

A campfire is burning brightly on a rocky beach. The fire is made of several logs and is surrounded by large, smooth, grey rocks. In the background, the ocean stretches to the horizon under a sunset sky with soft orange and blue hues. Distant mountains are visible on the horizon line.

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 | • Cloud Identity | • Architecture & Design |
| • DNS | • Security | • Governance |
| • Firewall's | • Automation | • Networking |



Marc Dekeyser

Sr. Customer Experience Engineer



Who me?

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

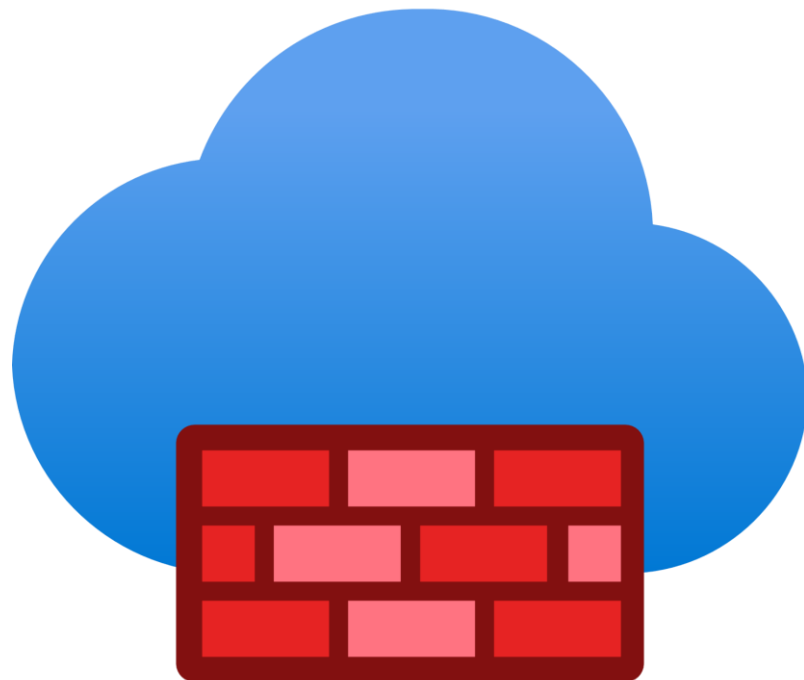
- Tinkerer & Evil Mastermind
- Microsoftie since 2012
- Azure Worldwide Communities SME
- Diversity & Inclusion Advisor
- Primary audience: Start-ups!

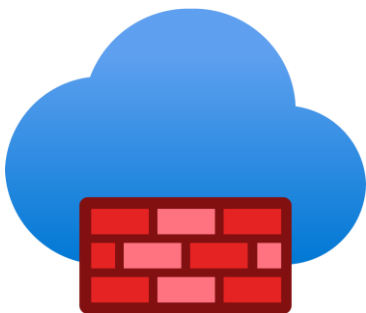
Expertise

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

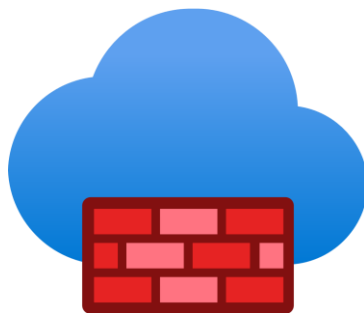
Dare to be Authentic, Curious, and Passionate

