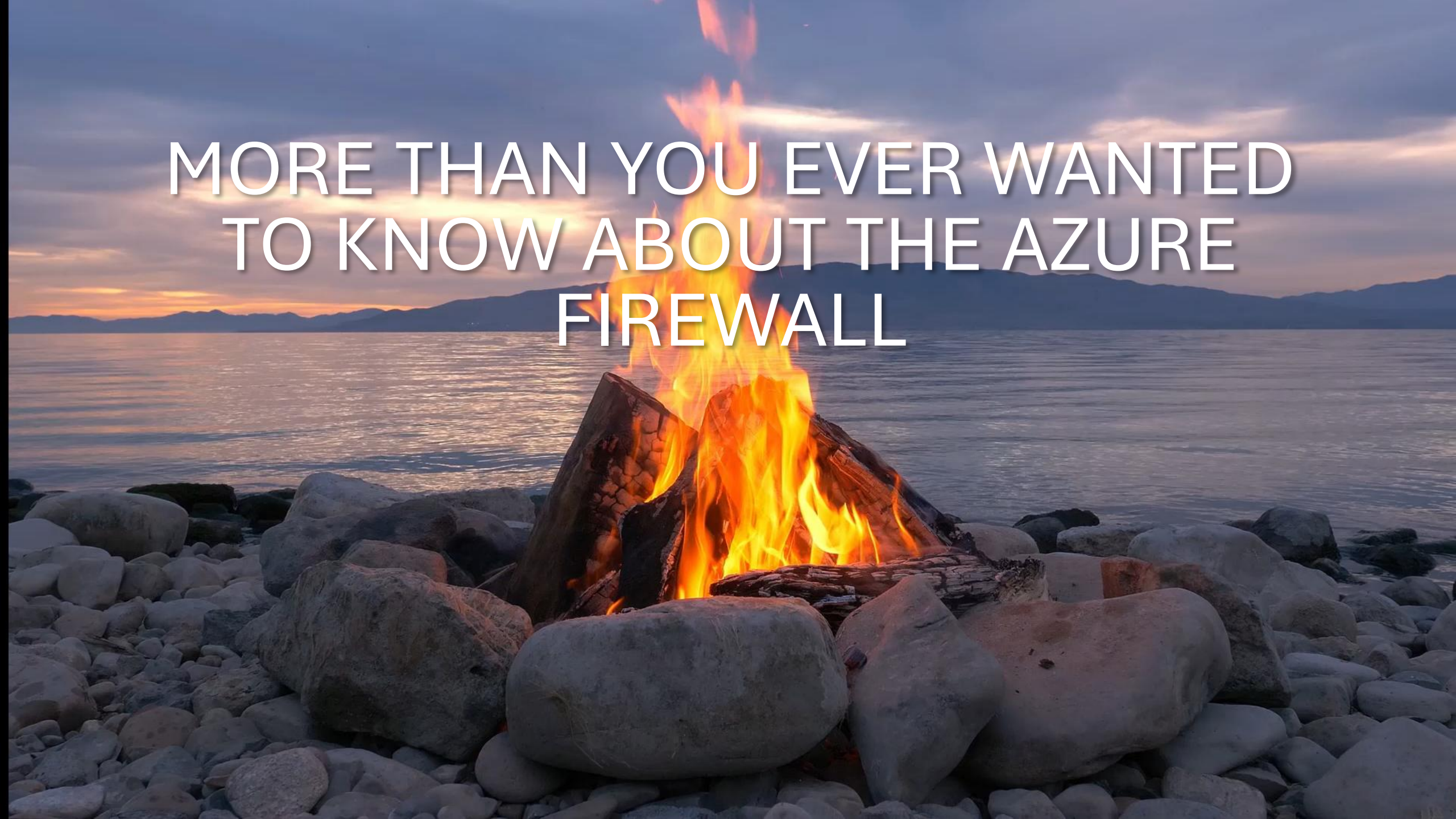

MORE THAN YOU EVER WANTED
TO KNOW ABOUT THE AZURE
FIREWALL

YOUR RESIDENT NUTCASES

Edward Verweij

Principal Consultant at Strict

About me

Passion for Cloud Infrastructure, Security and Networking

Interests:

- Azure
- Security
- Networking,
- Skiing
- Formula 1

Expertise

- Azure Infrastructure
- DNS
- Firewall’s
- Cloud Identity
- Security
- Automation
- Architecture & Design
- Governance
- Networking

Marc Dekeyser

Sr. Customer Experience Engineer

Who me?

Cloud Obsessed with experience since 2004 over 4 continents and multiple industries.

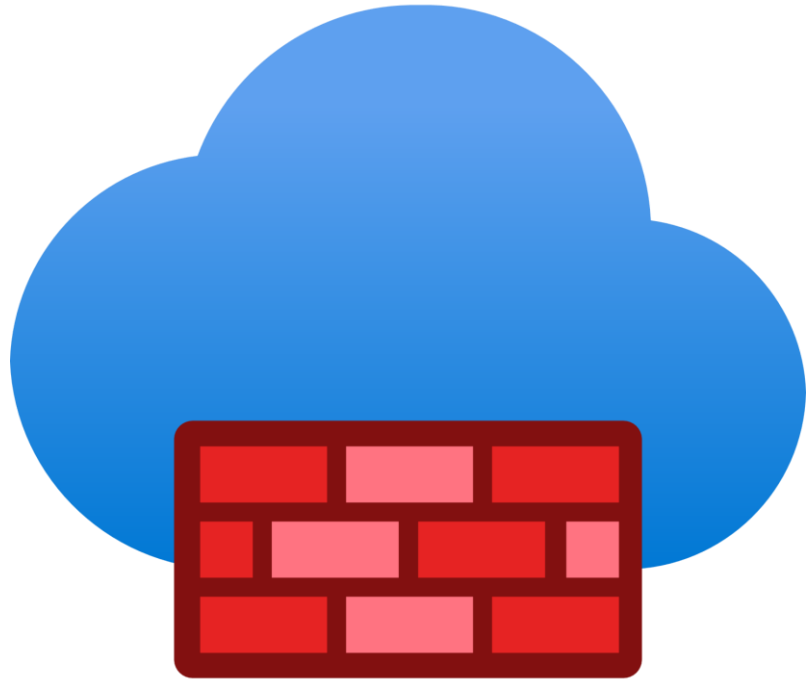
- Tinkerer & Evil Mastermind
- Microsoftie since 2012
- Azure Worldwide Communities SME
- Diversity & Inclusion Advisor
- Primary audience: Start-ups!

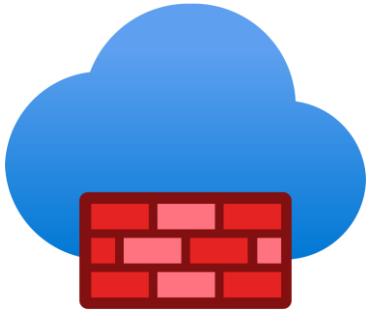
Expertise

- Azure Infrastructure
- Azure Containers
- Azure Kubernetes
- Cloud Identity
- Security
- Automation
- Architecture & Design
- Governance
- Cost Management

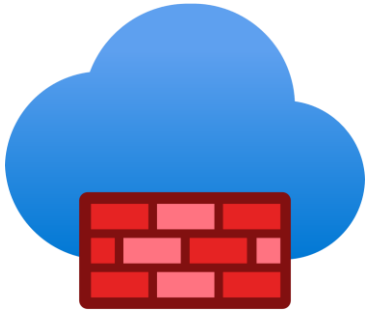
Dare** to be **Authentic**, **Curious**, and **Passionate

AZURE FIREWALL

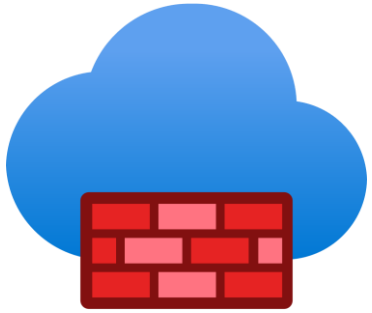




Firewall Basic



Firewall Standard



Firewall Premium

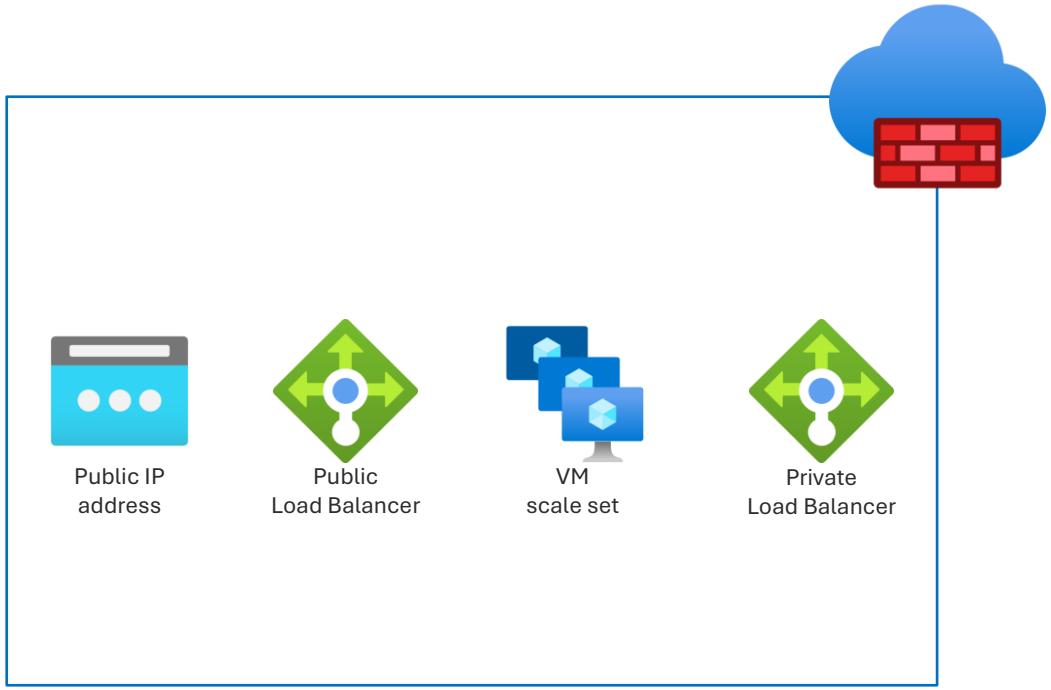
Feature Category	Feature	Firewall Basic	Firewall Standard	Firewall Premium
L3-L7 Filtering	Application level FQDN filtering (SNI based) for HTTPS/SQL	✓	✓	✓
	Network level FQDN filtering – all ports and protocols		✓	✓
	Stateful firewall (5 tuple rules)	✓	✓	✓
	Network Address Translation (SNAT+DNAT)	✓	✓	✓
Reliability & Performance	Availability zones	✓	✓	✓
	Built-in HA	✓	✓	✓
	Cloud scalability (auto-scale as traffic grows)	Up to 250Mbps	Up to 30 Gbps	Up to 100 Gbps
	Fat Flow support	N/A	1 Gbps	10 Gbps
Ease of Management	Central management via Firewall Manager	✓	✓	✓
	Policy Analytics (Rule Management over time)	✓	✓	✓
Enterprise Integration	Full logging including SIEM integration	✓	✓	✓
	Service Tags and FQDN Tags for easy policy management	✓	✓	✓
	Easy DevOps integration using REST/PS/CLI/Templates/ Terraform	✓	✓	✓
	Web content filtering (web categories)		✓	✓
	DNS Proxy + Custom DNS		✓	✓
Advanced Threat Protection	Threat intelligence-based filtering (known malicious IP address/ domains)	Alert	✓	✓
	Inbound TLS termination (TLS reverse proxy)			Using App GW
	Outbound TLS termination (TLS forward proxy)			✓
	Fully managed IDPS			✓
	URL filtering (full path - incl. SSL termination)			✓

