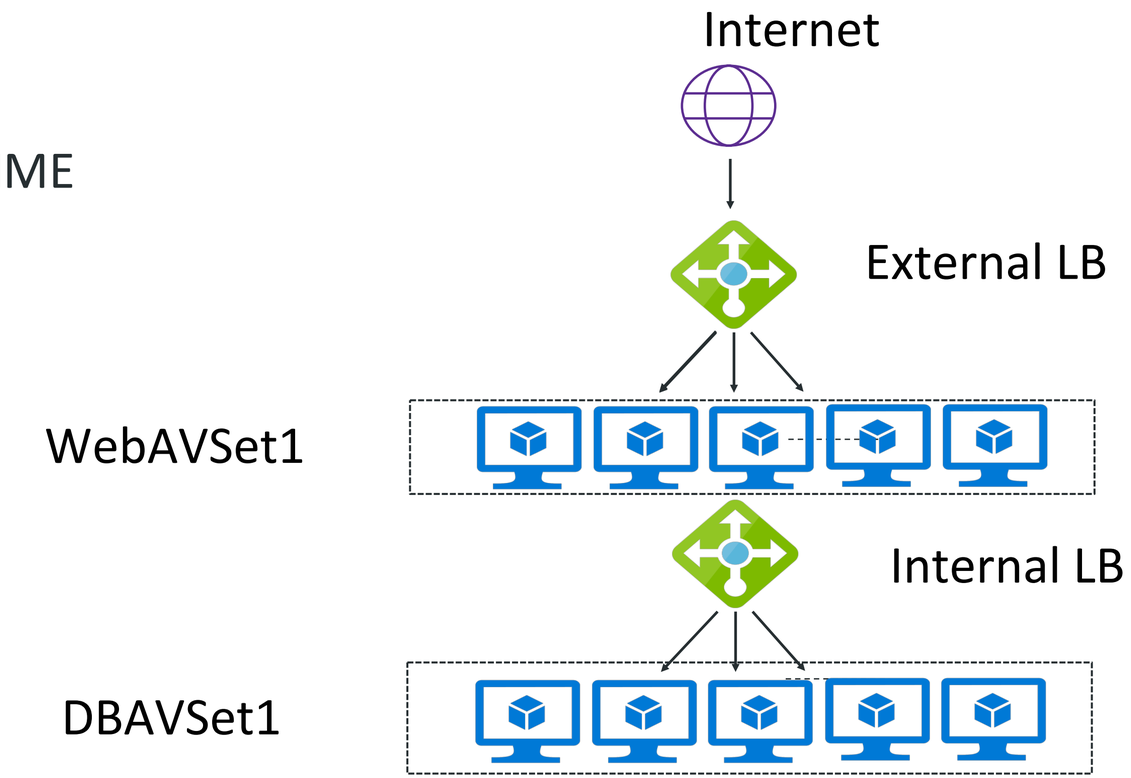
**SCENARIOS WITH:**

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

| Standard |
| --- |
| Up to 1000 backend instances |
| Zone-redundant frontend<br>Zonal frontend |
| Availability Sets not required<br>and Availability Zones |
| Integrated Frontend and<br>Backend health metrics |
| Supports HA Ports |
| NSG required |

# INTERNAL LOAD BALANCER

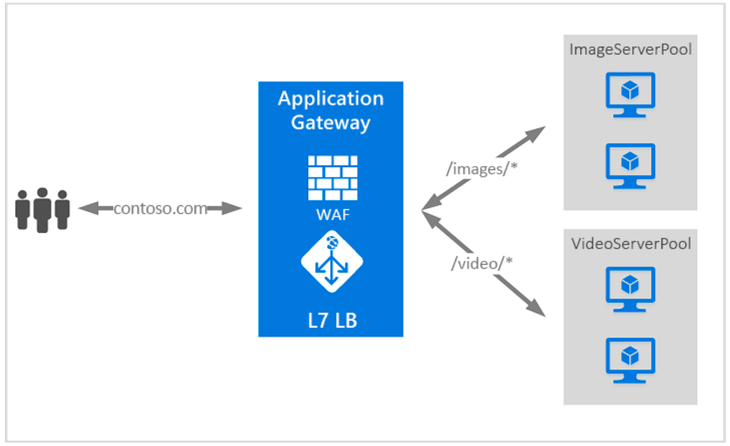
- LOAD BALANCER WITH A PRIVATE IP-ADDRESS, SENDING TRAFFIC ALONG TO THE BACK-END POOL SERVERS
- TCP, UDP TRAFFIC
- CANNOT BE PUBLIC / PRIVATE AT THE SAME TIME

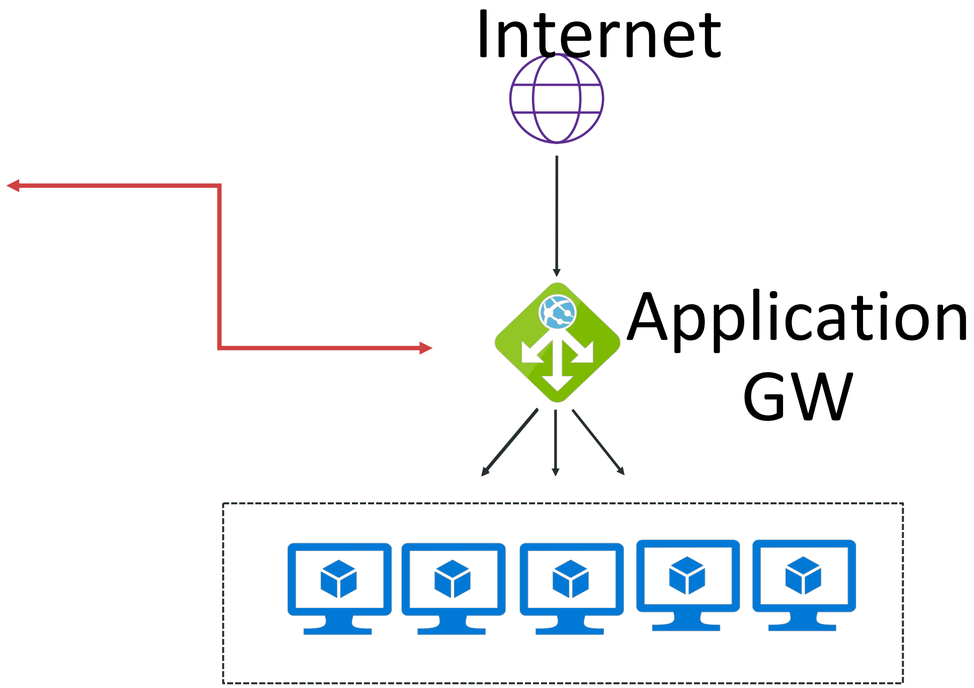


# AZURE APPLICATION GATEWAY

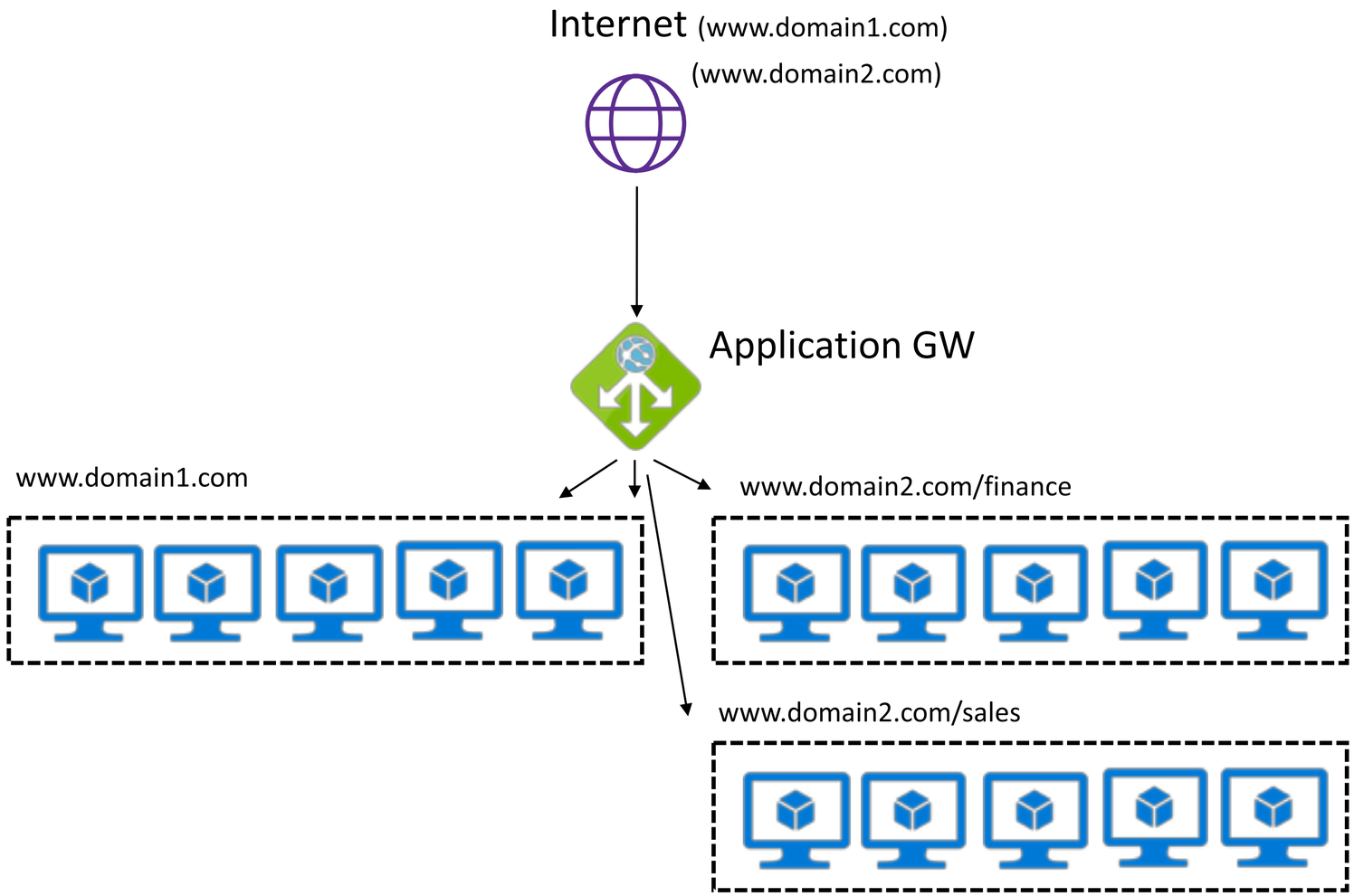
LOAD BALANCER WITH A PUBLIC IP-ADDRESS, SENDING TRAFFIC ALONG TO THE BACK-END POOL SERVERS