AZURE FIREWALL

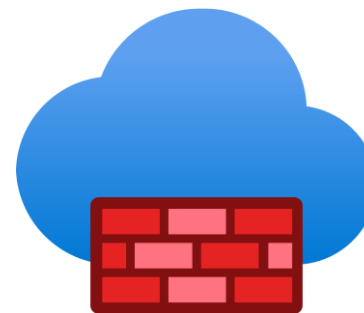




Firewall Basic



Firewall Standard



Firewall Premium

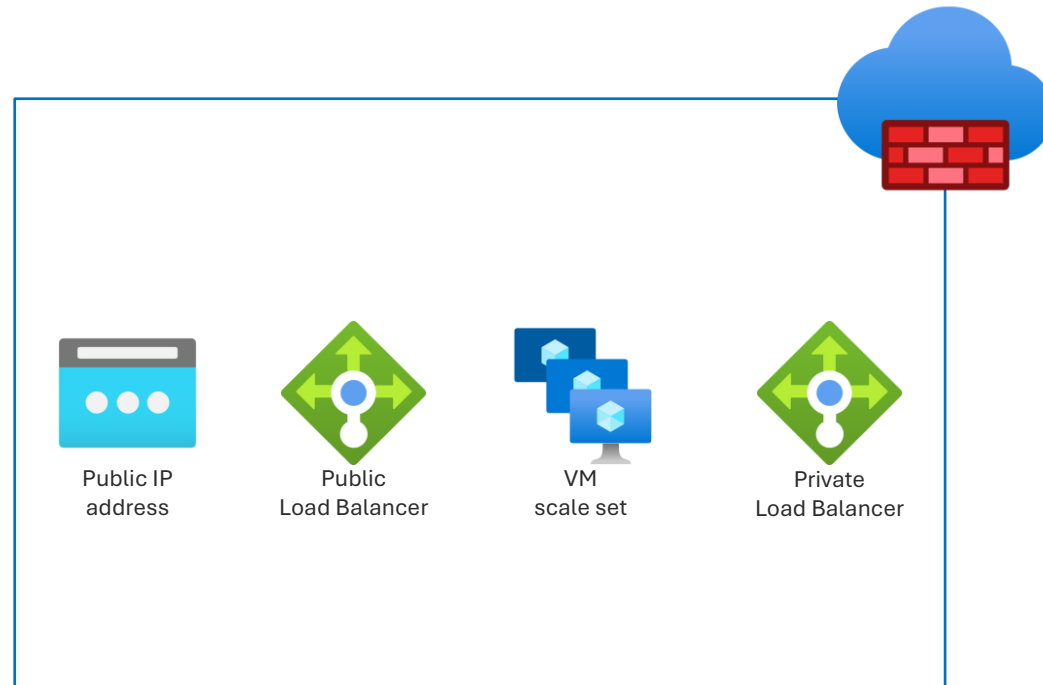
Feature Category	Feature	Firewall Basic	Firewall Standard	Firewall Premium
L3-L7 Filtering	Application level FQDN filtering (SNI based) for HTTPS/SQL	✓	✓	✓
	Network level FQDN filtering – all ports and protocols		✓	✓
	Stateful firewall (5 tuple rules)	✓	✓	✓
	Network Address Translation (SNAT+DNAT)	✓	✓	✓
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