COMPARING AZ FW TO OTHER FW'S

Scalability

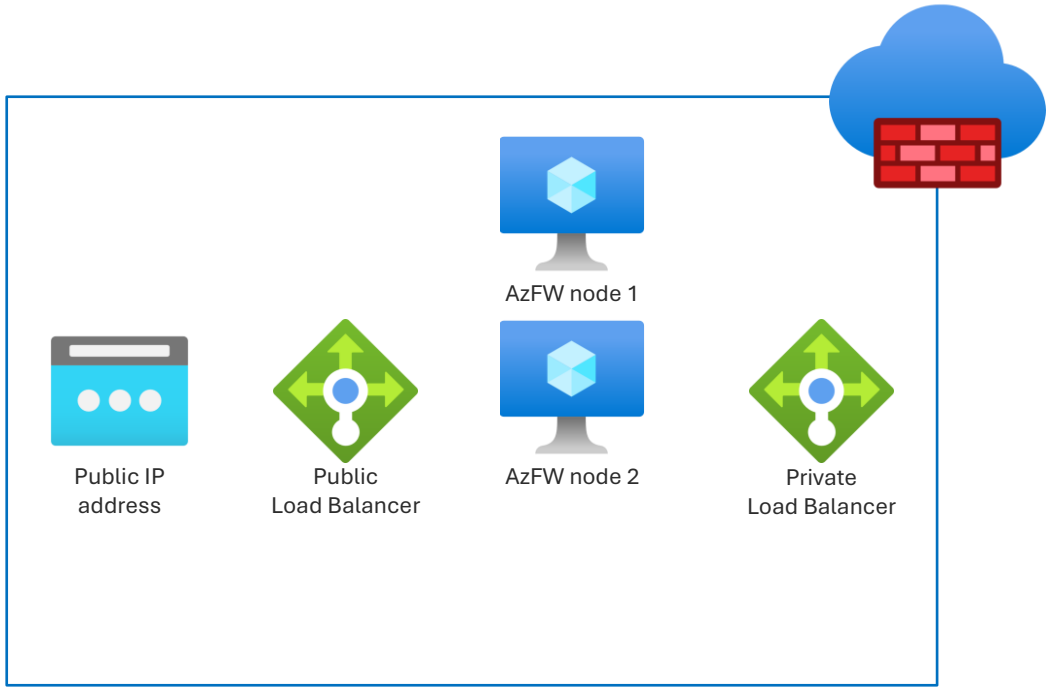
AZURE FIREWALL SCALING

AZURE FIREWALL SCALING



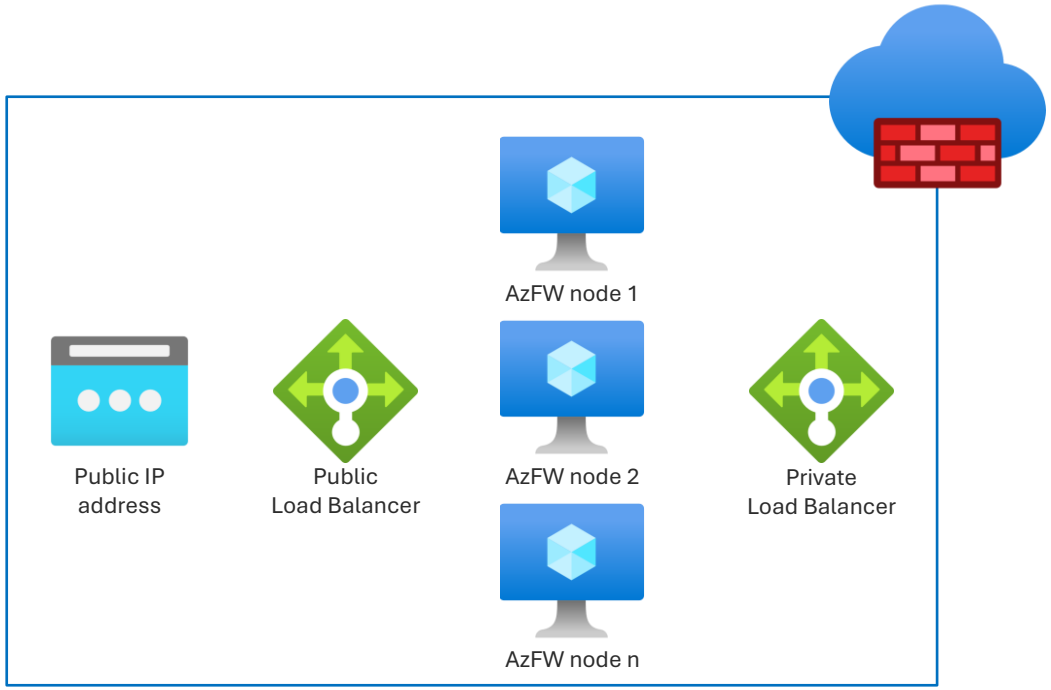
- Azure Firewall underlying architecture.

AZURE FIREWALL SCALING



- Scales out at 60% CPU consumption.
- Or number of connections is at 80%.

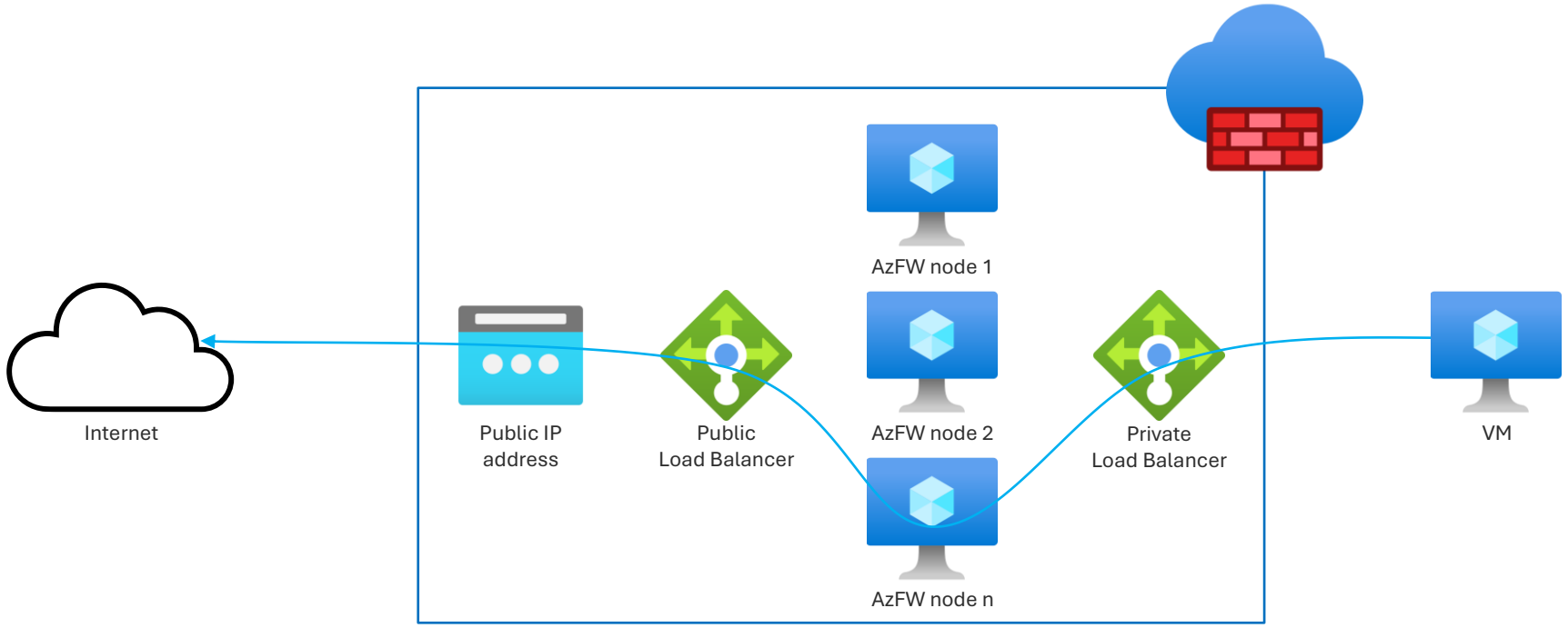
AZURE FIREWALL SCALING



- Scales in below 20% CPU consumption or the number of connections.
- Max bandwidth for single TCP connection 1,5 Gbps Standard or 9 Gbps Premium (6x).