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

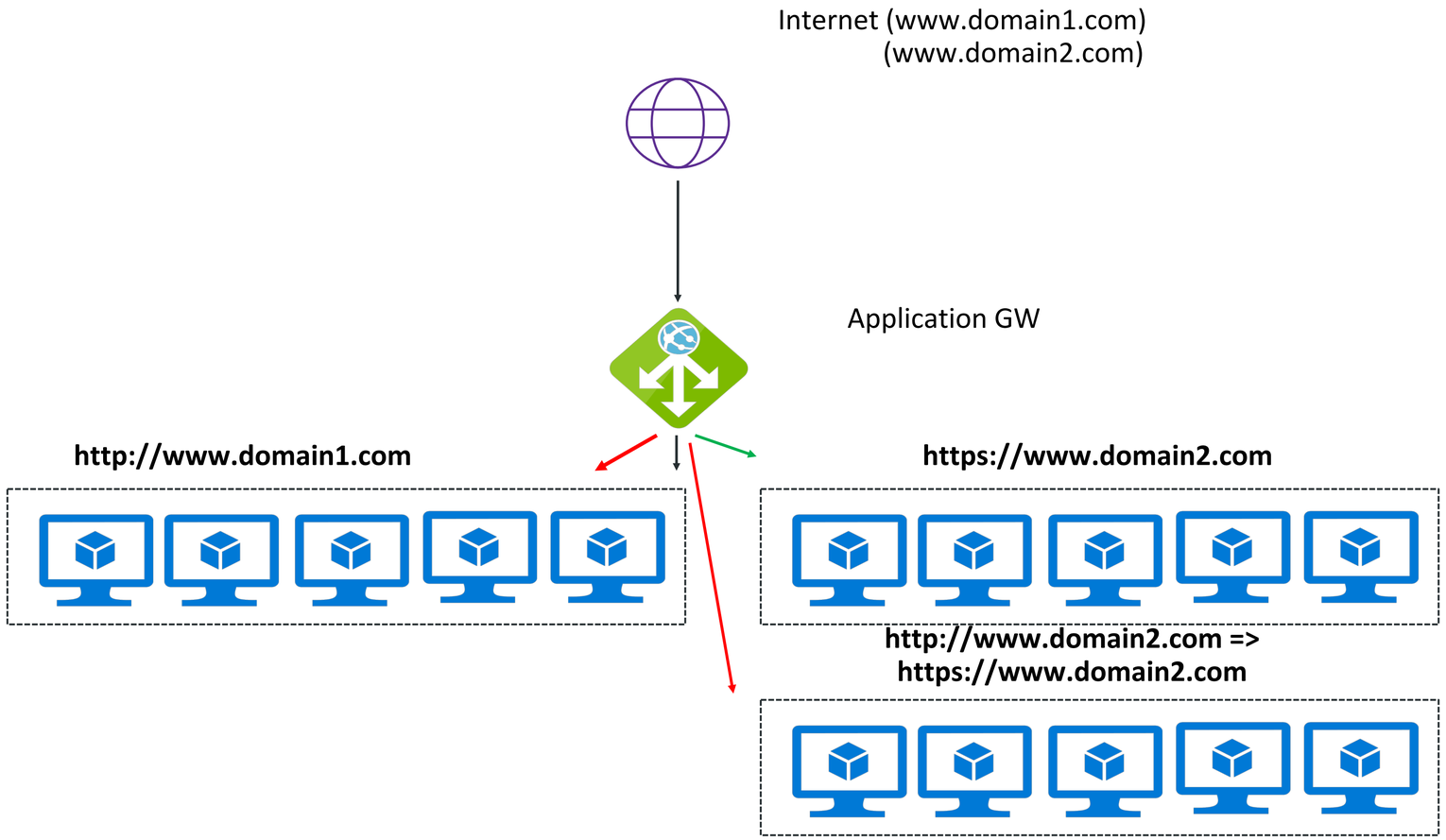


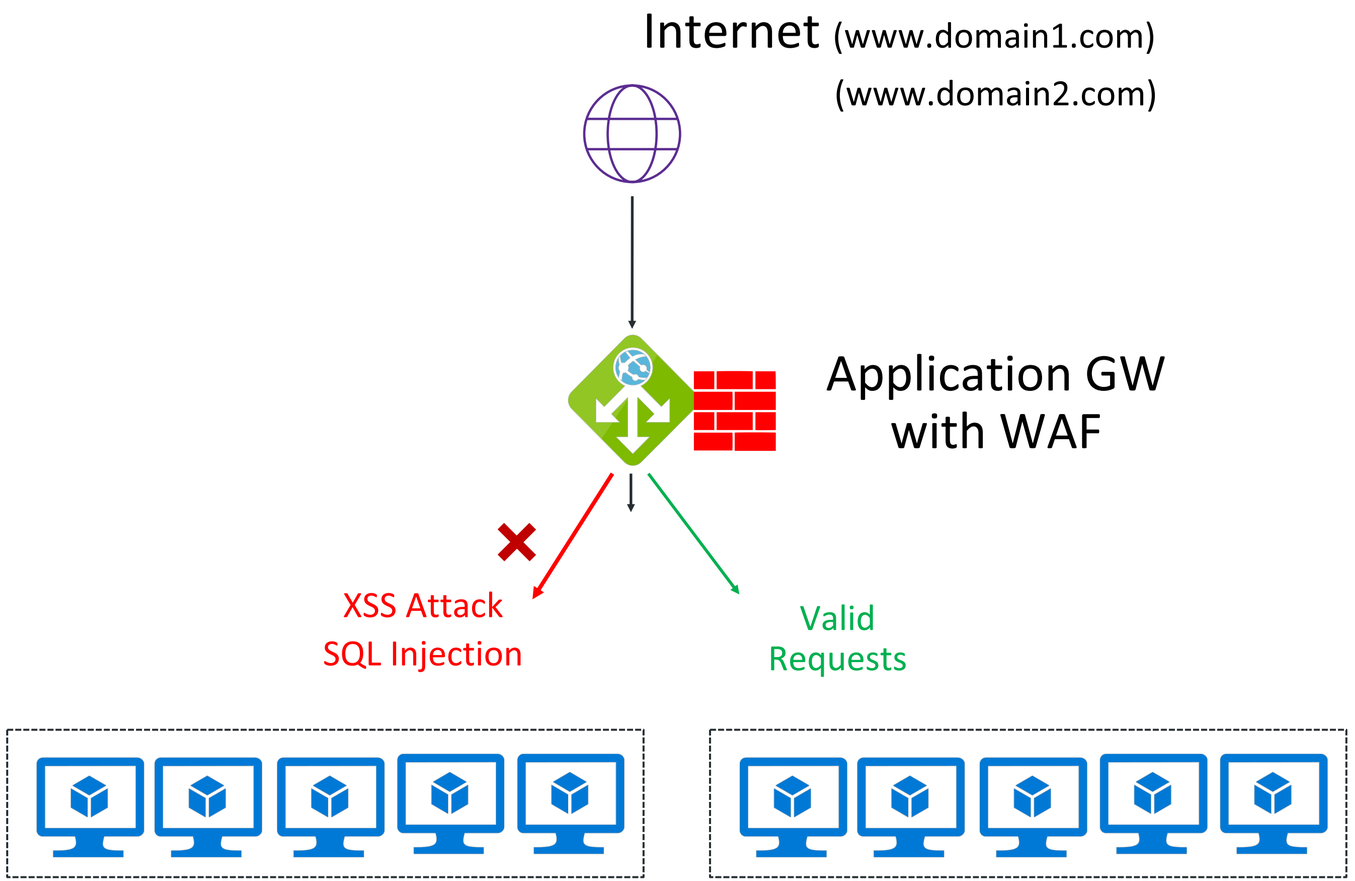
# AZURE APPLICATION GATEWAY



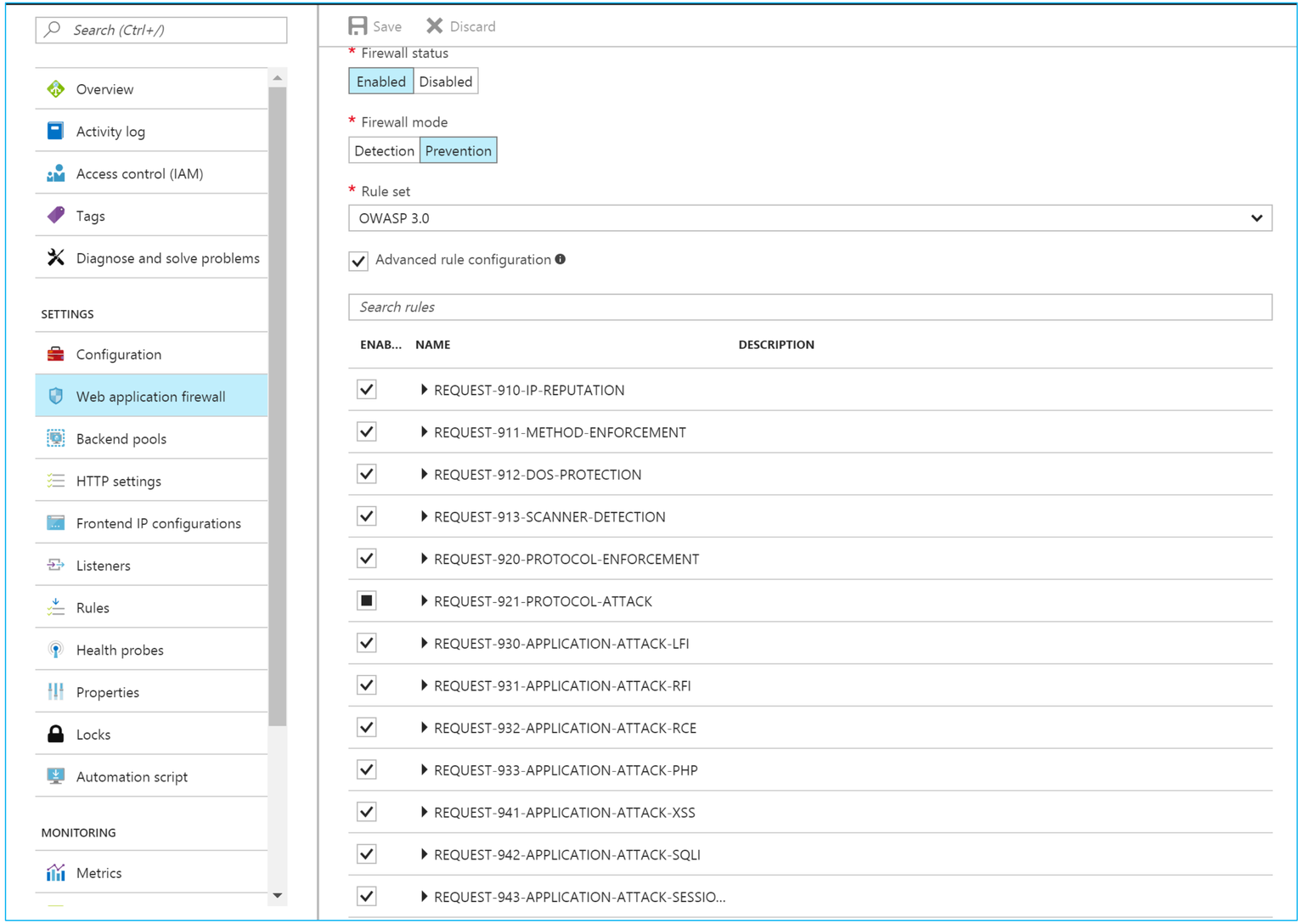
# AZURE APPLICATION GATEWAY – SSL TERMINATION