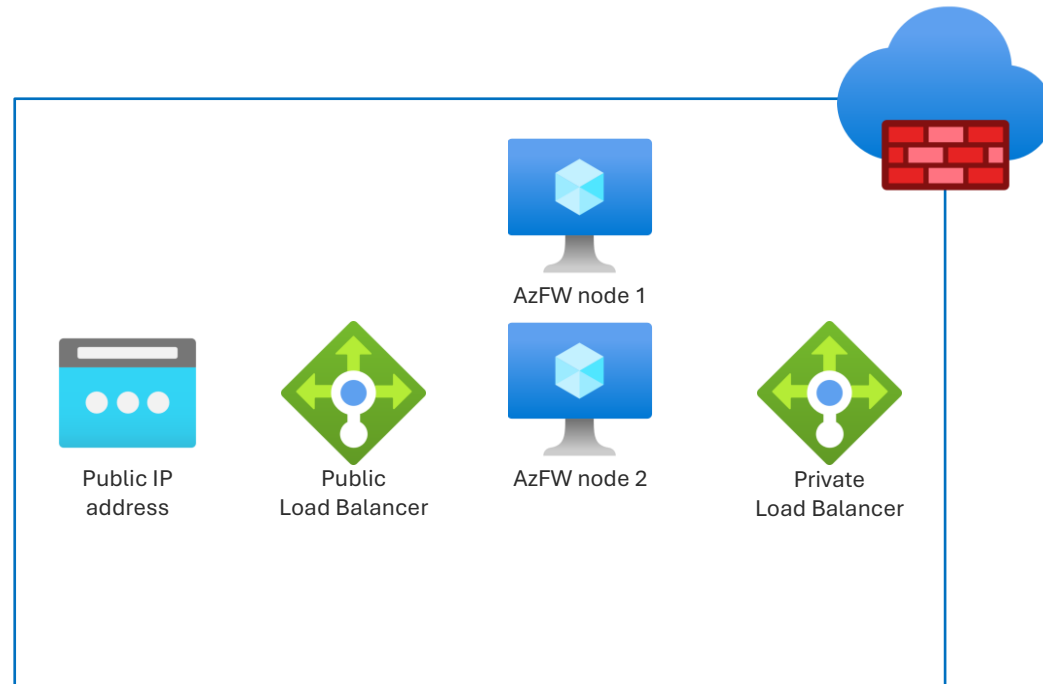
AZURE FIREWALL SCALING

AZURE FIREWALL SCALING



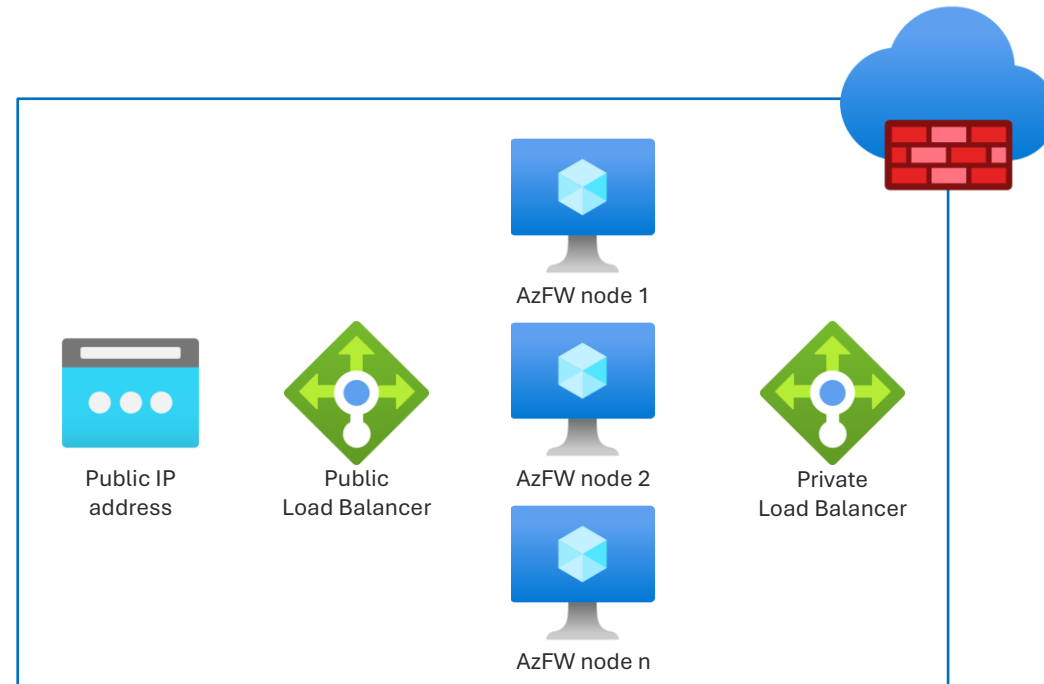
- Azure Firewall underlying architecture.

AZURE FIREWALL SCALING



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

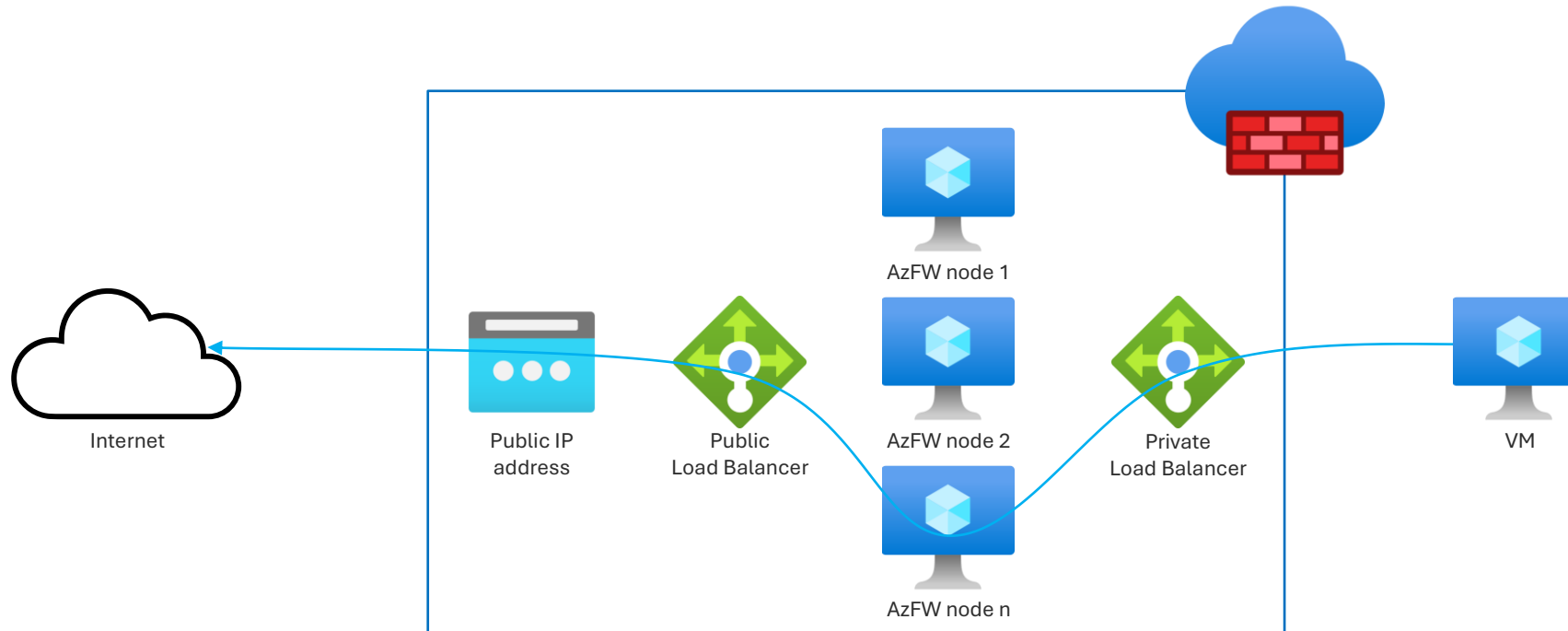
AZURE FIREWALL SCALING



- 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).