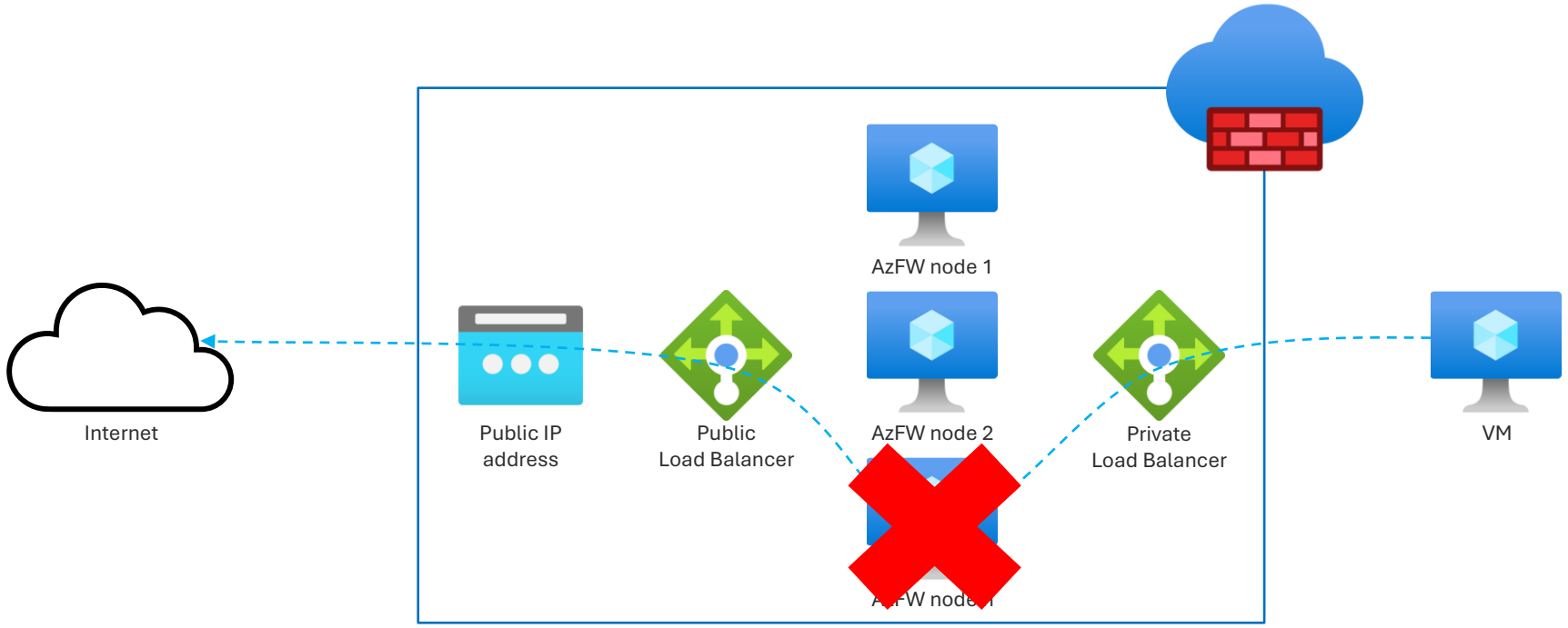
AZURE FIREWALL
TCP TRAFFIC TIMEOUT

TCP TRAFFIC TIMEOUT



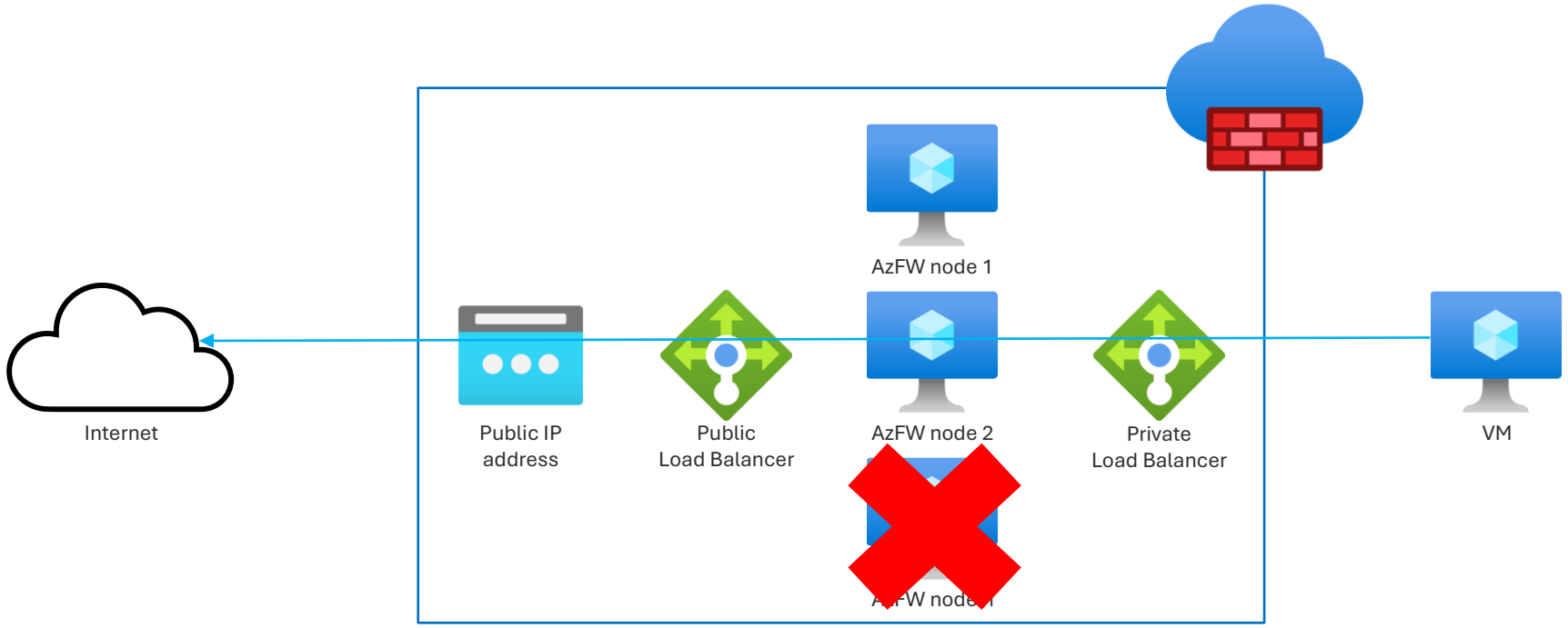
- Default TCP idle timeout of 4 minutes.
- The timeout can be set between 4 and 15 minutes via a support request.

TCP TRAFFIC TIMEOUT



- Azure Firewall can terminate long-running TCP sessions due to scale-in.

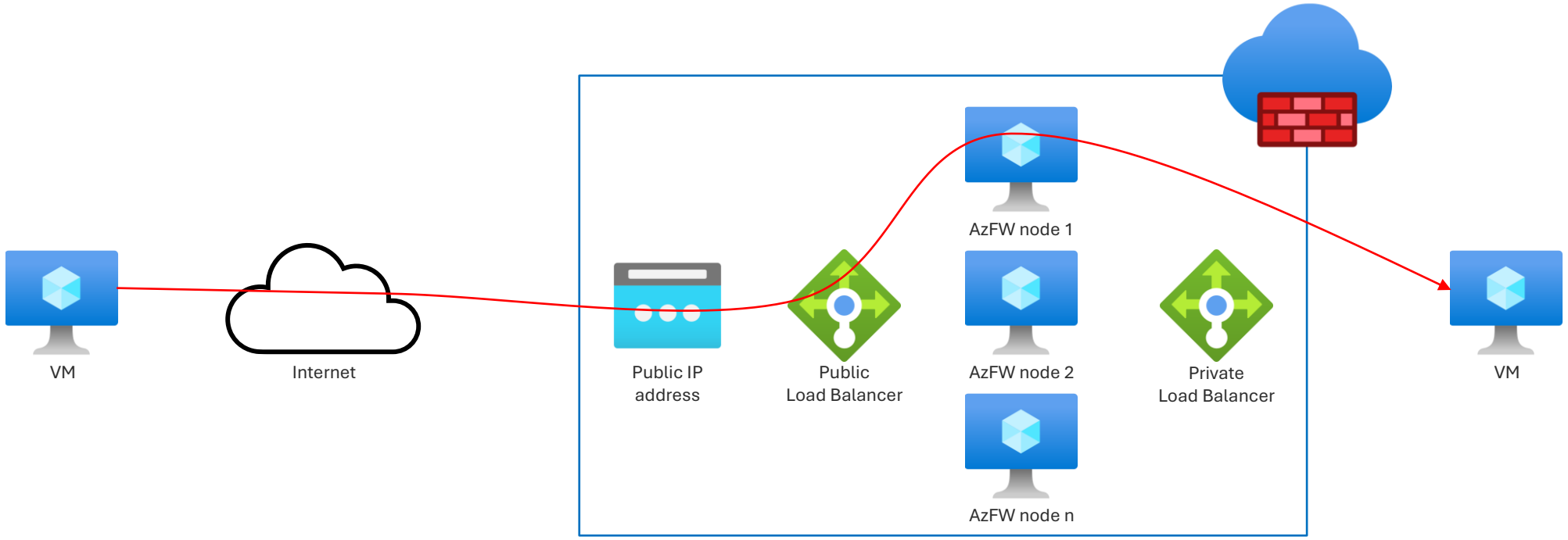
TCP TRAFFIC TIMEOUT



- Applications like SSH, RDP, VPN and database connections are sensitive to TCP session resets.