# AZURE APPLICATION GATEWAY – WAF

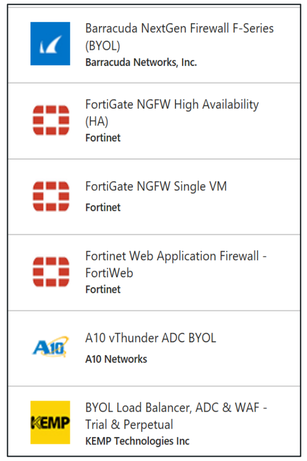


# AZURE APPLICATION GATEWAY – PRECONFIGURED WAF RULES (OWSPA 3.0 / 2.0 )



# 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



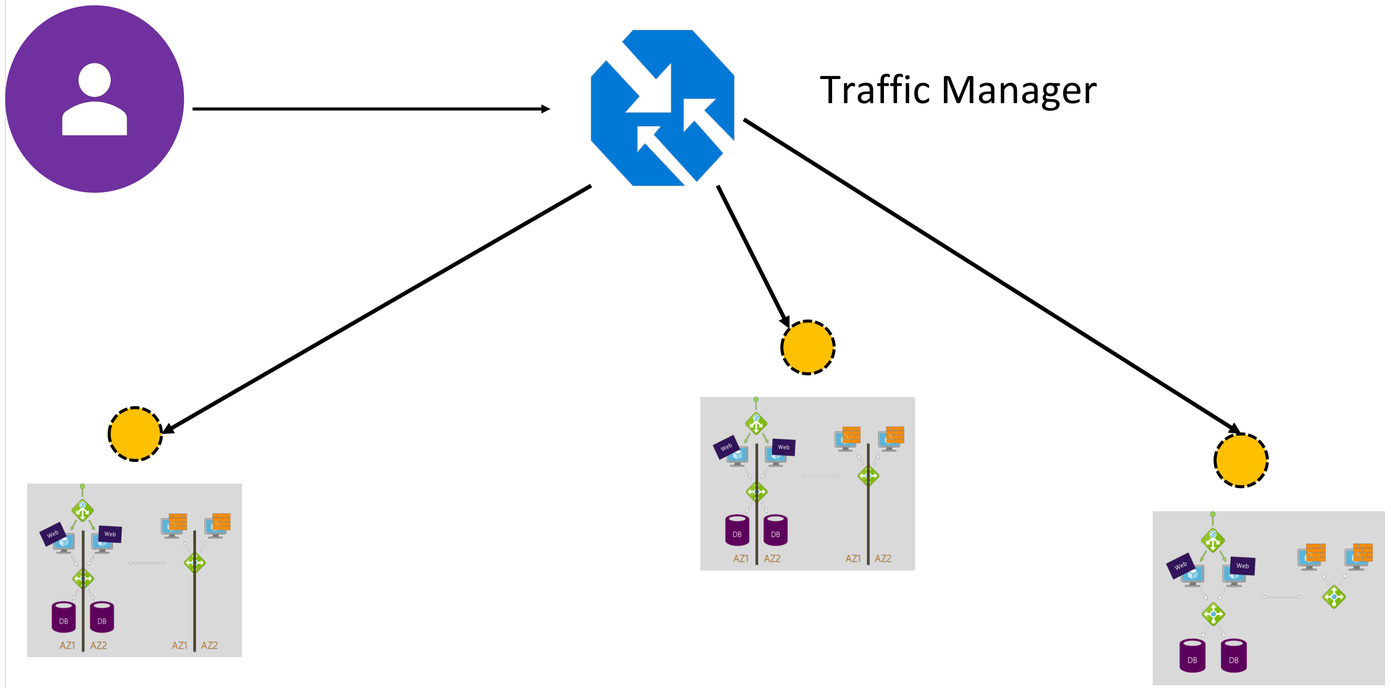

# AZURE TRAFFIC MANAGER

- 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

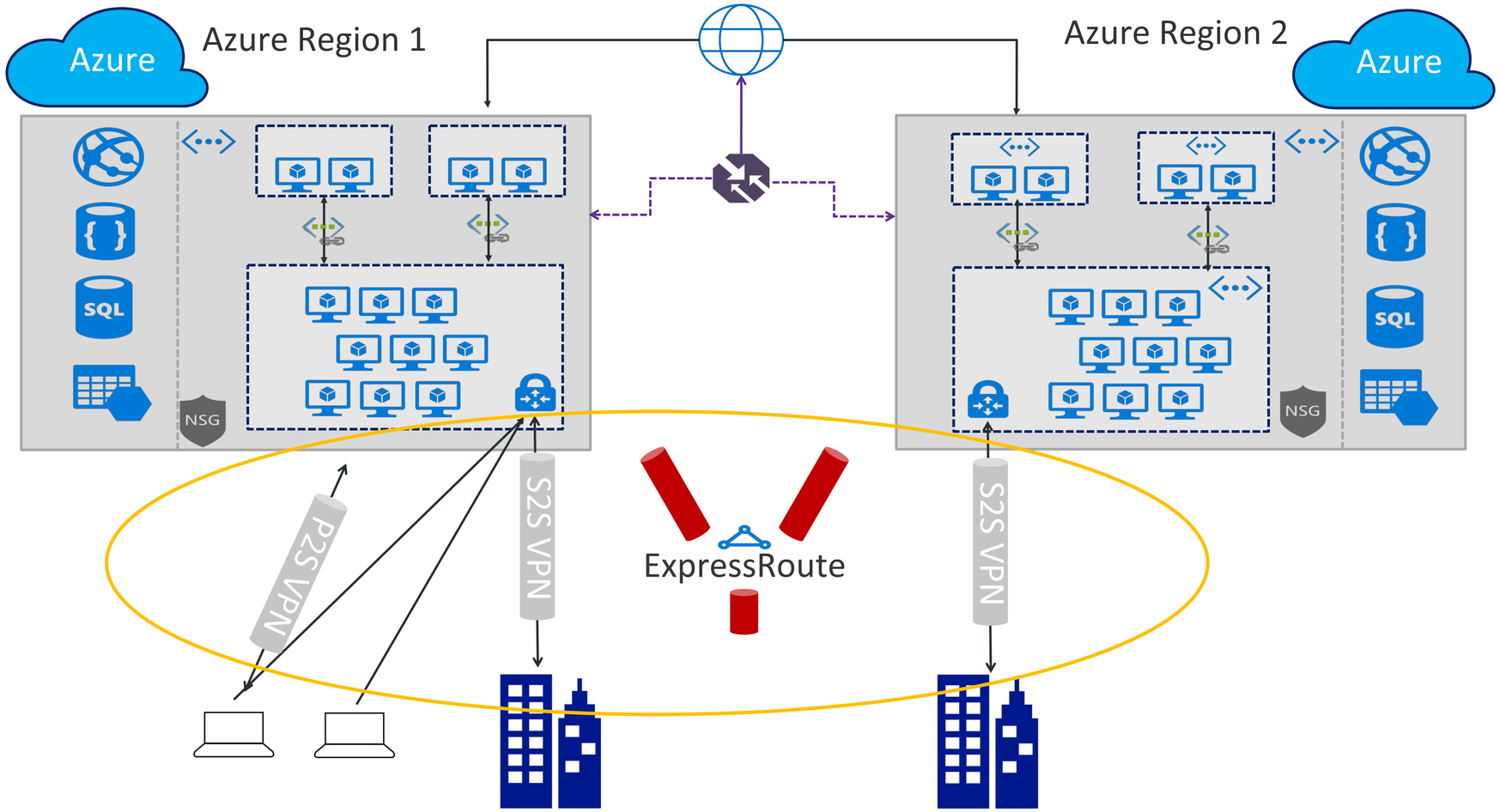
- AZURE LOAD BALANCER (LAYER 4)
- AZURE APPLICATION GATEWAY (LAYER 7)
- AZURE MARKETPLACE LOAD BALANCING APPLIANCE (LAYER 7)
- AZURE TRAFFIC MANAGER (DNS-BASED)

# EXTERNAL CONNECTIVITY

# EXTERNAL CONNECTIVTY

- 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 | ▪ ExpressRoute as primary cross-premises connectivity<br>▪ Multiple circuits for redundancy & better routing<br>▪ ExpressRoute-VPN co-existence for highly available, redundant paths<br>▪ Access to PaaS or SaaS offerings<br>▪ Dedicated ports and dedicated NAT IP’s on the datacenter site |
| Site-to-Site VPN | ▪ S2S VPN over Internet for remote branch locations<br>▪ BGP & active-active configuration for HA and transit<br>▪ Easy to deploy and cheap to maintain, fast to provision<br>▪ Very broad support for devices available |
| Point-to-Site VPN | ▪ P2S VPN for mobile users & developers to connect from anywhere with macOS & Windows<br>▪ AD/radius authentication for enterprise grade security<br>▪ Possibility to require authentication with Azure AD |

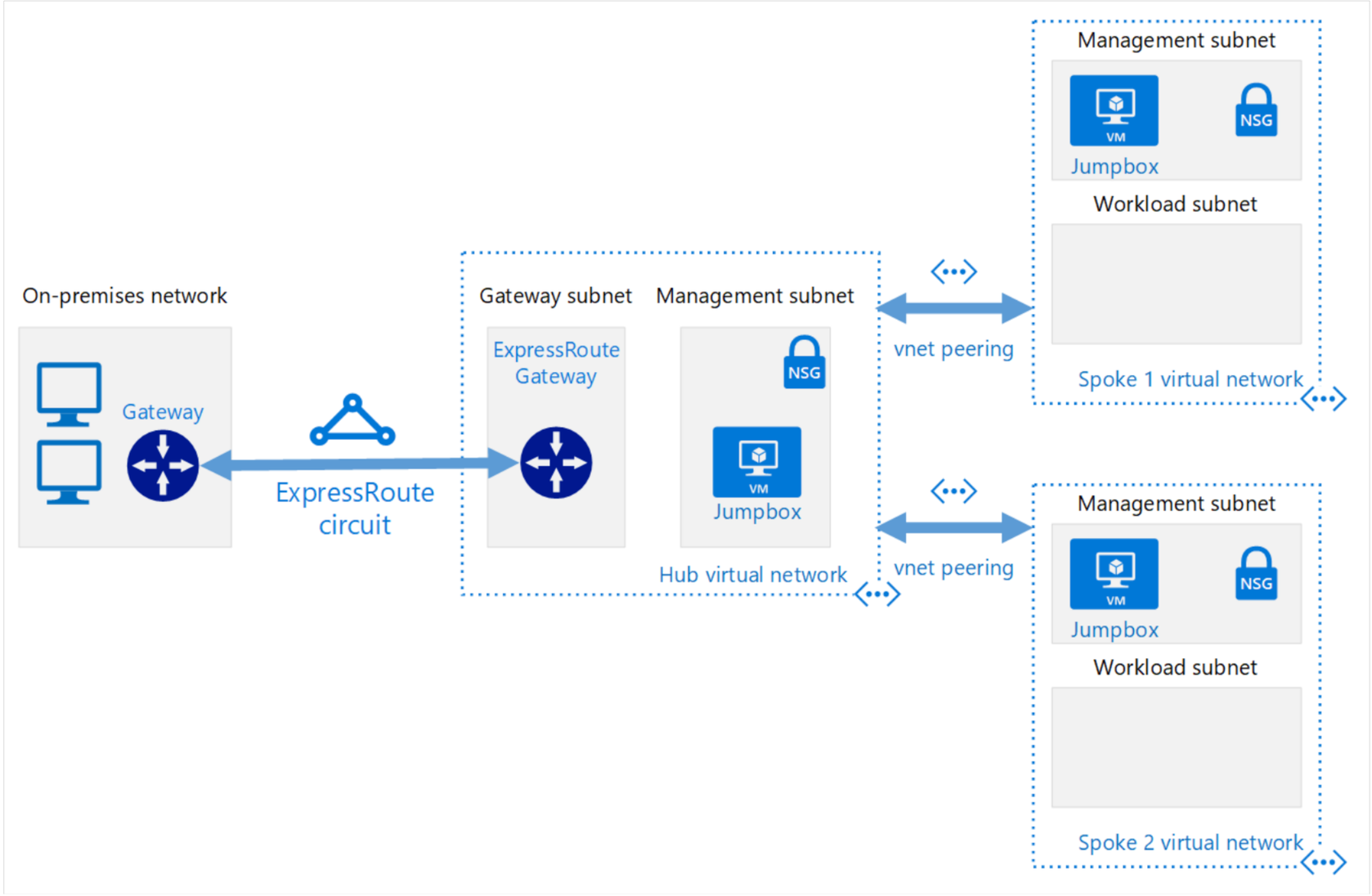
# HIGH-PERF VPN GATEWAYS

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 SSTP 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 |