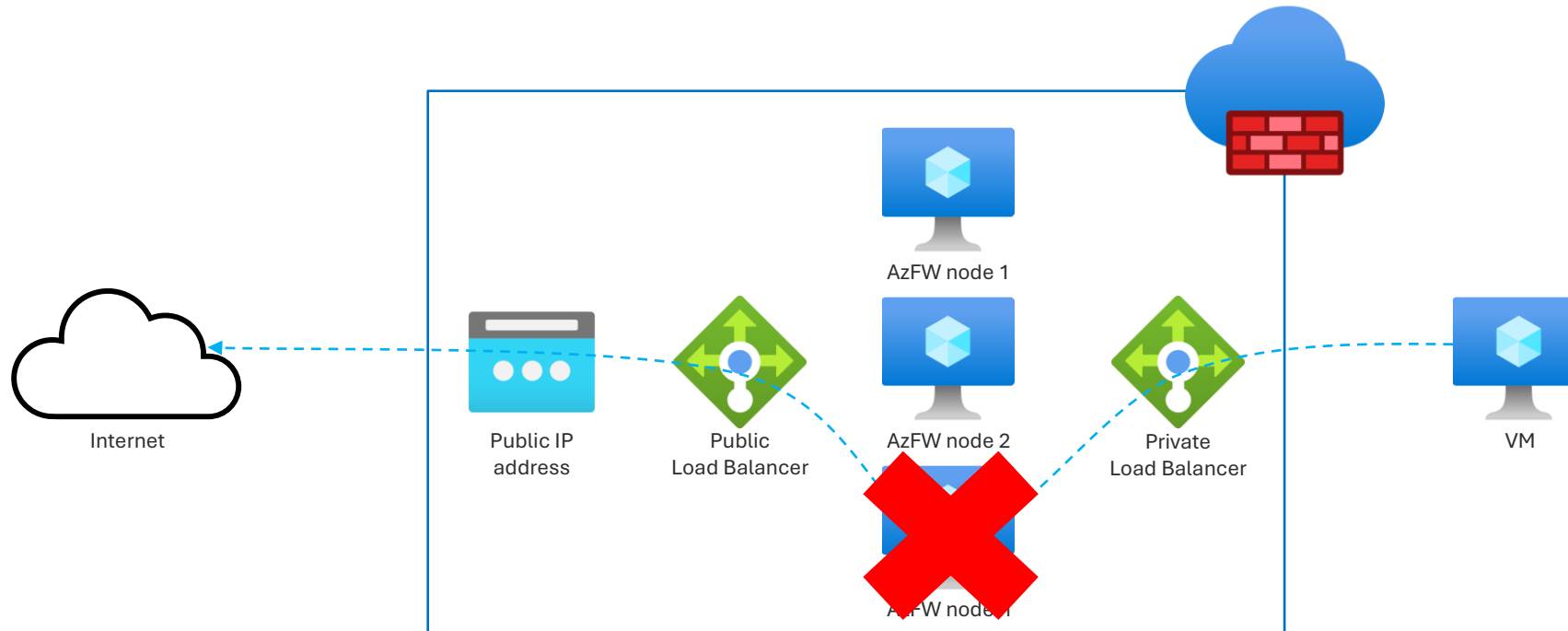
AZURE FIREWALL TCP TRAFFIC TIMEOUT

TCP TRAFFIC TIMEOUT



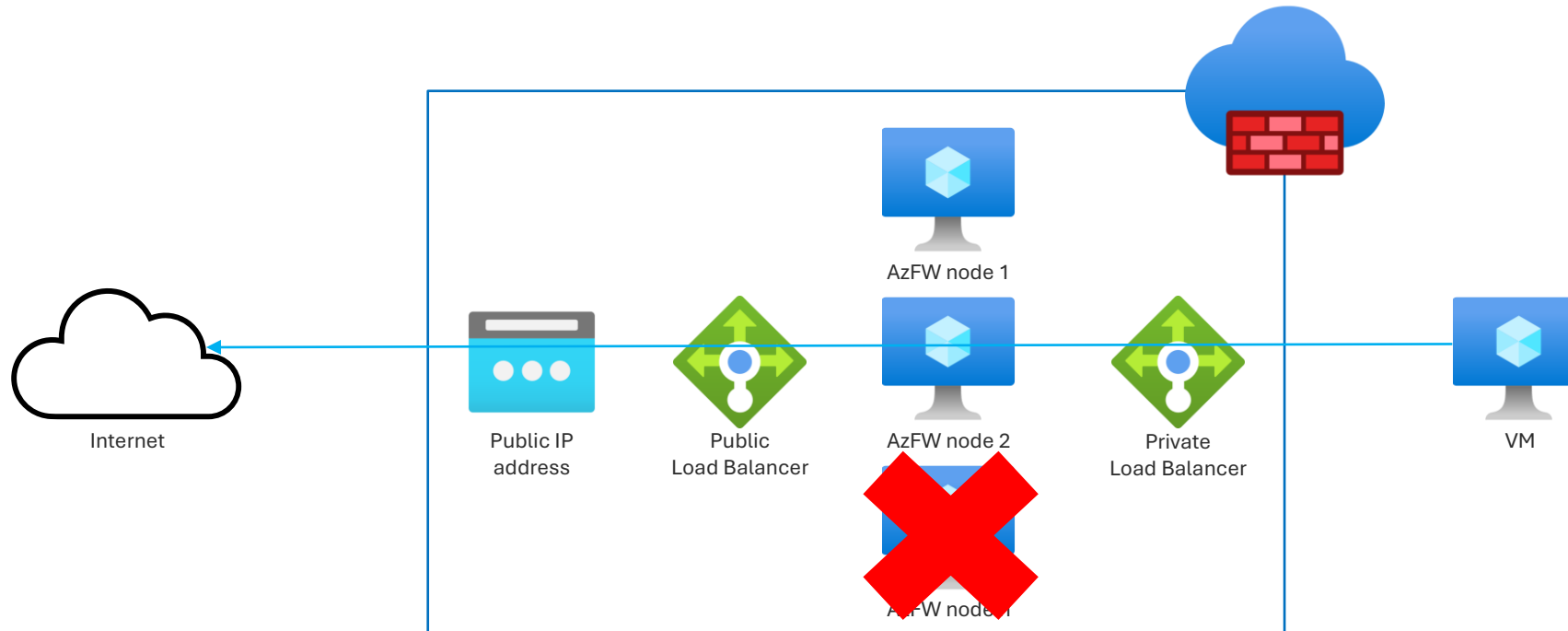
- Default TCP idle timeout of 4 minutes.
- The timeout can be set between 4 and 15 minutes via a support request.