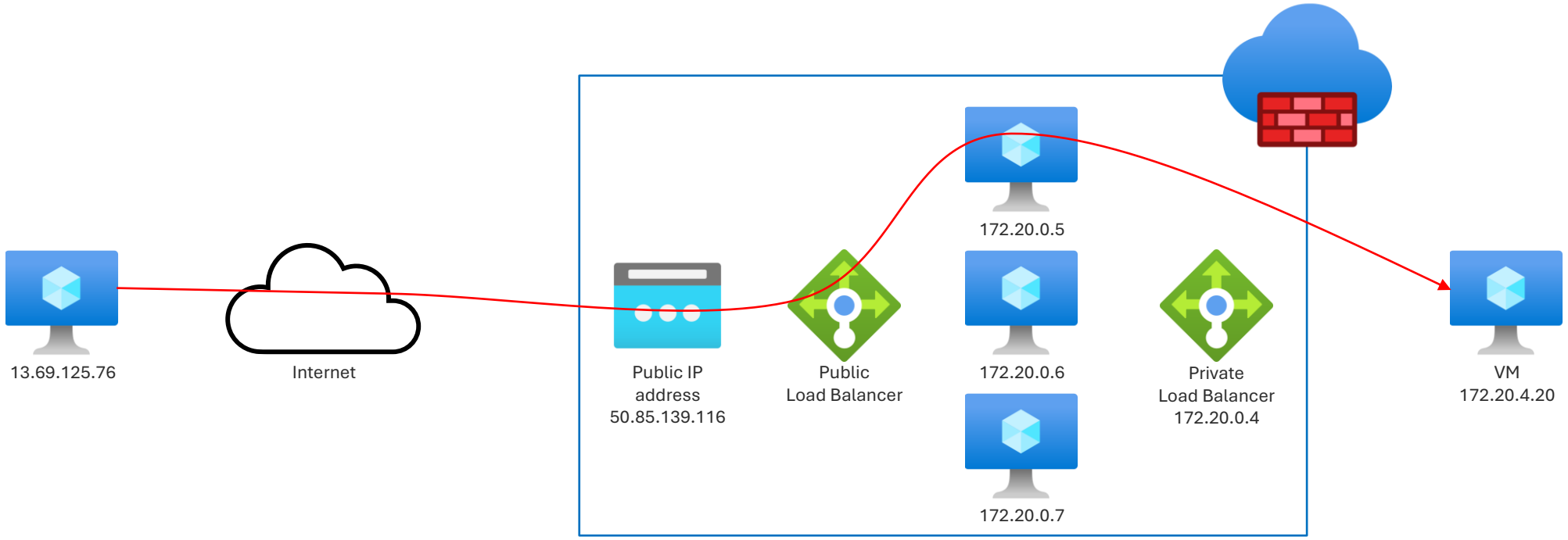
AZURE FIREWALL DNAT
DESTINATION NETWORK ADDRESS TRANSLATION

DNAT



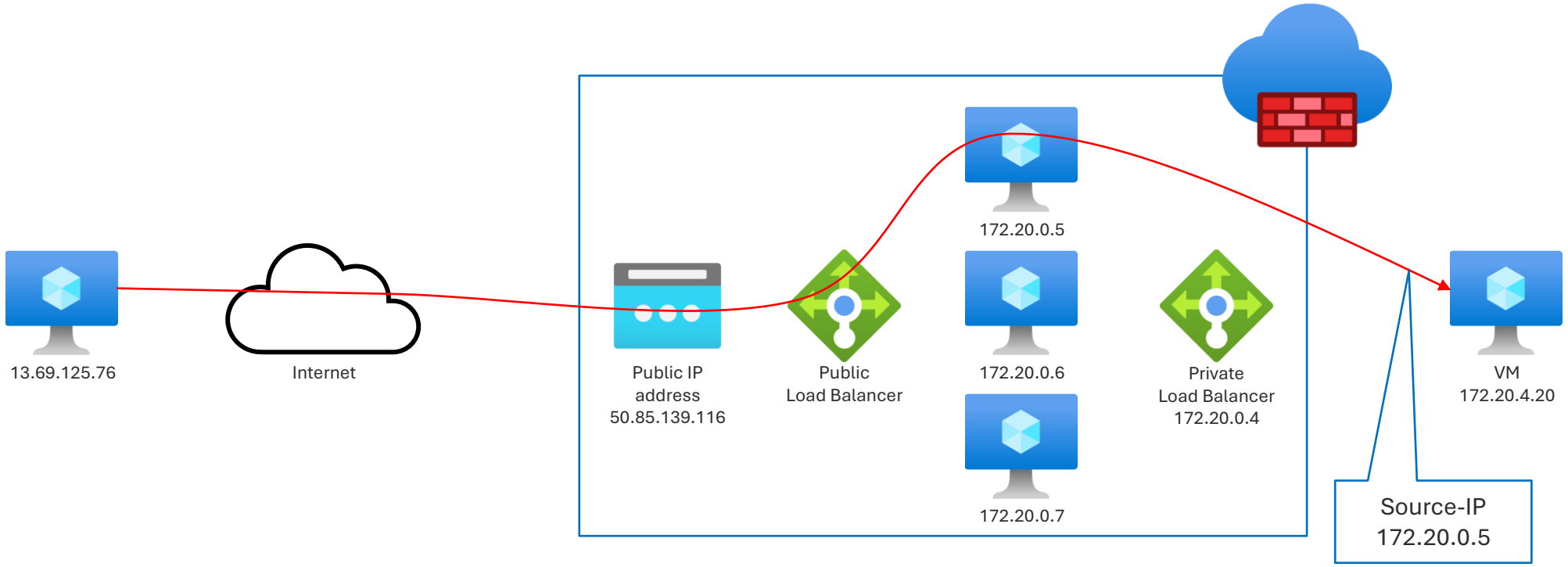
- DNAT filters and translates inbound Internet traffic by translating the firewall's public IP Address.

DNAT



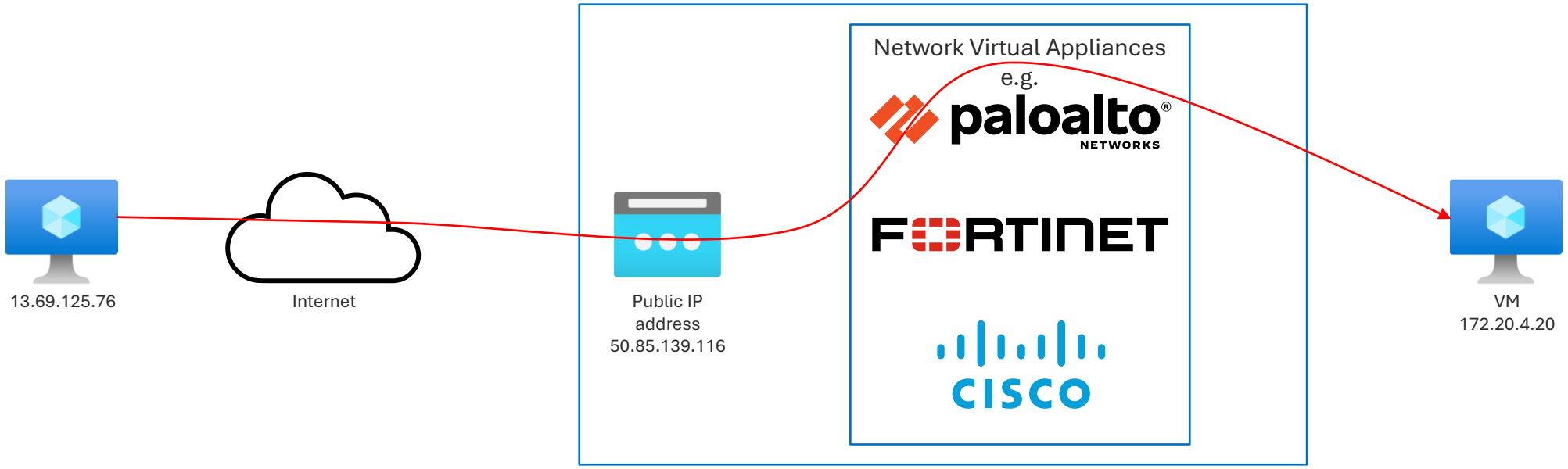
- What will the source IP address be?

DNAT



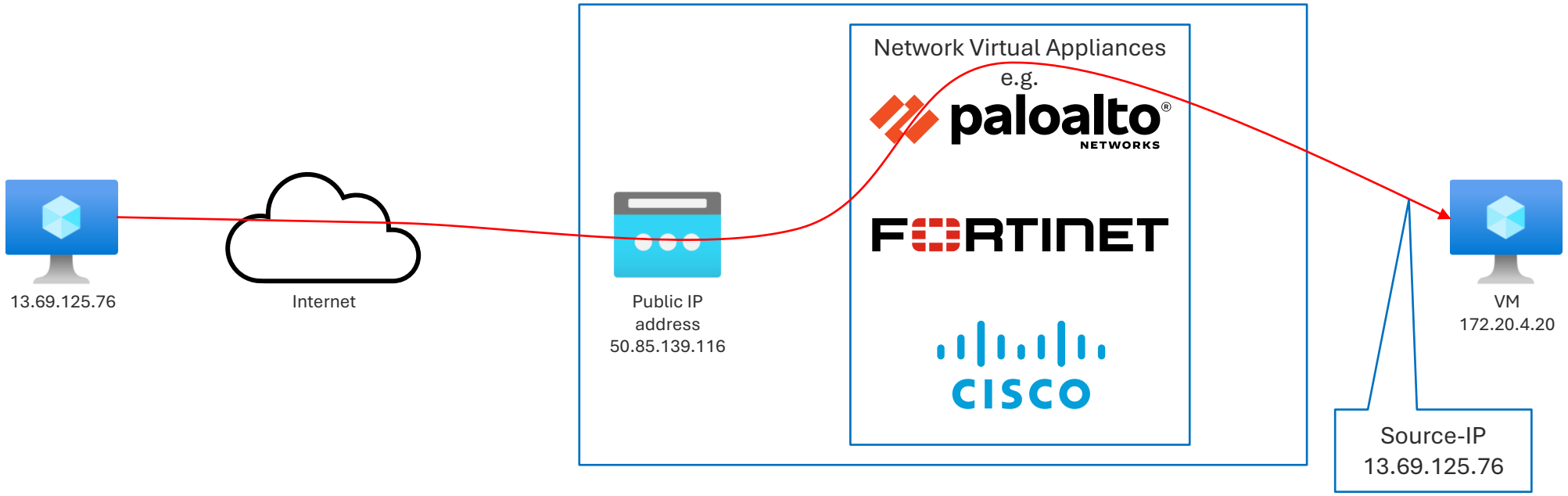
- DNAT rules are applied before network rules.

DNAT



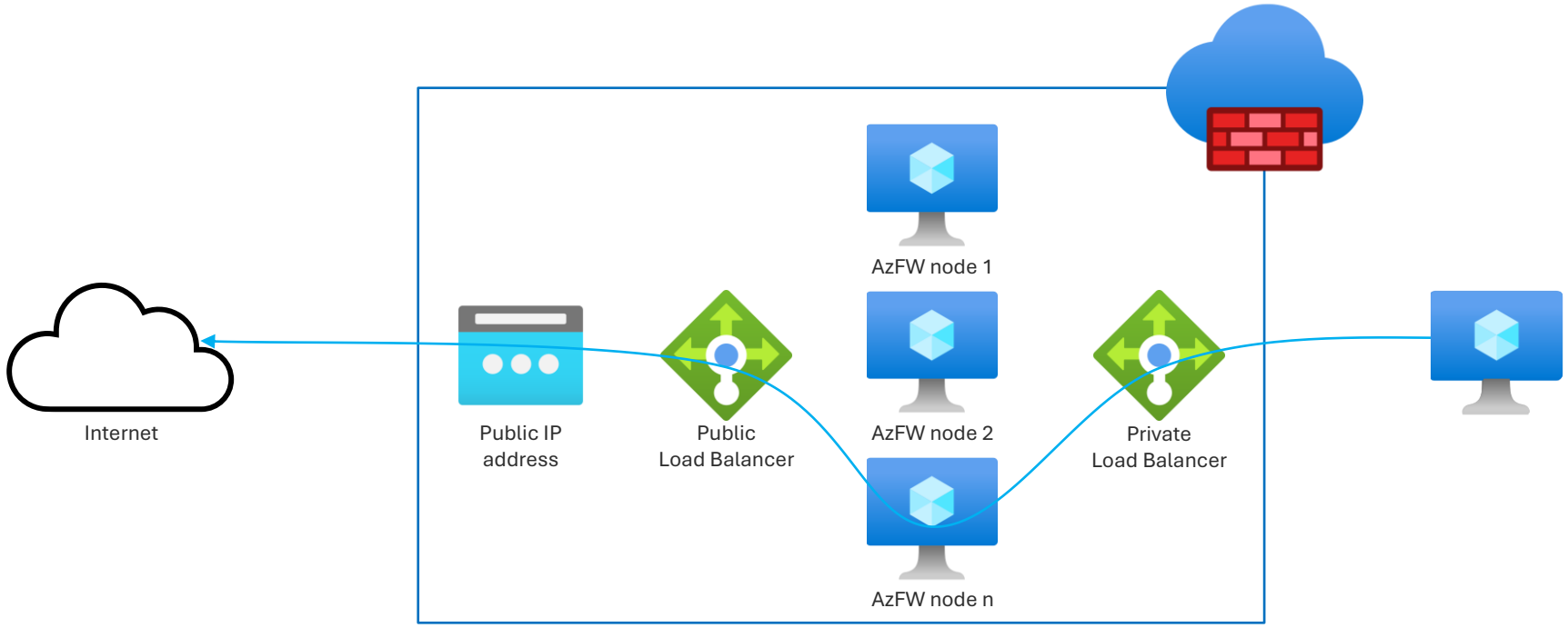
- What will the source IP address be?