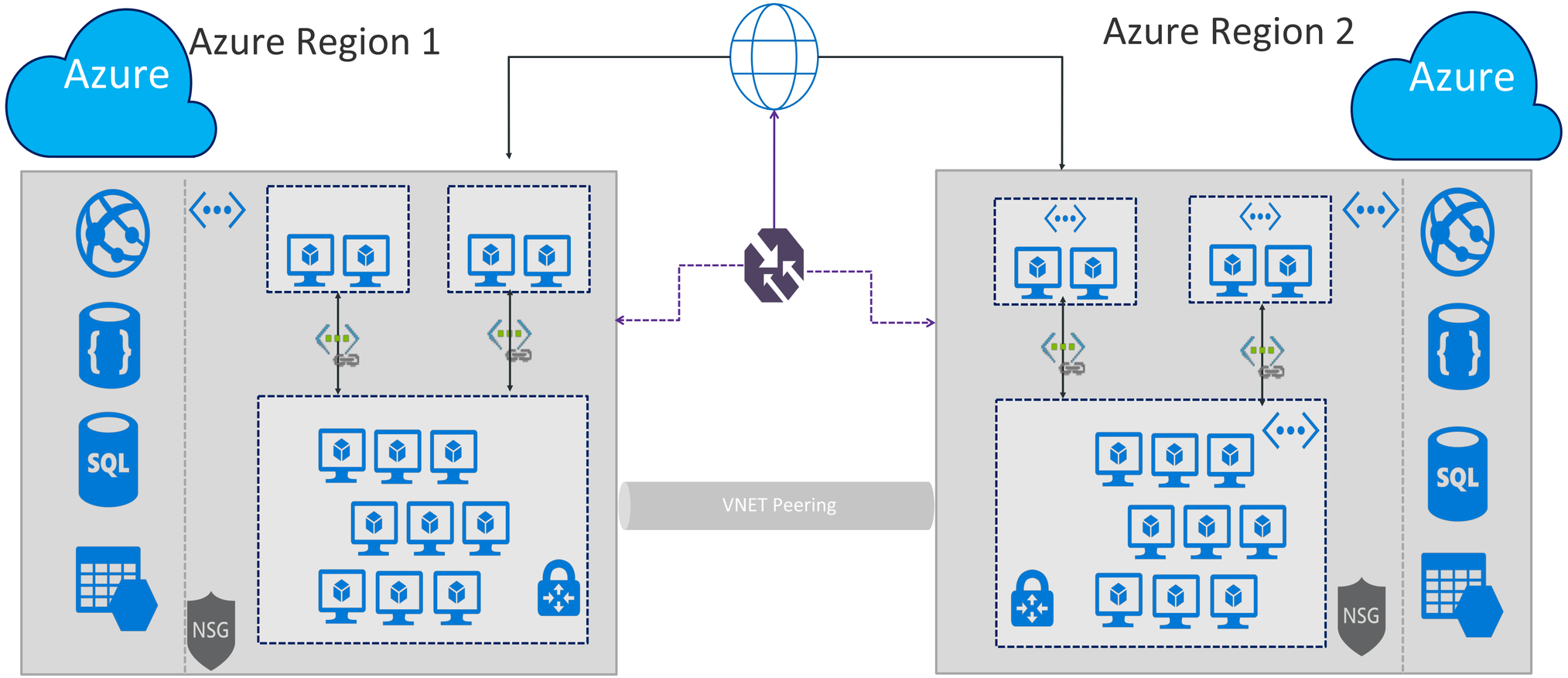
# VPN GATEWAYS ARCHITECTURE



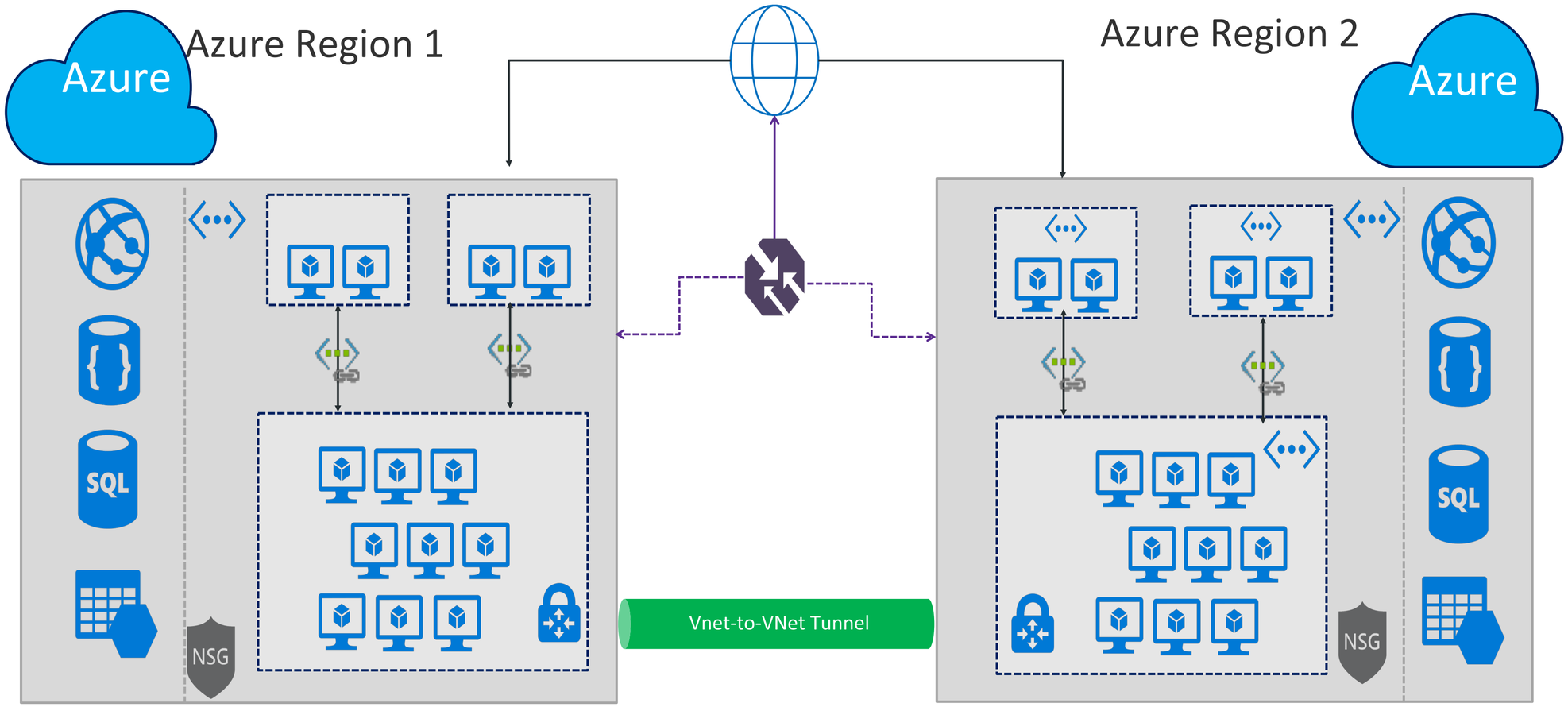
# VNET PEERING

- 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



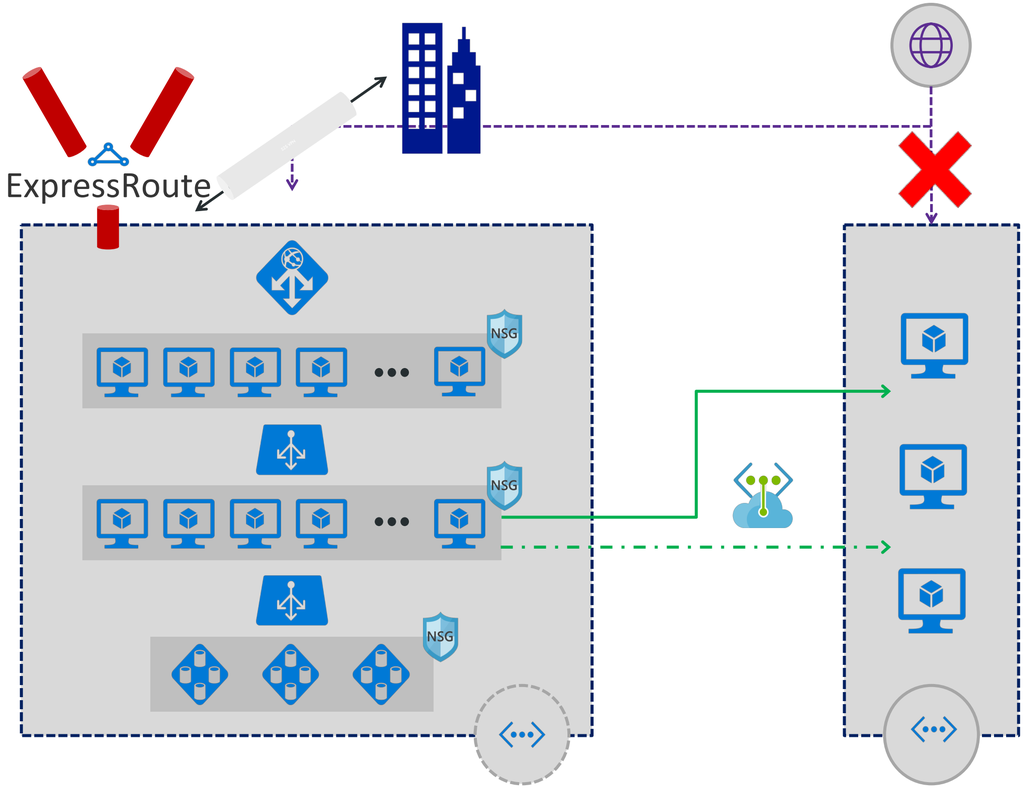
# FORCED TUNNELING

**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



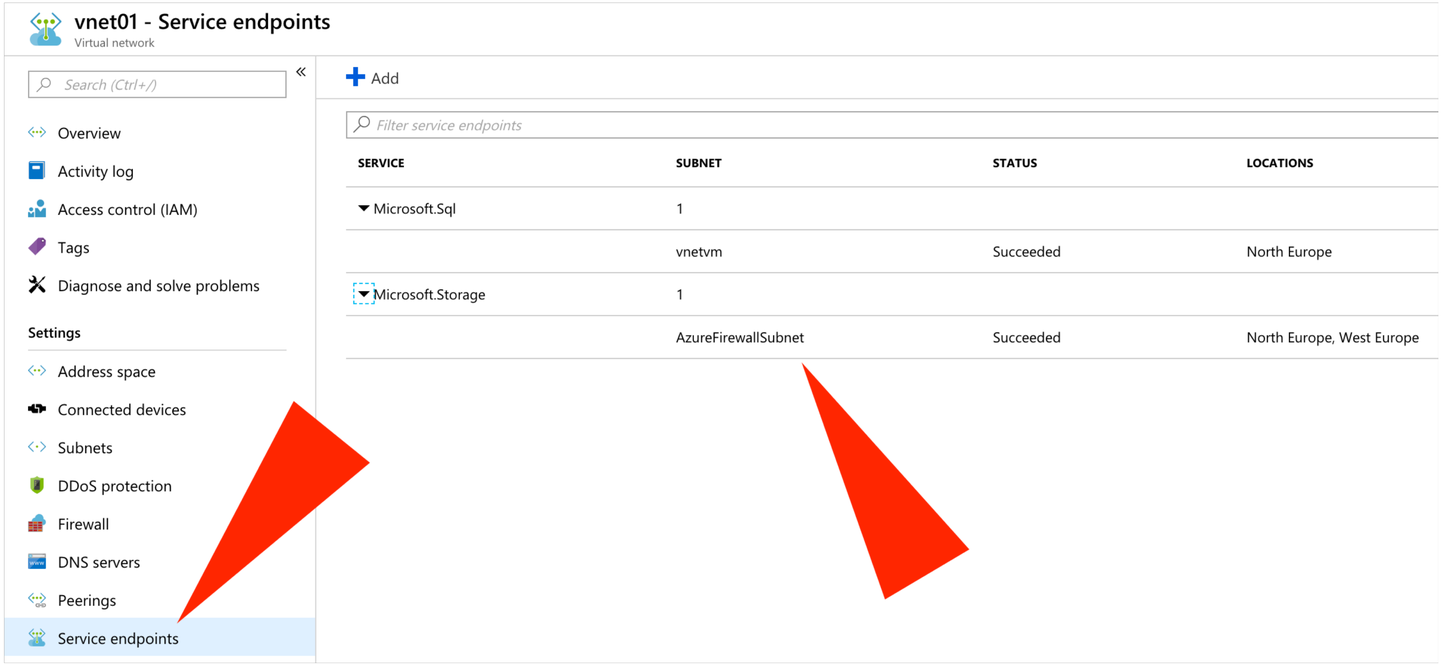
# SERVICE ENDPOINTS

**CHALLENGES:**

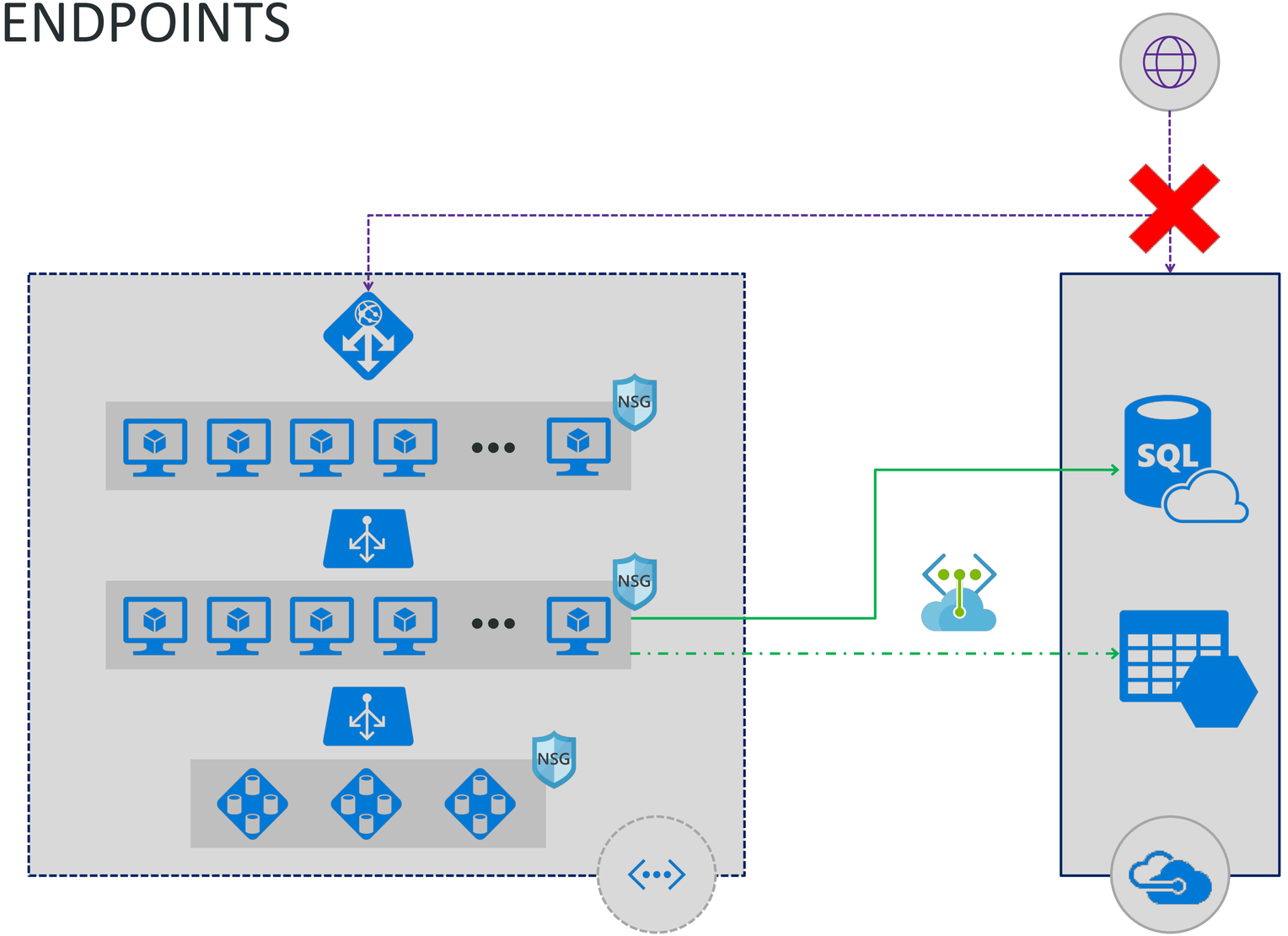