TCP TRAFFIC TIMEOUT



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

TCP TRAFFIC TIMEOUT

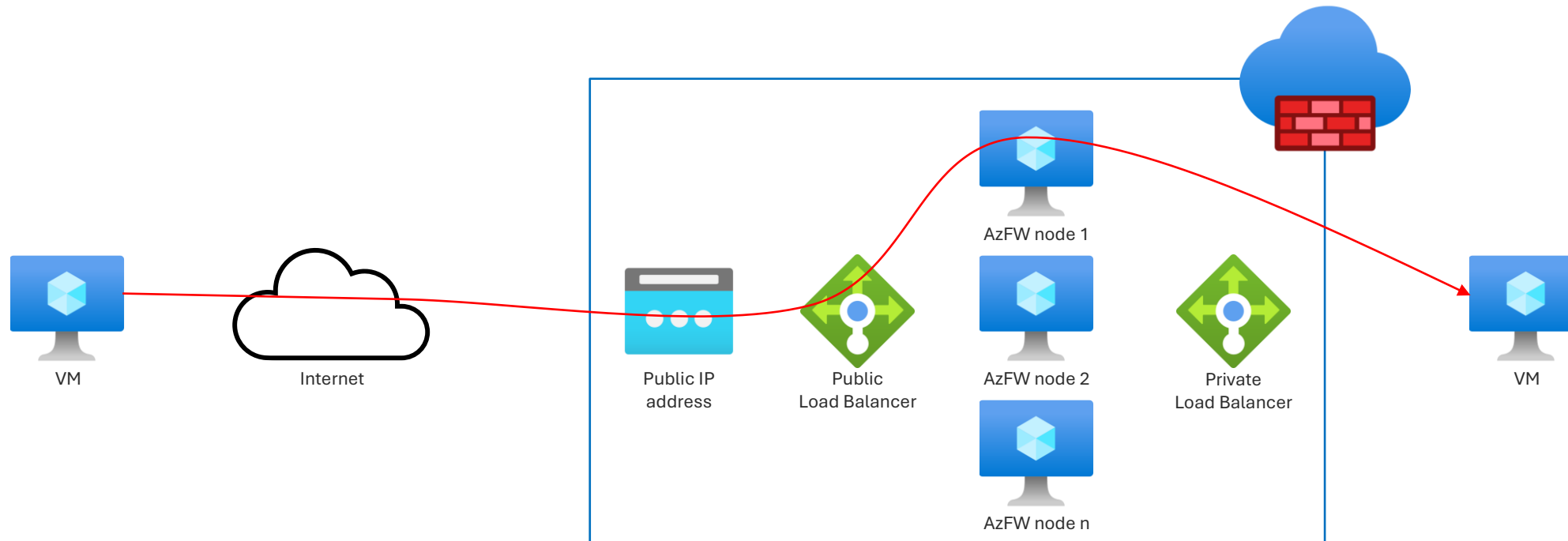


- Applications like SSH, RDP, VPN and database connections are sensitive to TCP session resets.