DNAT


13.69.125.76
Internet
Public IP
address
50.85.139.116
Network Virtual Appliances
e.g.
paloalto
NETWORKS
FORTINET
CISCO
VM
172.20.4.20
Source-IP
13.69.125.76

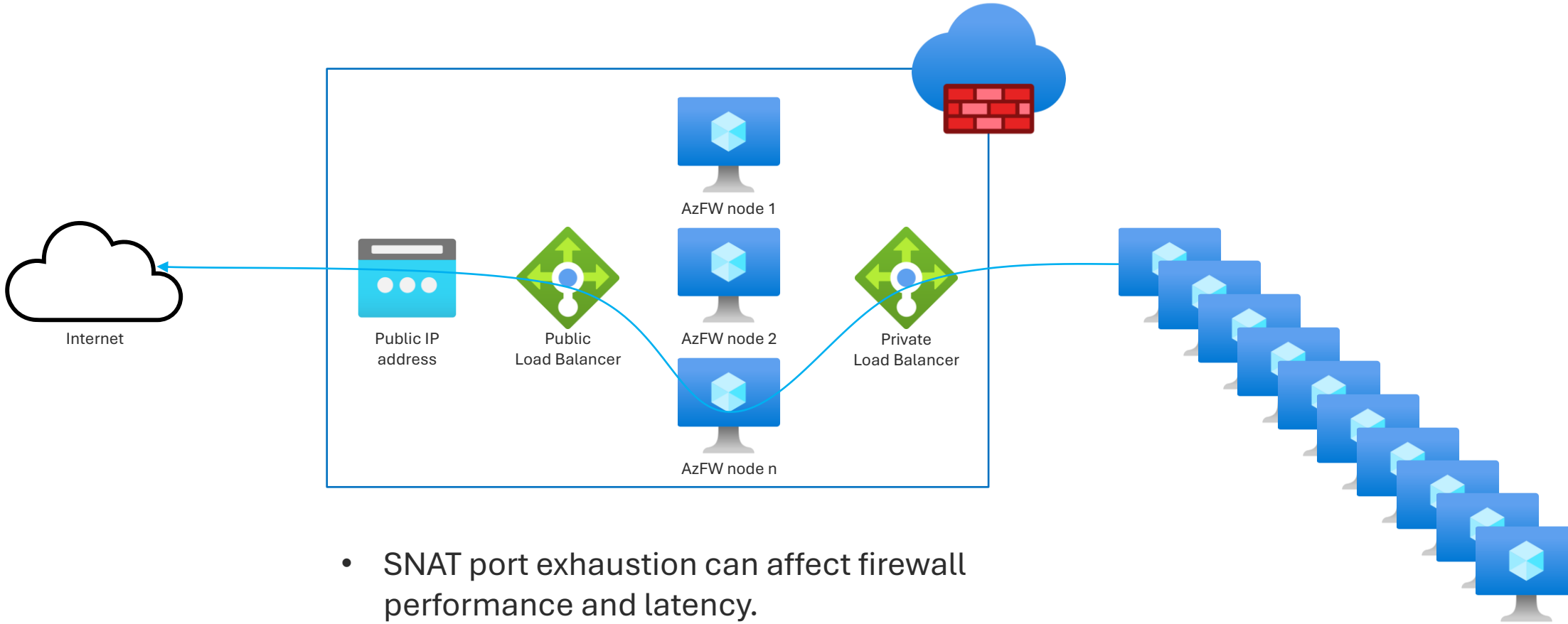
AZURE FIREWALL SNAT
SOURCE NETWORK ADDRESS TRANSLATION

SNAT



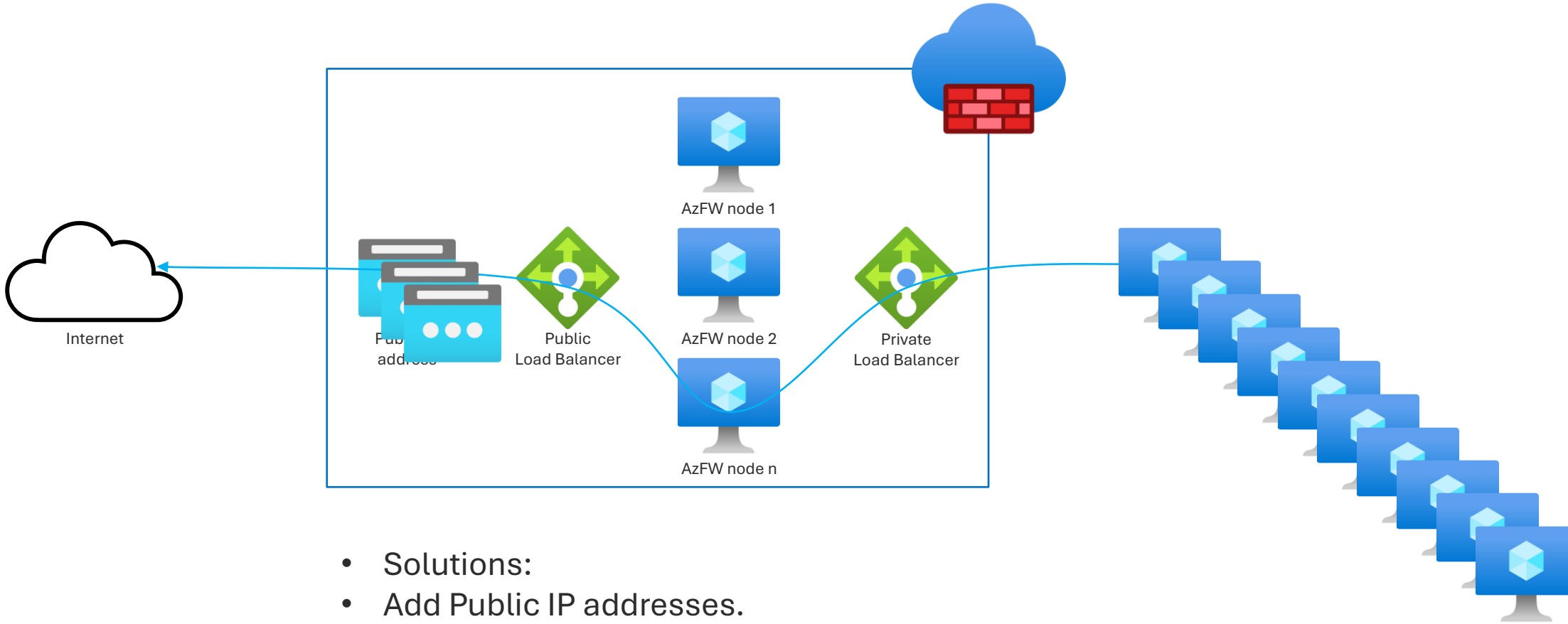
- Azure Firewall SNAT ports are limited to 2496 ports per Public IP and not 65K.

SNAT



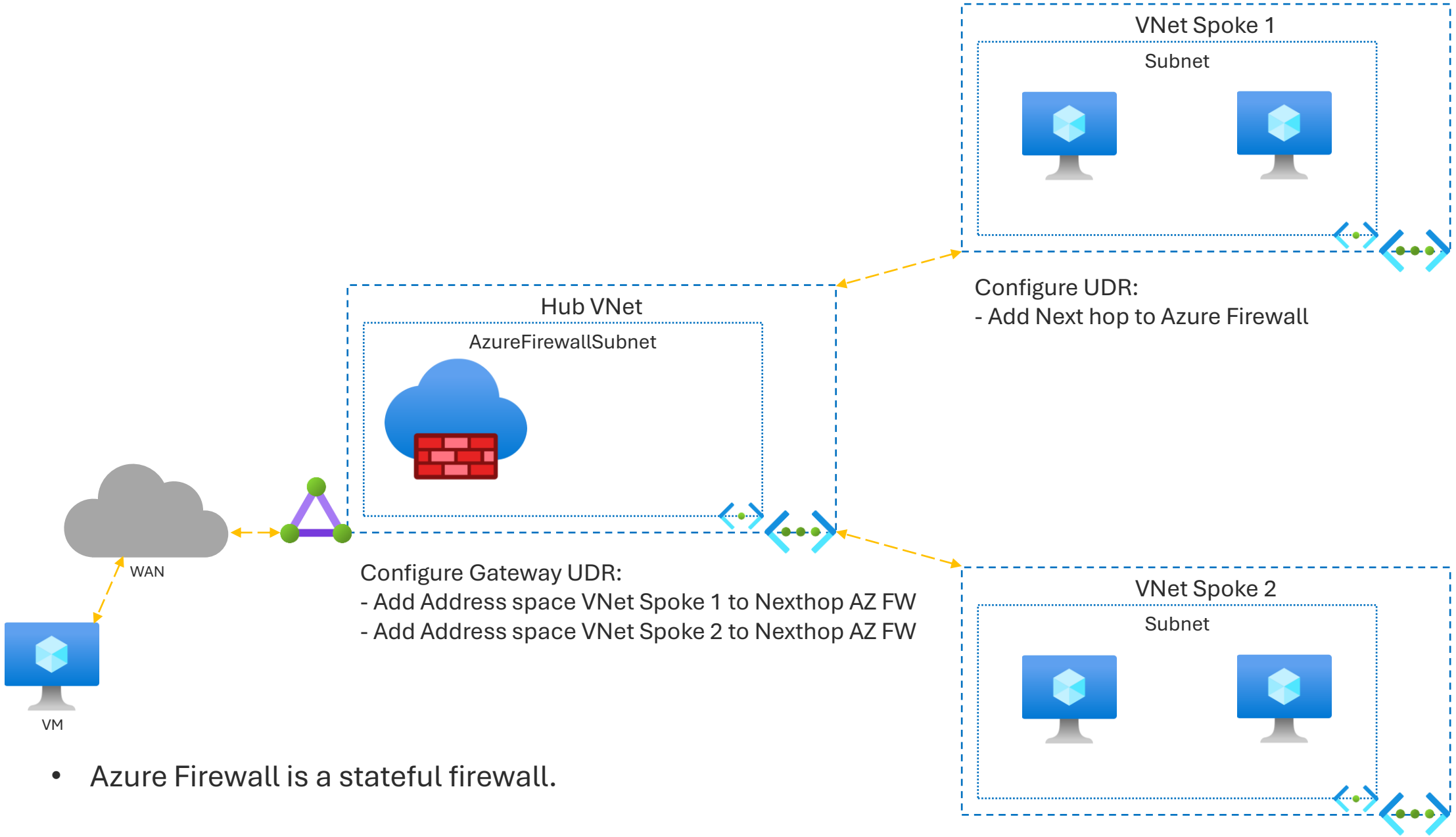
- SNAT port exhaustion can affect firewall performance and latency.
- AVD's are SNAT intensive.
- Monitor SNAT port Metric.