- PAAS SERVICES ACCESSIBLE THROUGH INTERNET
- CUSTOMERS MAY REQUIRE THEIR SERVICES ENDPOINTS
  TO BE ONLY ACCESSED FROM THEIR VNETS

**SOLUTION—VNET SERVICE ENDPOINTS:**

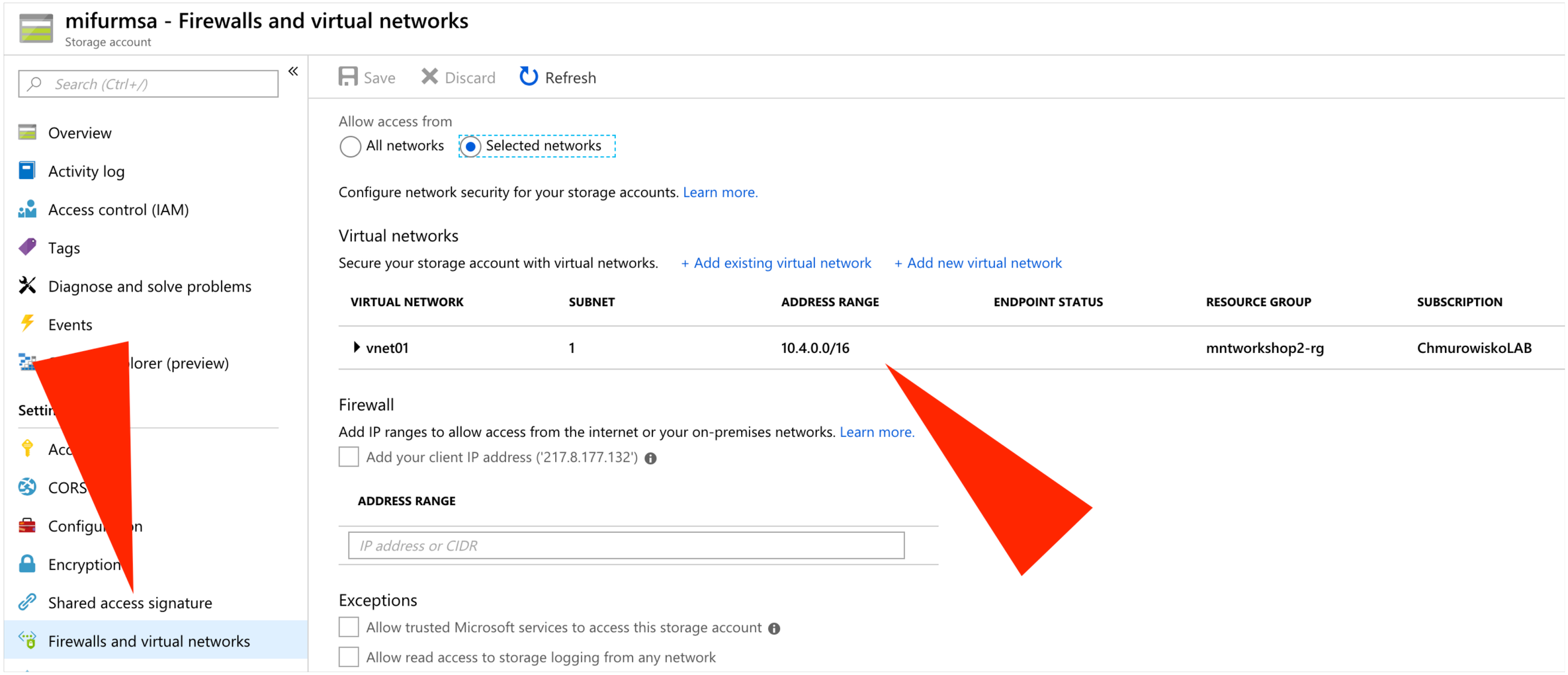
- PAAS SERVICES ONLY ACCESSIBLE FROM A VNET
- AVAILABLE NOW FOR  STORAGE, SQL DB, COSMOS DB AND MANY MORE
- WILL ROLL OUT TO OTHER PAAS SERVICES IN THE FUTURE