AZURE FIREWALL DNAT

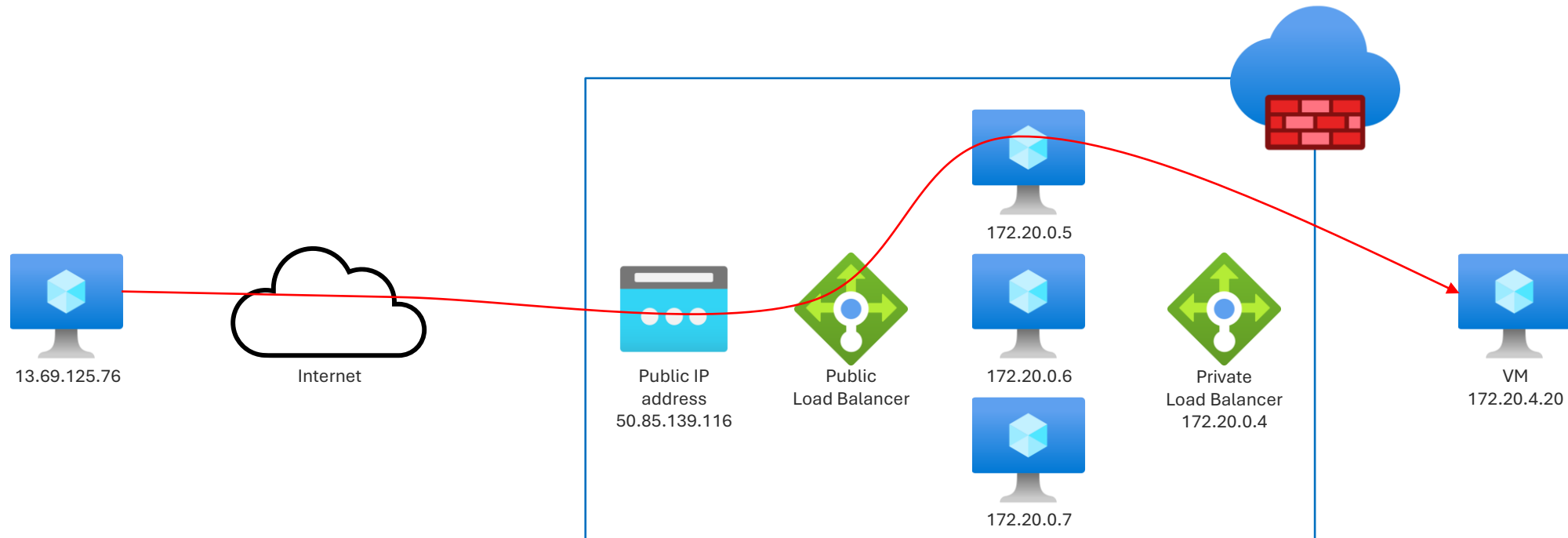
DESTINATION NETWORK ADDRESS TRANSLATION

DNAT



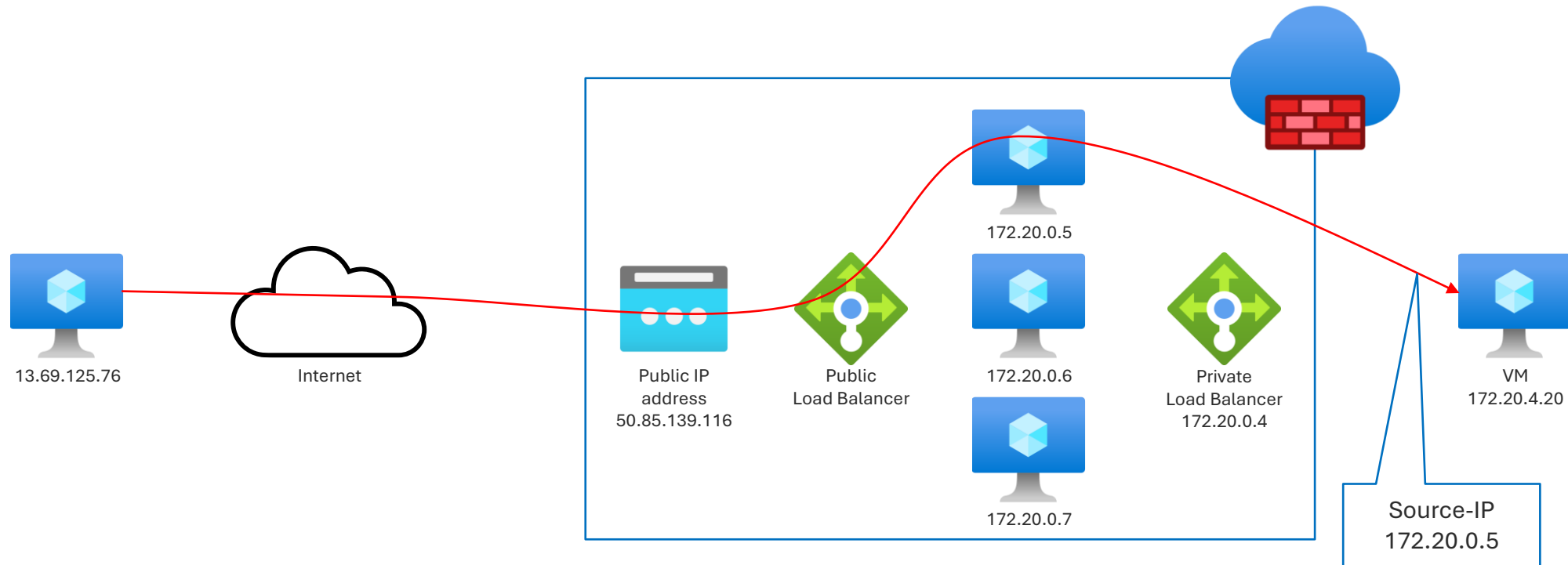
- DNAT filters and translates inbound Internet traffic by translating the firewall's public IP Address.