SNAT

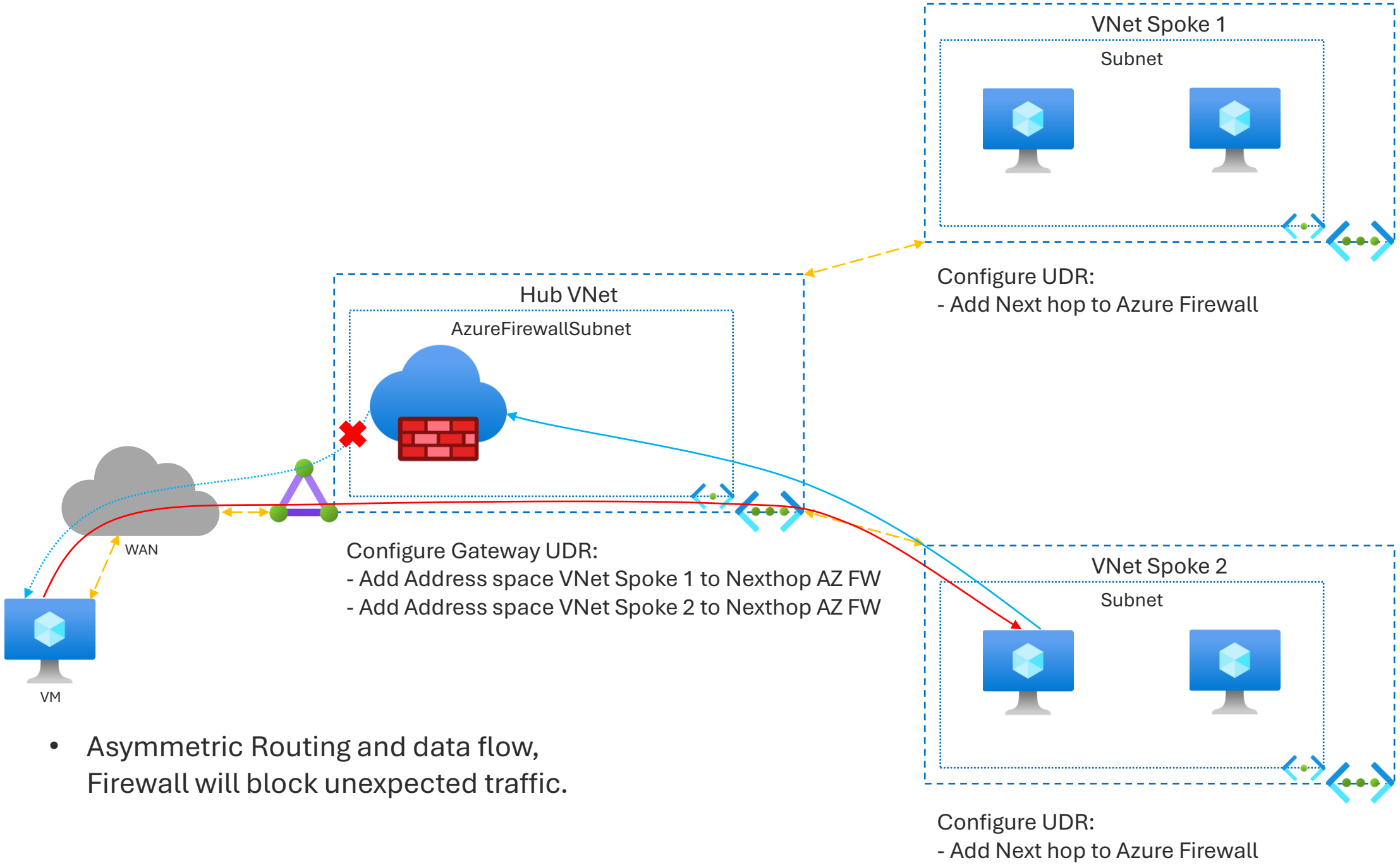


- Solutions:
- Add Public IP addresses.
- “Azure NAT Gateway”.

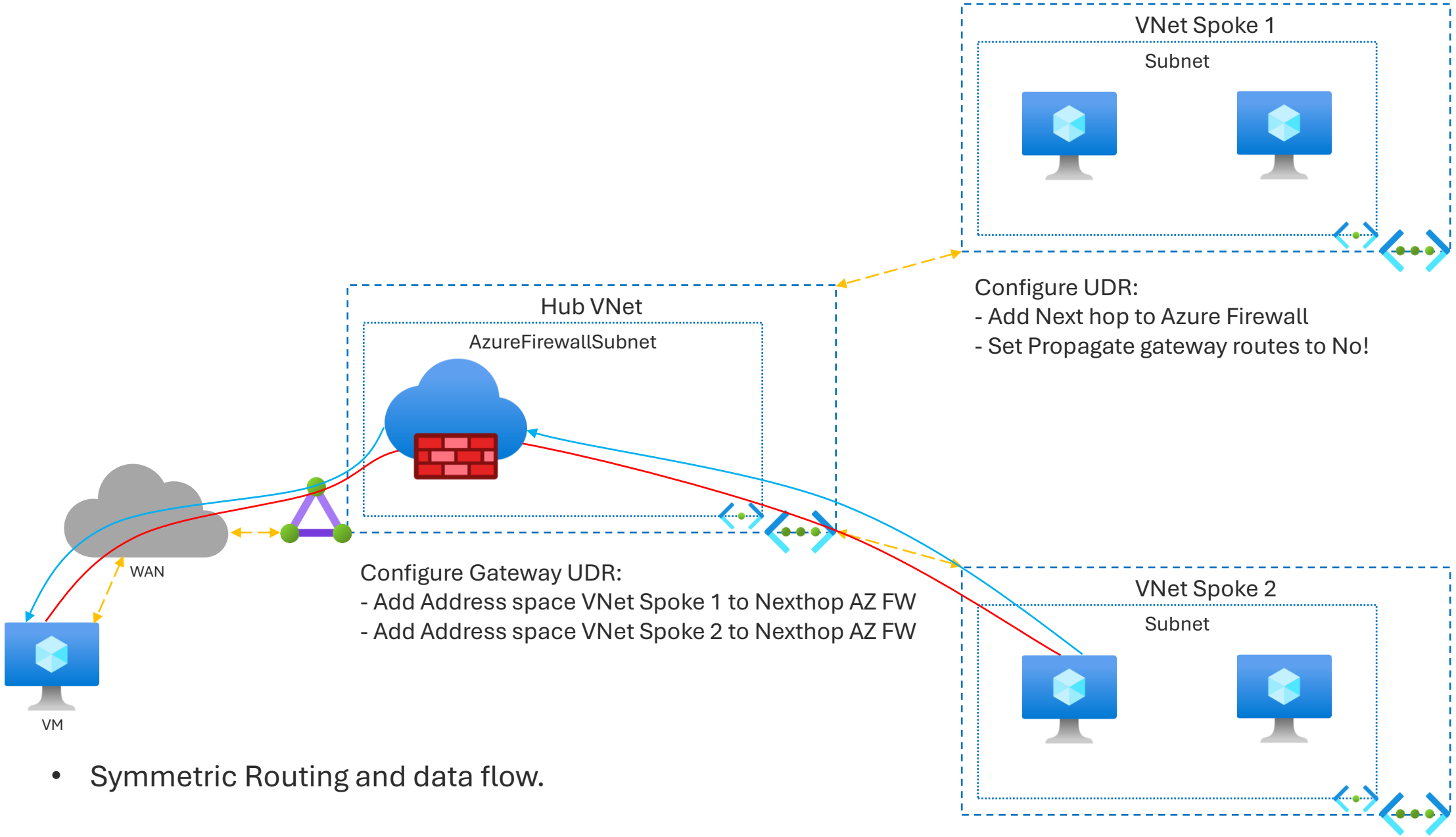
SYMMETRIC VS ASYMMETRIC ROUTING



- Azure Firewall is a stateful firewall.



- Asymmetric Routing and data flow, Firewall will block unexpected traffic.



- Symmetric Routing and data flow.

AZURE FIREWALL
LOGS VS STRUCTURED LOGS

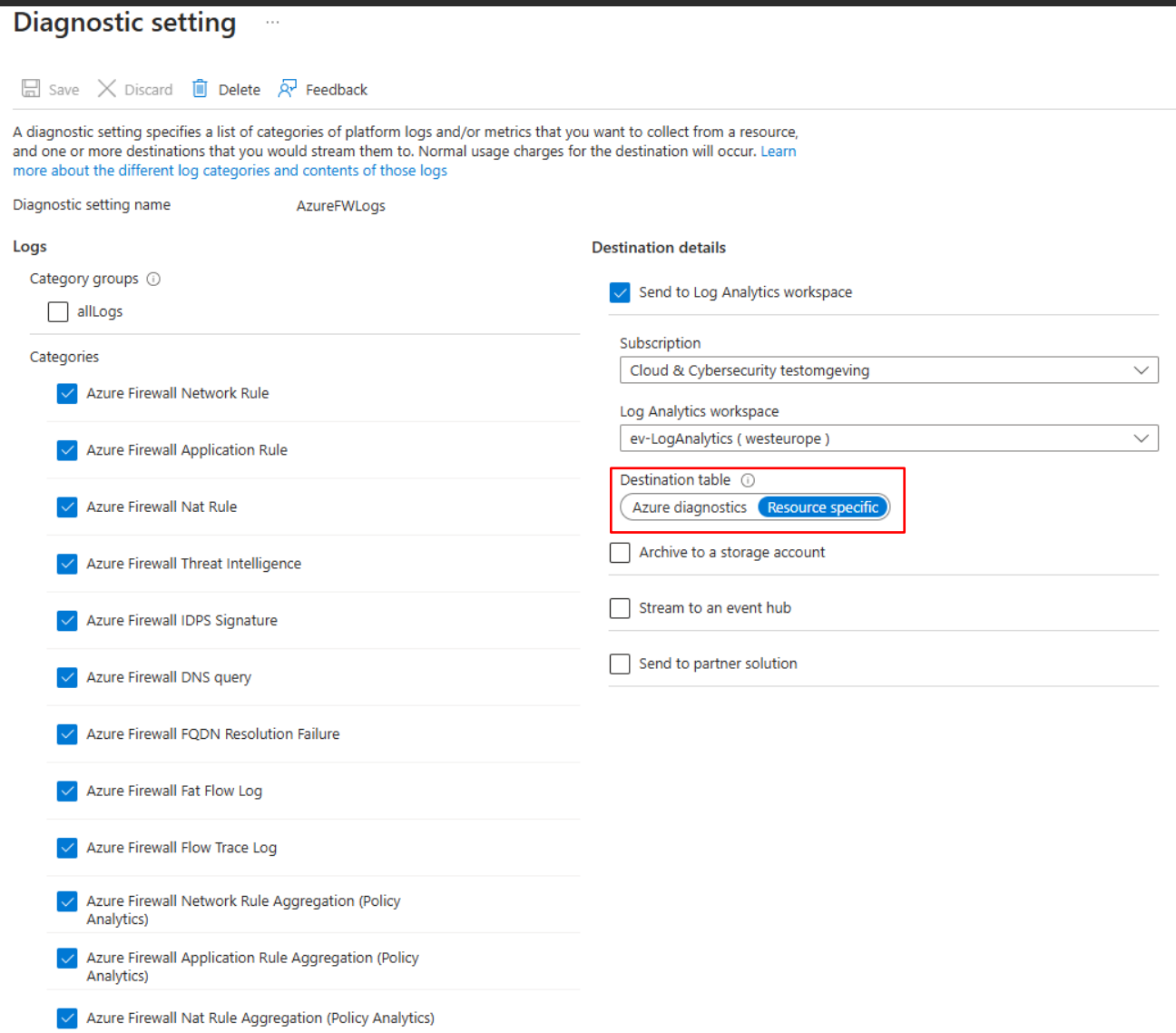
AZURE FIREWALL LOGS

```
// Network rule log data
// Parses the network rule log data.
AzureDiagnostics
| where Category == "AzureFirewallNetworkRule"
| where OperationName == "AzureFirewallNatRuleLog" or OperationName == "AzureFirewallNetworkRuleLog"
//case 1: for records that look like this:
//PROTO request from IP:PORT to IP:PORT.
| parse msg_s with Protocol " request from " SourceIP ":" SourcePortInt:int " to " TargetIP ":" TargetPortInt:int *
//case 1a: for regular network rules
| parse kind=regex flags=U msg_s with * ". Action\\: " Action1a "\\."
//case 1b: for NAT rules
//TCP request from IP:PORT to IP:PORT was DNAT'ed to IP:PORT
| parse msg_s with * " was " Action1b:string " to " TranslatedDestination:string ":" TranslatedPort:int *
//Parse rule data if present
| parse msg_s with * ". Policy: " Policy ". Rule Collection Group: " RuleCollectionGroup "." *
| parse msg_s with * " Rule Collection: "  RuleCollection ". Rule: " Rule
//case 2: for ICMP records
//ICMP request from 10.0.2.4 to 10.0.3.4. Action: Allow
| parse msg_s with Protocol2 " request from " SourceIP2 " to " TargetIP2 ". Action: " Action2
| extend
SourcePort = tostring(SourcePortInt),
TargetPort = tostring(TargetPortInt)
| extend
    Action = case(Action1a == "", case(Action1b == "",Action2,Action1b), split(Action1a,".")[0]),
    Protocol = case(Protocol == "", Protocol2, Protocol),
    SourceIP = case(SourceIP == "", SourceIP2, SourceIP),
    TargetIP = case(TargetIP == "", TargetIP2, TargetIP),
    //ICMP records don't have port information
    SourcePort = case(SourcePort == "", "N/A", SourcePort),
    TargetPort = case(TargetPort == "", "N/A", TargetPort),
    //Regular network rules don't have a DNAT destination
    TranslatedDestination = case(TranslatedDestination == "", "N/A", TranslatedDestination),
    TranslatedPort = case(isnull(TranslatedPort), "N/A", tostring(TranslatedPort)),
    //Rule information
    Policy = case(Policy == "", "N/A", Policy),
    RuleCollectionGroup = case(RuleCollectionGroup == "", "N/A", RuleCollectionGroup ),
    RuleCollection = case(RuleCollection == "", "N/A", RuleCollection ),
    Rule = case(Rule == "", "N/A", Rule)
| project TimeGenerated, msg_s, Protocol, SourceIP,SourcePort,TargetIP,TargetPort,Action, TranslatedDestination, TranslatedPort, Policy, RuleCollectionGroup, RuleCollection, Rule
```