# SERVICE ENDPOINTS



# SERVICE ENDPOINTS




SZKOŁA CHMURY

Chmurowisko

# 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)

Impacts 0 subnets, 1 network interfaces

Add inbound port rule

| PRIORITY | NAME | PORT | PROTOCOL | SOURCE | DESTINATION | ACTION | |
|---|---|---|---|---|---|---|---|
| 300 | SSH | 22 | TCP | Any | Any | Allow | ... |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow | ... |
| 65001 | AllowAzureLoadBalancerInB... | Any | Any | AzureLoadBal... | Any | Allow | ... |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny | ... |

# NETWORK SECURITY GROUPS – OUTBOUND RULES

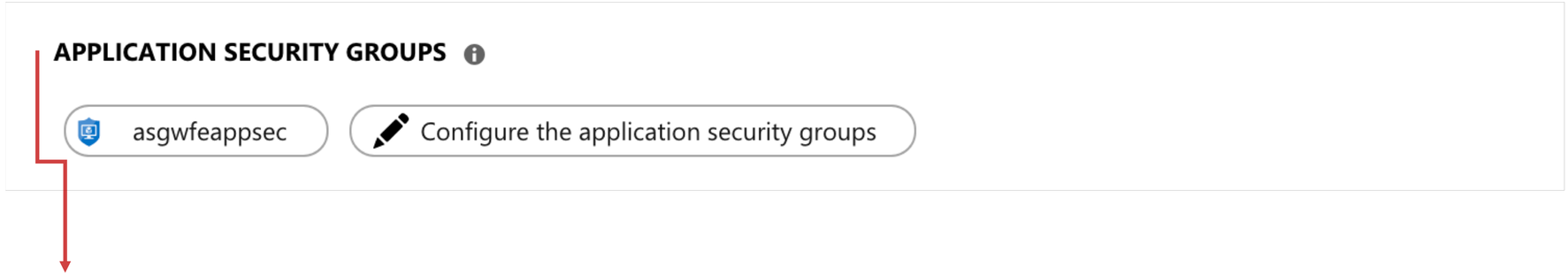
**OUTBOUND PORT RULES**

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

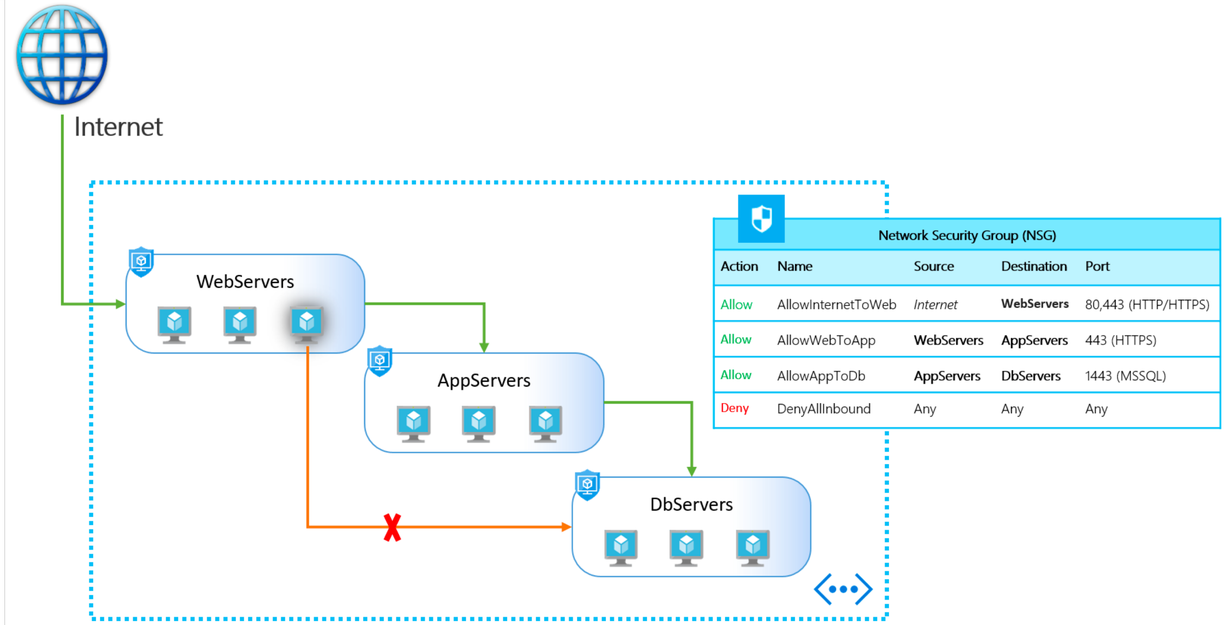
Add outbound port rule

| PRIORITY | NAME | PORT | PROTOCOL | SOURCE | DESTINATION | ACTION |
|---|---|---|---|---|---|---|
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow ... |
| 65001 | AllowInternetOutBound | Any | Any | Any | Internet | Allow ... |
| 65500 | DenyAllOutBound | Any | Any | Any | Any | Deny ... |

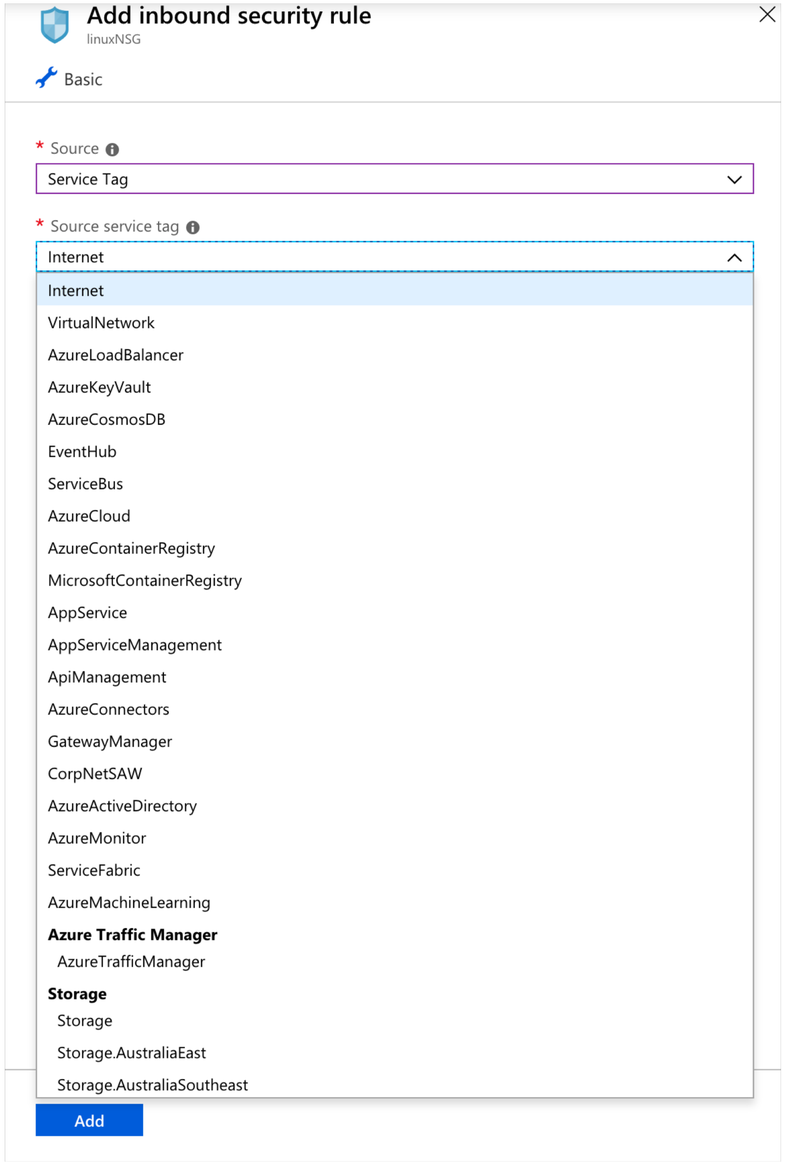
# APPLICATION SECURITY GROUPS




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4096 | denyall | Any | Any | asgwfeapp... | asgwfeapp... | Deny | ... |