DNAT



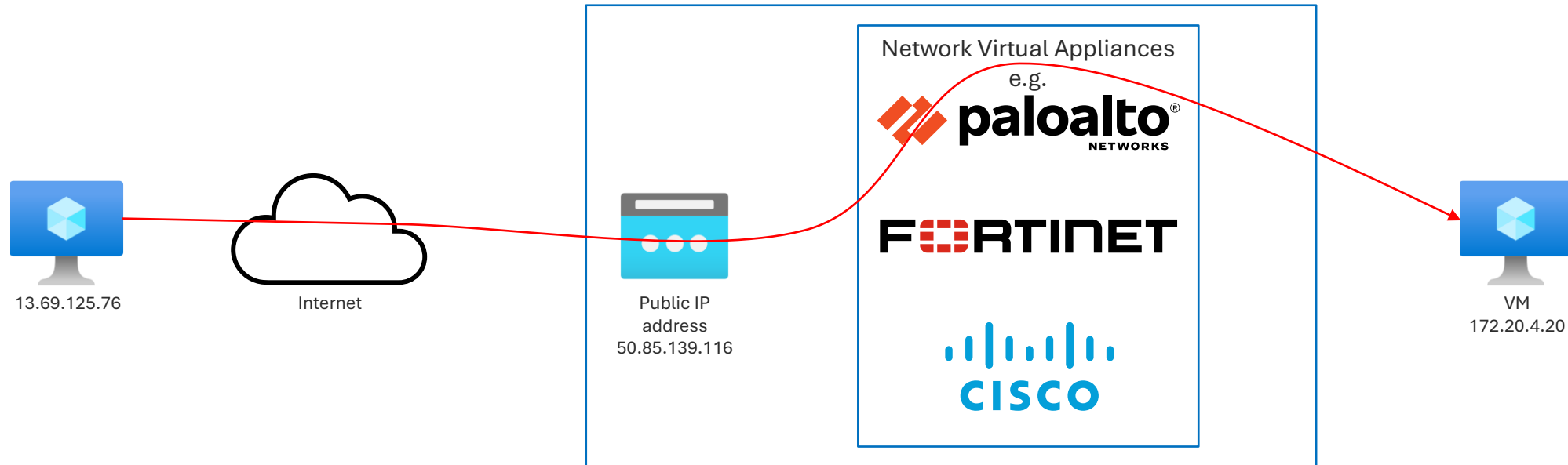
- What will the source IP address be?