TimeGenerated [UTC]	msg_s	Protocol	SourceIP	SourcePort	TargetIP	TargetPort	Action	TranslatedDestination	TranslatedPort	Policy	RuleCollectionGroup	RuleCollection	Rule
3/11/2025, 1:16:25.282 PM	TCP request from 167.94.145.29:47528 to 50.85.139.116:3389. Action: Deny..	TCP	167.94.145.29	47528	50.85.139.116	3389	Deny	N/A	N/A	N/A	N/A	N/A	N/A
3/11/2025, 1:15:02.162 PM	TCP request from 172.20.4.21:57420 to 51.116.253.169:443. Action: Allow.. Policy: FirewallPolicy_ev-hub-...	TCP	172.20.4.21	57420	51.116.253.169	443	Allow	N/A	N/A	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp
3/11/2025, 1:08:43.479 PM	TCP request from 204.76.203.15:38878 to 50.85.139.116:80. Action: Deny..	TCP	204.76.203.15	38878	50.85.139.116	80	Deny	N/A	N/A	N/A	N/A	N/A	N/A
3/11/2025, 1:03:58.106 PM	TCP request from 172.20.4.20:57252 to 13.107.21.239:443. Action: Allow.. Policy: FirewallPolicy_ev-hub-pr...	TCP	172.20.4.20	57252	13.107.21.239	443	Allow	N/A	N/A	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp
3/11/2025, 1:01:48.154 PM	TCP request from 172.20.4.20:57196 to 20.189.173.17:443. Action: Allow.. Policy: FirewallPolicy_ev-hub-pr...	TCP	172.20.4.20	57196	20.189.173.17	443	Allow	N/A	N/A	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp
3/11/2025, 1:00:01.164 PM	TCP request from 172.20.4.21:57050 to 40.79.173.40:443. Action: Allow.. Policy: FirewallPolicy_ev-hub-prd...	TCP	172.20.4.21	57050	40.79.173.40	443	Allow	N/A	N/A	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp
3/11/2025, 12:59:35.329 PM	TCP request from 172.20.4.36:56849 to 151.101.38.172:80. Action: Allow.. Policy: FirewallPolicy_ev-hub-pr...	TCP	172.20.4.36	56849	151.101.38.172	80	Allow	N/A	N/A	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp
3/11/2025, 12:58:35.308 PM	TCP request from 172.20.4.36:56824 to 13.69.116.109:443. Action: Allow.. Policy: FirewallPolicy_ev-hub-pr...	TCP	172.20.4.36	56824	13.69.116.109	443	Allow	N/A	N/A	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp
3/11/2025, 12:52:12.905 PM	TCP request from 188.90.163.27:19888 to 50.85.139.116:80 was DNAT'ed to 172.20.4.20:80. Policy: Firewa...	TCP	188.90.163.27	19888	50.85.139.116	80	DNAT'ed	172.20.4.20	80	FirewallPolicy_ev-hub-prd-fw	DefaultDnatRuleCollectionGroup	RDP-Test	ev-prd-dns-01-www
3/11/2025, 12:52:12.905 PM	TCP request from 188.90.163.27:19889 to 50.85.139.116:80 was DNAT'ed to 172.20.4.20:80. Policy: Firewa...	TCP	188.90.163.27	19889	50.85.139.116	80	DNAT'ed	172.20.4.20	80	FirewallPolicy_ev-hub-prd-fw	DefaultDnatRuleCollectionGroup	RDP-Test	ev-prd-dns-01-www

AZURE FIREWALL LOGS

- Change Azure Firewall logging to Resource Specific.



STRUCTURED AZURE FIREWALL LOGS

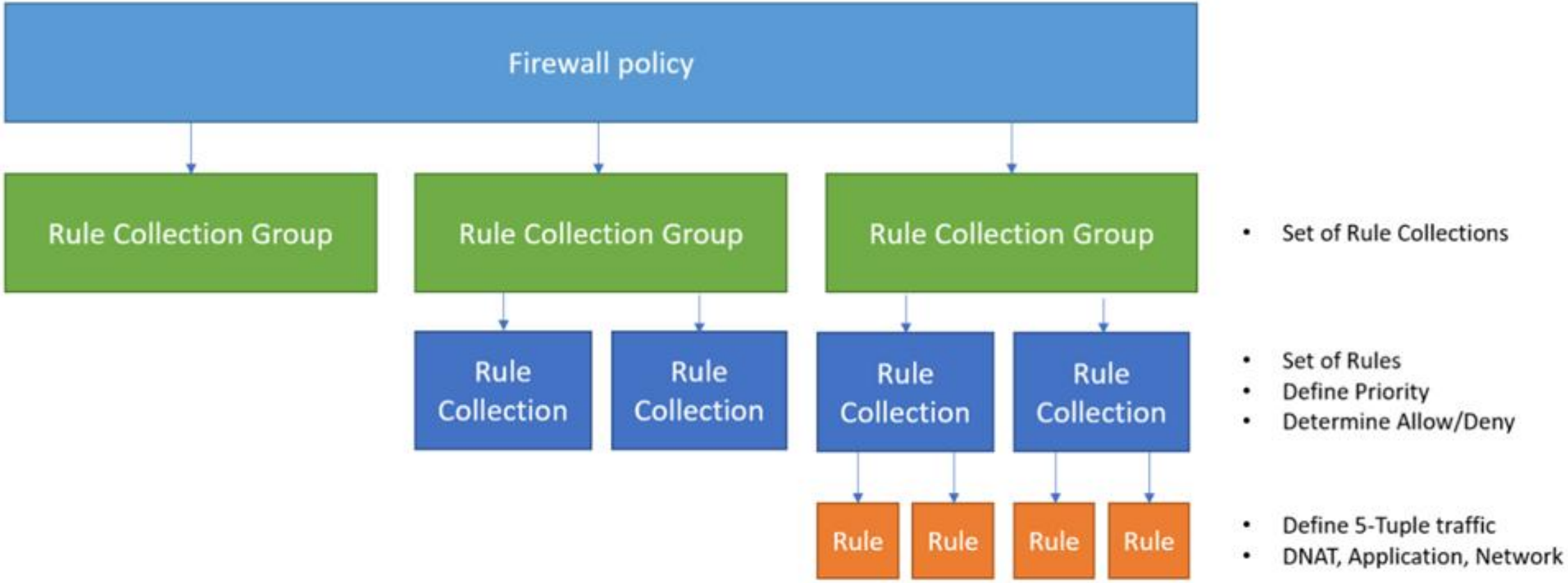
```
1  // Network rule logs
2  // Packets that matched Network rules. Both packet and rule metadata is displayed.
3  AZFWNetworkRule
4  | take 100
```

Results | Chart

TimeGenerated [UTC]	Protocol	SourceIp	SourcePort	DestinationIp	DestinationPort	Action	Policy	RuleCollectionGroup	RuleCollection	Rule	ActionReason
3/11/2025, 1:44:18.845 PM	TCP	172.20.4.36	57953	4.231.128.59	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:43:14.360 PM	TCP	172.20.4.21	58119	51.104.136.2	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:41:22.016 PM	TCP	172.20.4.20	58173	4.231.128.59	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:38:09.939 PM	TCP	172.20.4.36	57799	20.189.173.7	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:36:46.672 PM	TCP	172.20.4.20	58060	20.189.173.17	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:33:57.050 PM	TCP	66.240.205.34	17525	50.85.139.116	80	Deny					Default Action
3/11/2025, 1:32:21.917 PM	TCP	167.94.146.27	54337	50.85.139.116	3389	Deny					Default Action
3/11/2025, 1:30:02.800 PM	TCP	172.20.4.21	57794	13.69.109.130	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:24:28.830 PM	TCP	172.20.4.21	57657	13.107.21.239	80	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:24:28.347 PM	TCP	172.20.4.21	57656	13.107.21.239	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	
3/11/2025, 1:19:29.488 PM	TCP	172.20.4.20	57637	20.189.173.18	443	Allow	FirewallPolicy_ev-hub-prd-fw	DefaultNetworkRuleCollectionGroup	traffic-to-internet	traffic-to-internet-tcp	

AZURE FIREWALL RULE PROCESSING

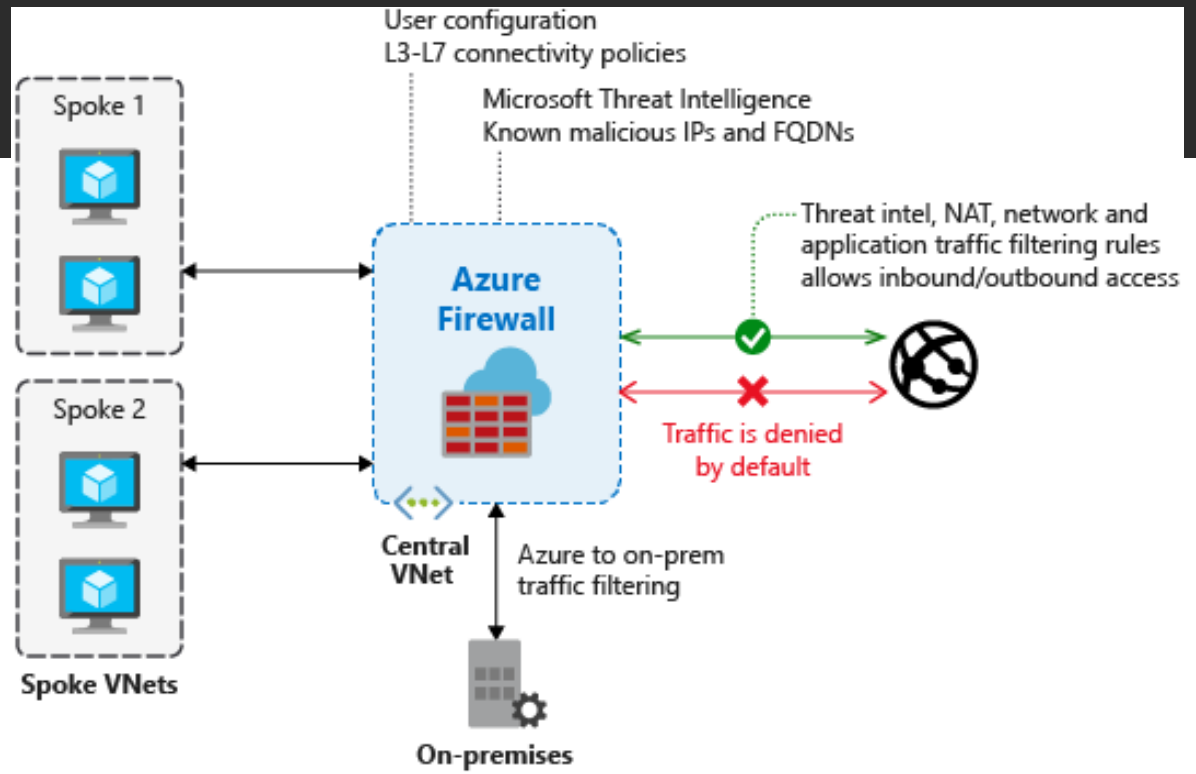
CLASSIC VS POLICY



- DNAT rules
- Network rules
- Application rules

THREAT INTELLIGENCE

- Filtering!
- Powered by intelligent security graph
- Why do we care?