# SERVICE TAGS



# SECURING CONNECTIVITY - SUMMARY

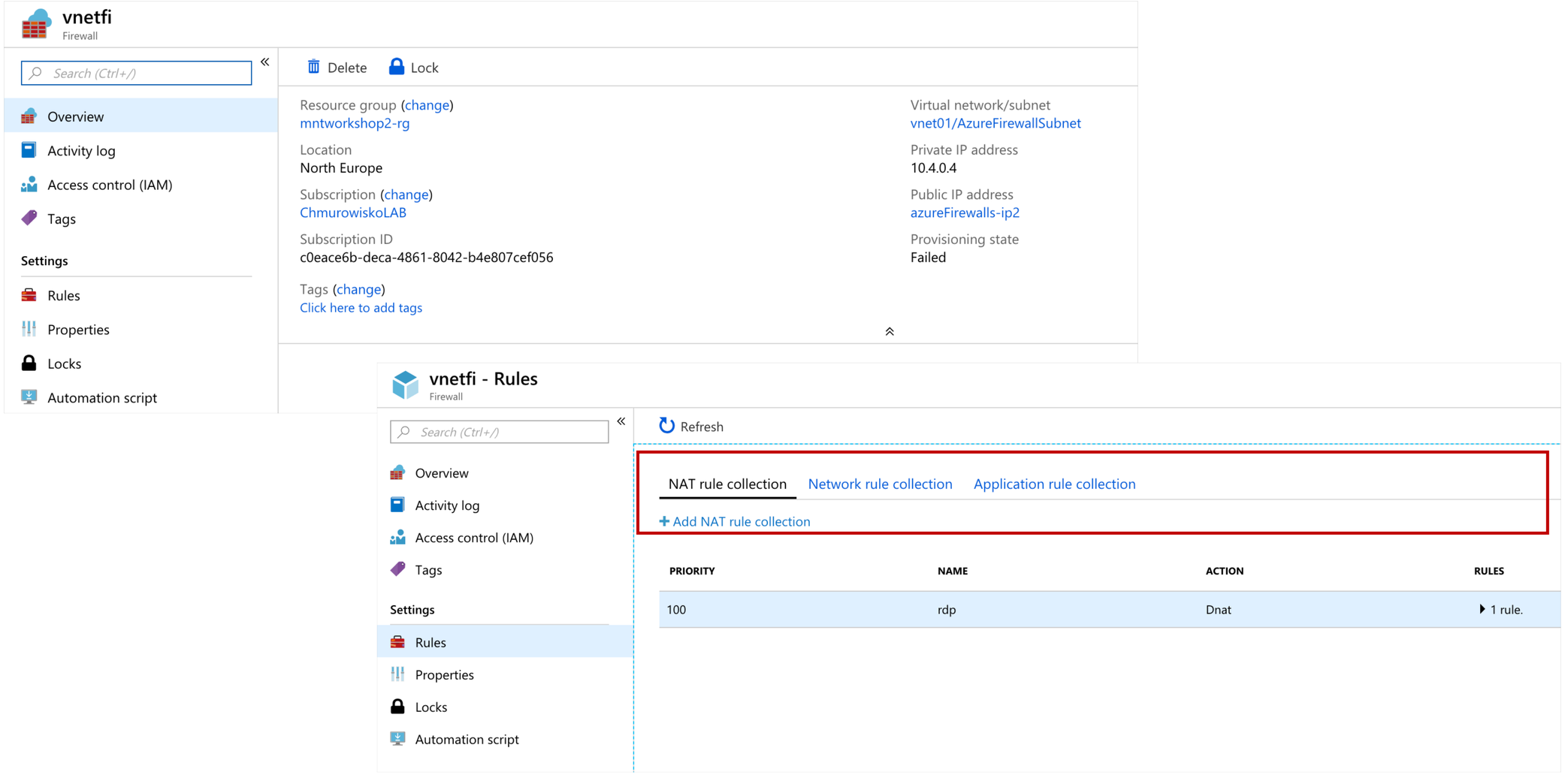
- NETWORK SECURITY GROUPS
- APPLICATION SECURITY GROUPS
- SERVICE TAGS

# OTHER SERVICES

# OTHER SERVICES

- AZURE FIREWALL
- AZURE NETWORK WATCHER
- AZURE DDOS

# AZURE FIREWALL

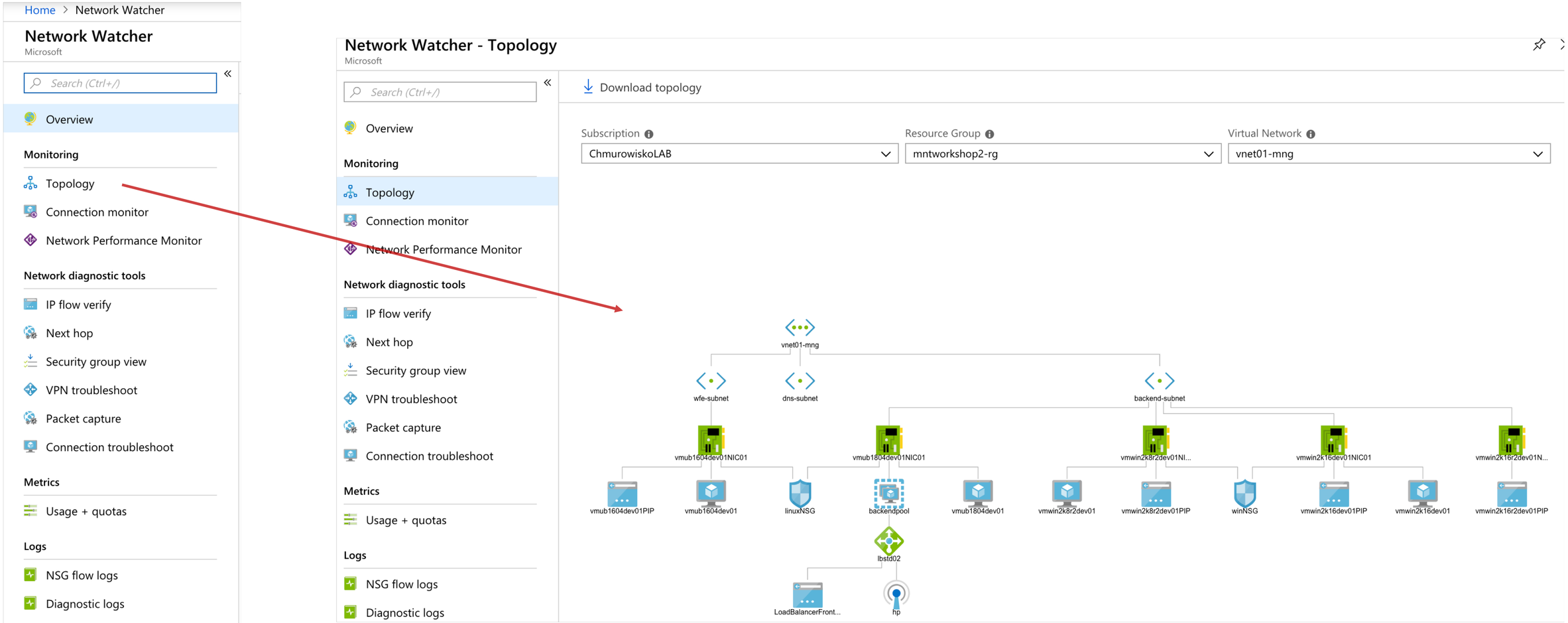



SZKOŁA CHMURY

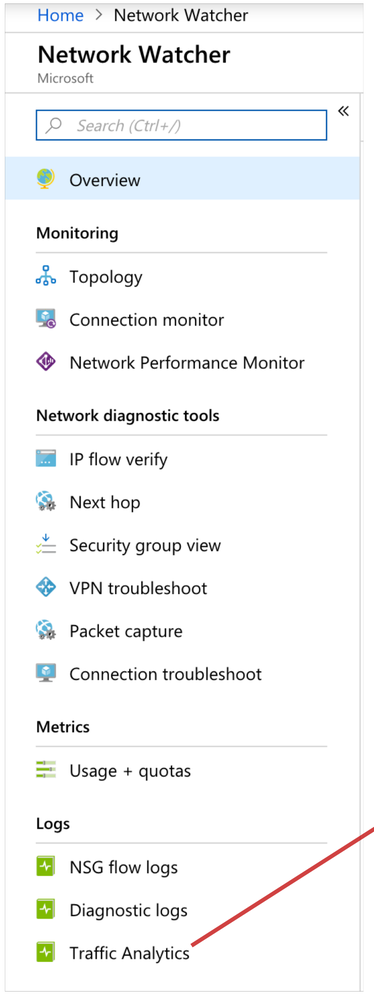
Chmurowisko

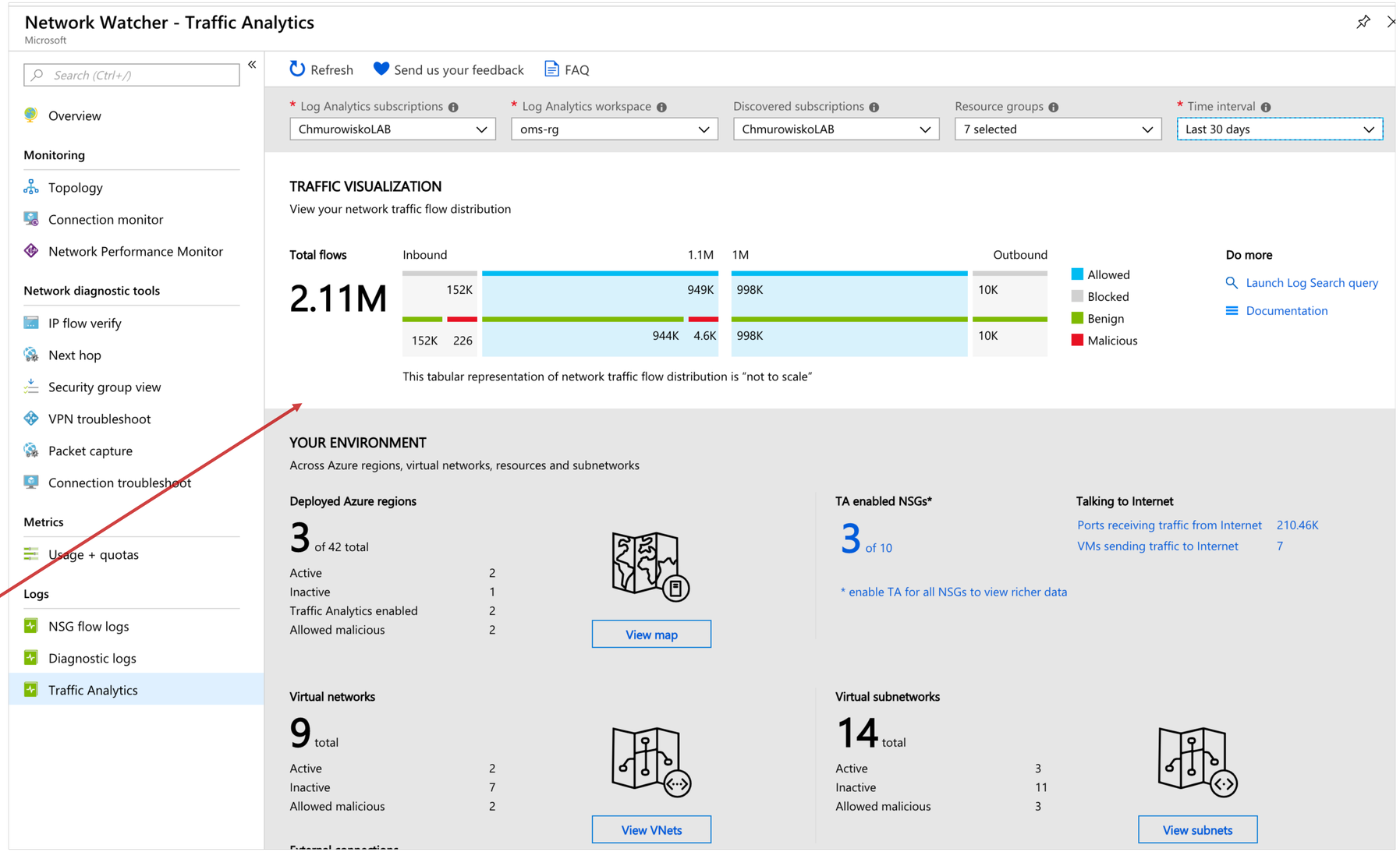