Priority:

- Threat Intelligence rules
- DNAT rules
- Network rules
- Application rules

INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

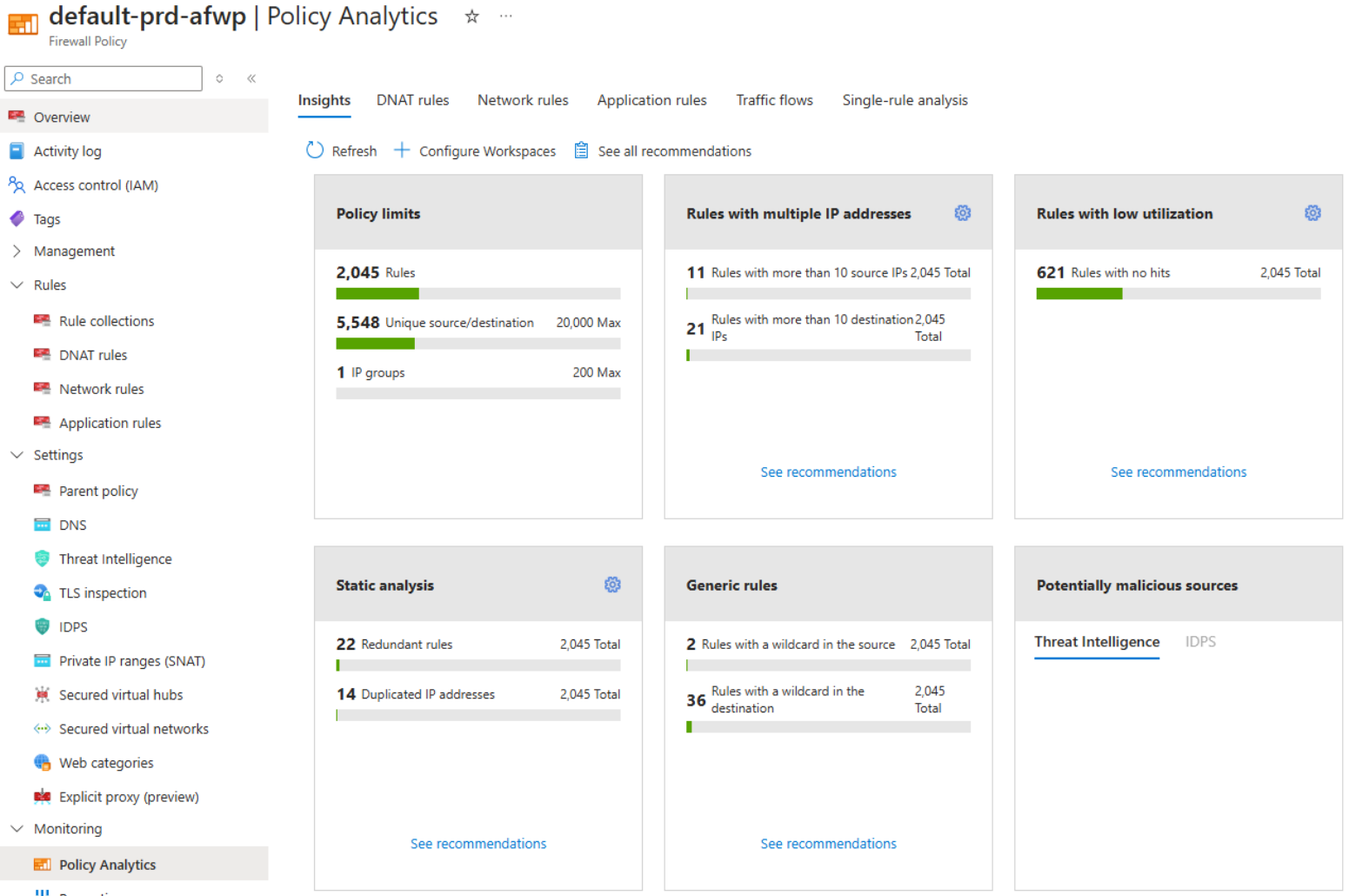
- Azure Firewall Premium
- Rapid detection, specific patterns
- Alert mode
- Alert and Deny mode

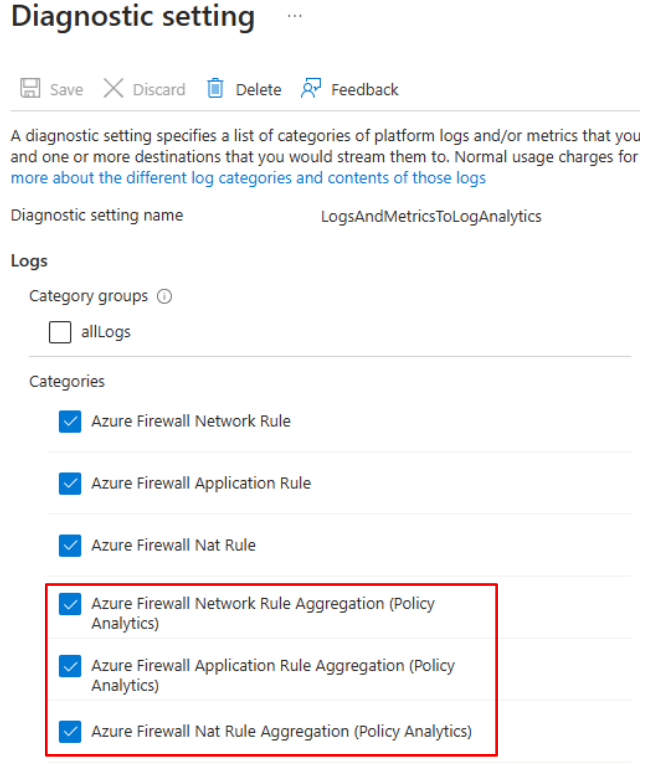
Priority:

- Threat Intelligence rules
- DNAT rules
- Network rules
- Application rules
- IDPS rules

AZURE FIREWALL POLICY ANALYTICS

POLICY ANALYTICS



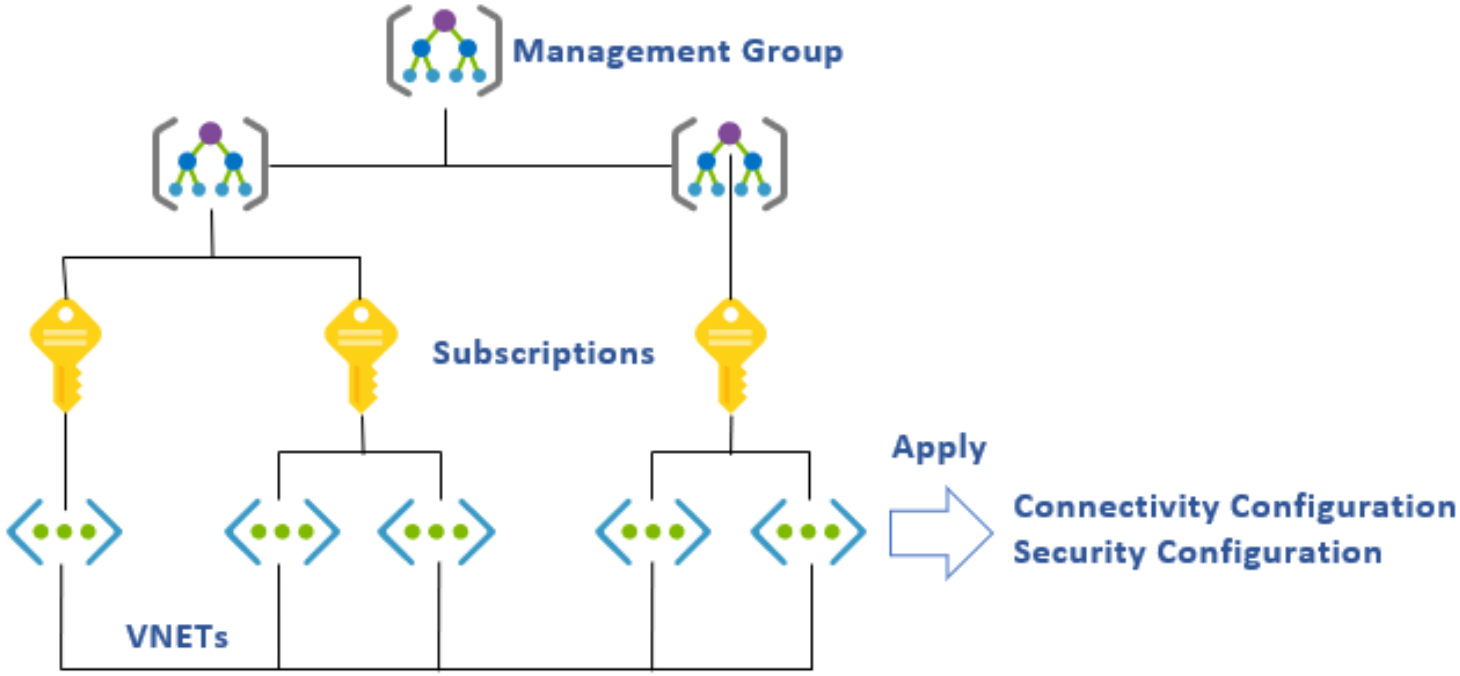


- Enable Policy Analytics logging to gain useful insights.

Unique source/destinations in network = sum of (unique source addresses * unique destination addresses for each rule) **and unique ports**

AZURE VIRTUAL NETWORK MANAGER (AVNM)

- Group, configure, deploy, and manage virtual networks!
- Globally across subscriptions!
- Automated!
- IPAM! (Preview)
- Cross-tenant!
- UDR Management!



AVNM LIMITATIONS

- Cross-tenant support
- +15 000 subscriptions
- Custom policy enforcement mode: Disabled
- No support for standard evaluation cycle in policy compliance
- Moving subscription with AVNM instance to another tenant
- 1000 vnet peerings for hub/spoke
- 1000 private endpoints per connected group
- Overlapping CIDrs…
- 1000 IP prefixes in security admin rules
- 100 admin rules in one level
- Service tags for DNS/IMDS/LKM are not supported

QUESTIONS?


That's all Folks!