# AZURE FIREWALL

# AZURE NETWORK WATCHER



# AZURE NETWORK WATCHER

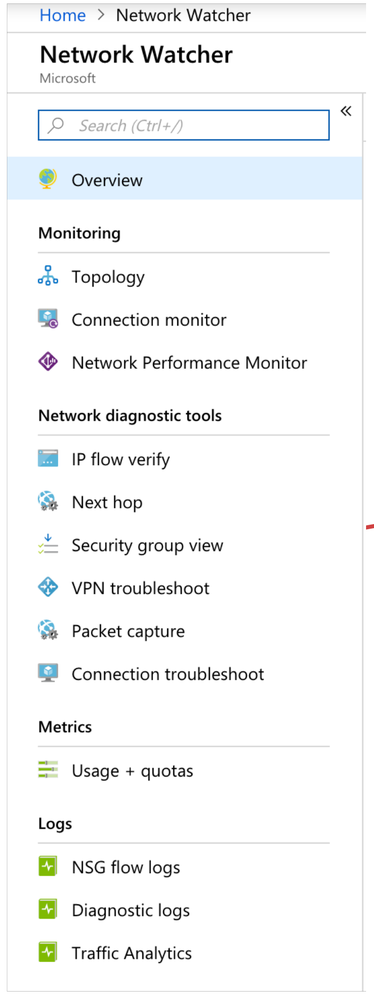


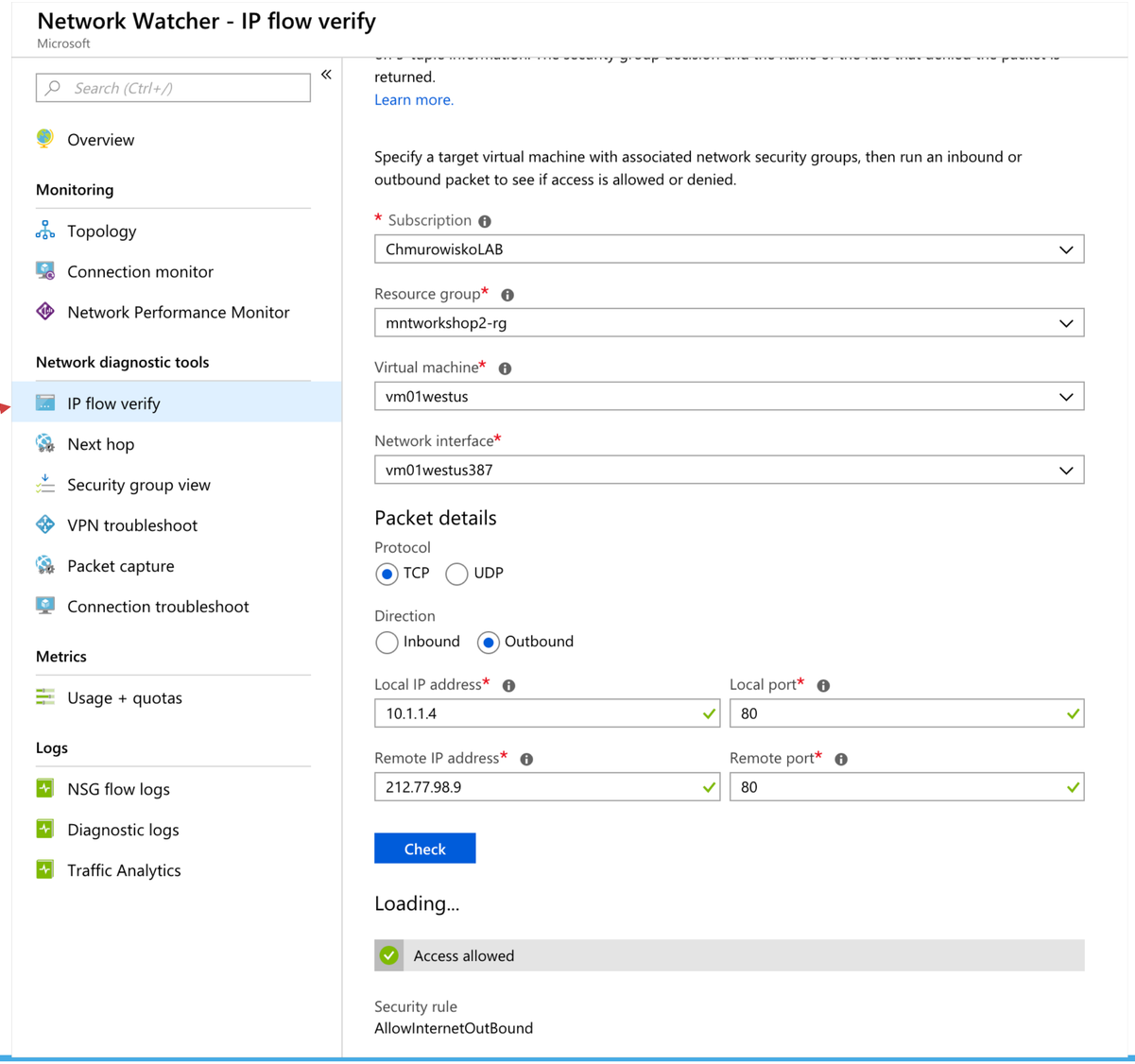




SZKOŁA CHMURY

Chmurowisko

# AZURE NETWORK WATCHER – IP FLOW VERIFY

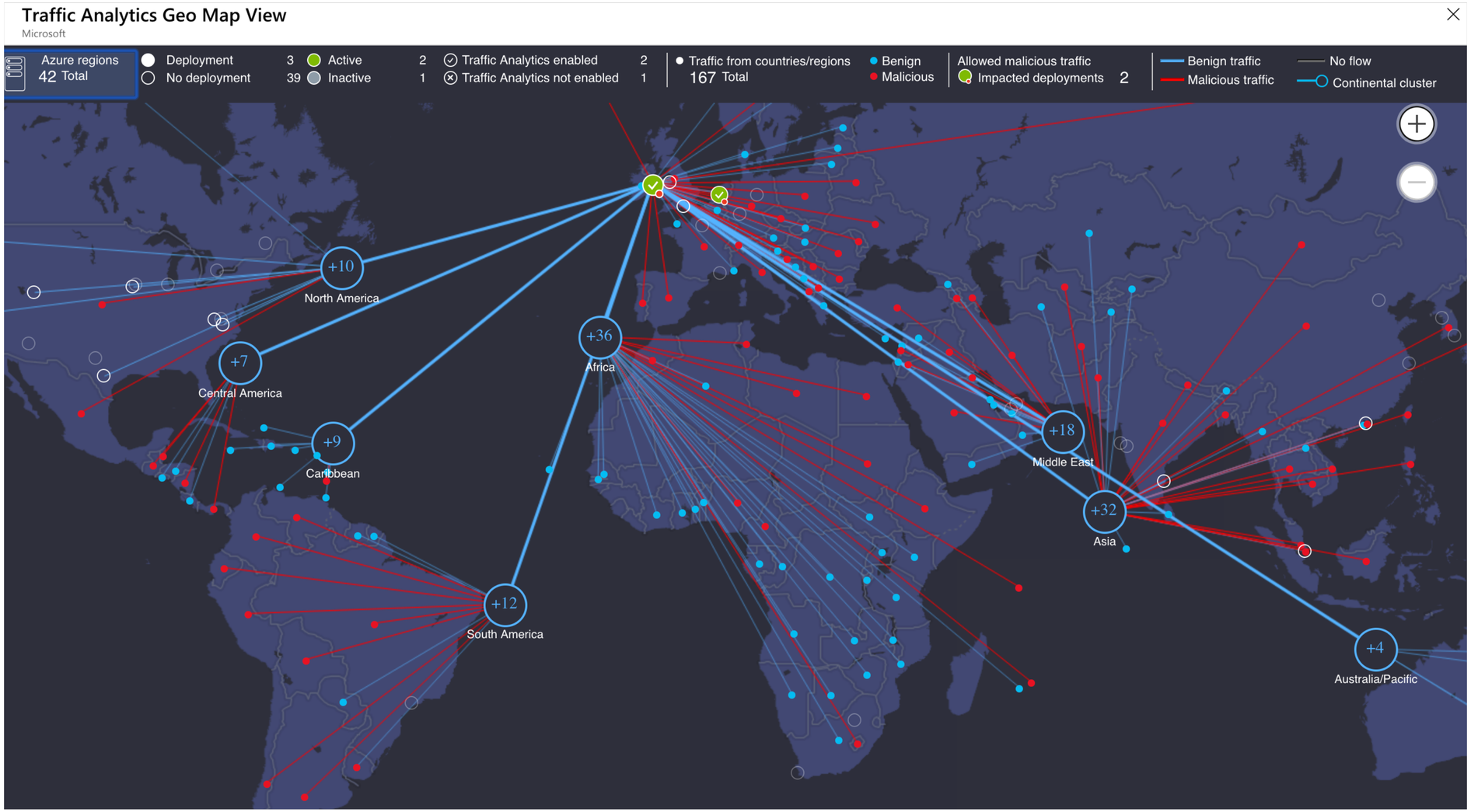


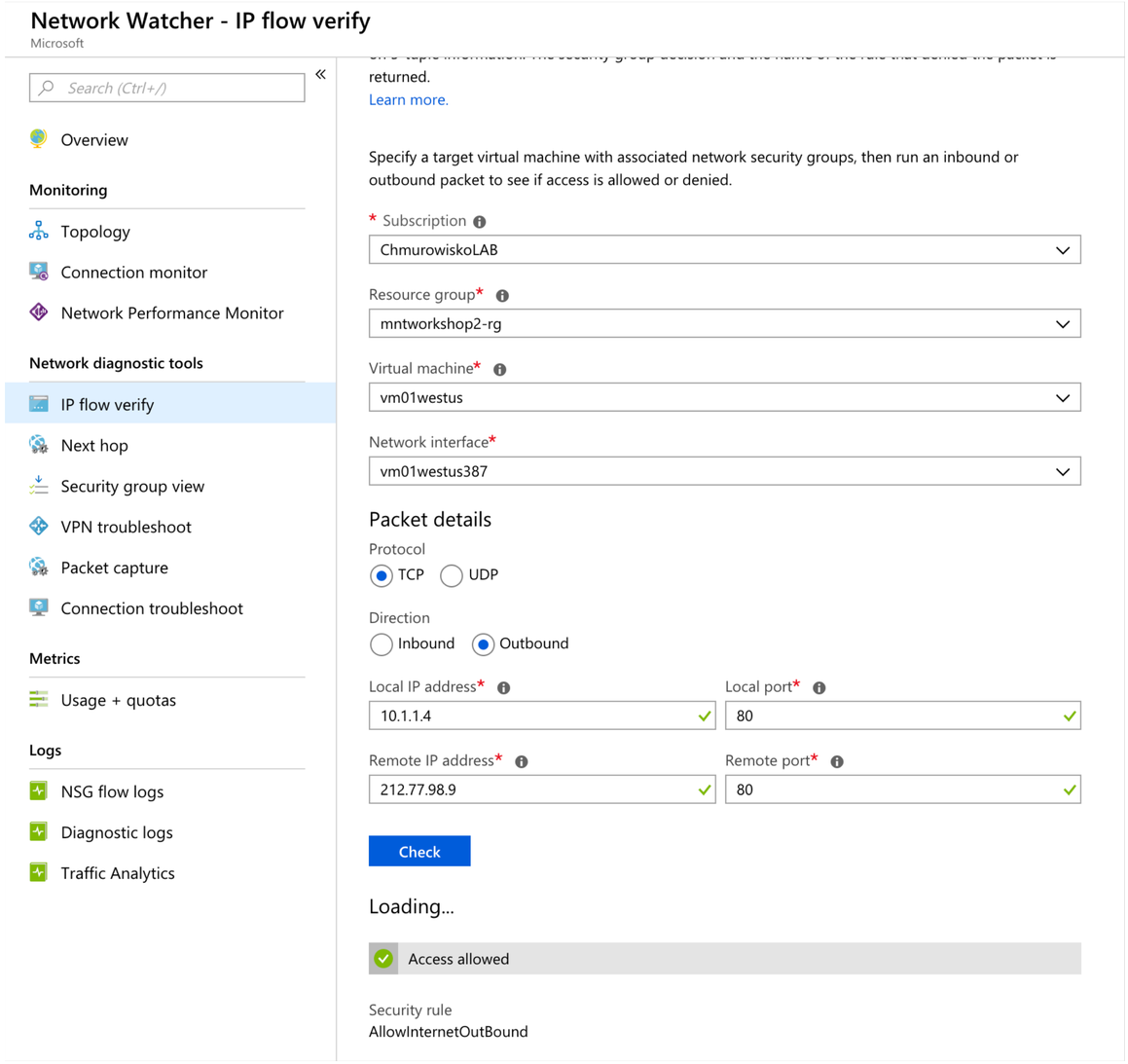

SZKOŁA CHMURY

Chmurowisko

# AZURE NETWORK WATCHER



# AZURE NETWORK WATCHER – TRAFFIC ANALYTICS




SZKOŁA CHMURY

Chmurowisko

# OTHER SERVICES - SUMMARY

- AZURE FIREWALL
- AZURE NETWORK WATCHER
- AZURE DDOS