DNAT



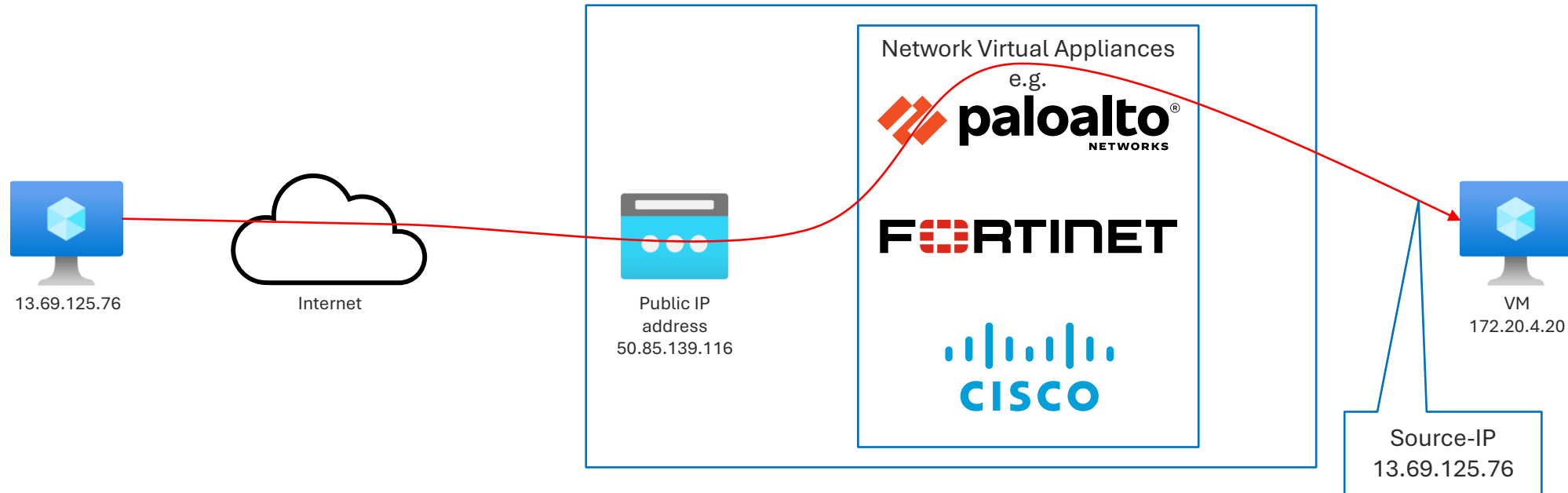
- DNAT rules are applied before network rules.

DNAT



- What will the source IP address be?

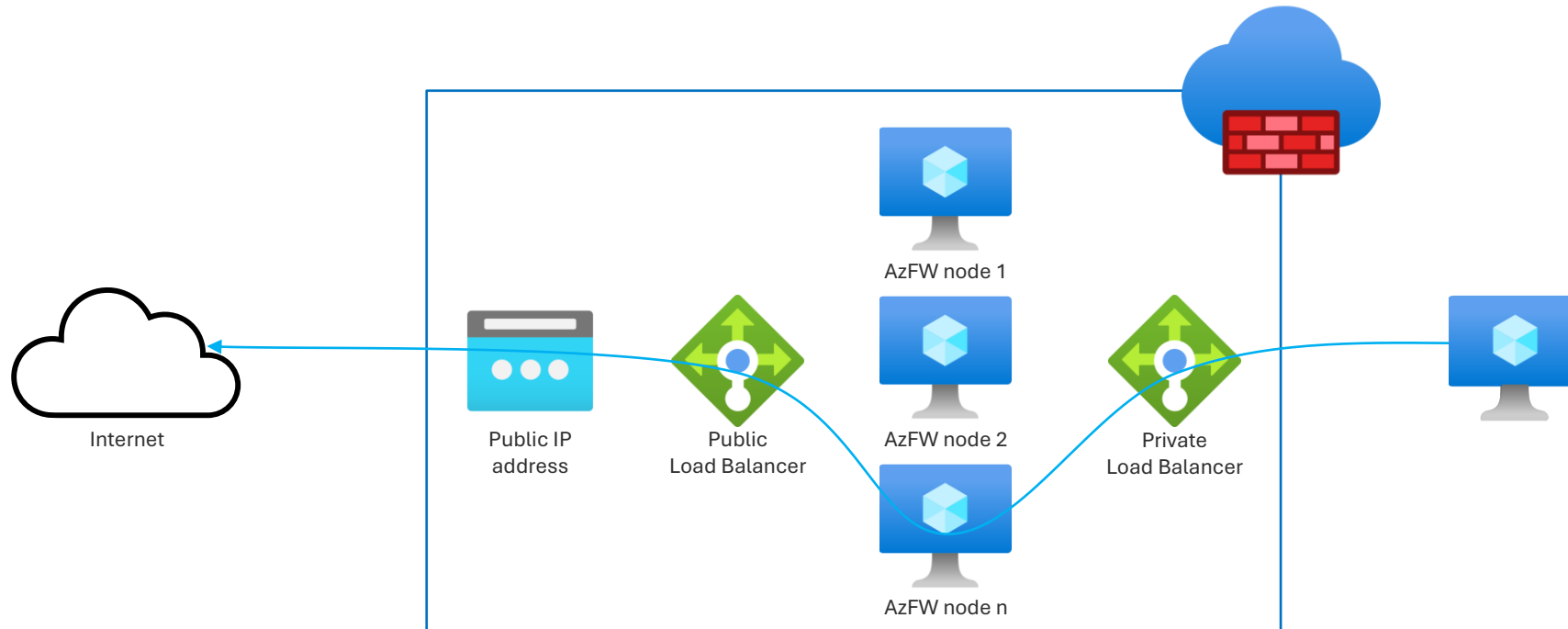
DNAT



AZURE FIREWALL SNAT

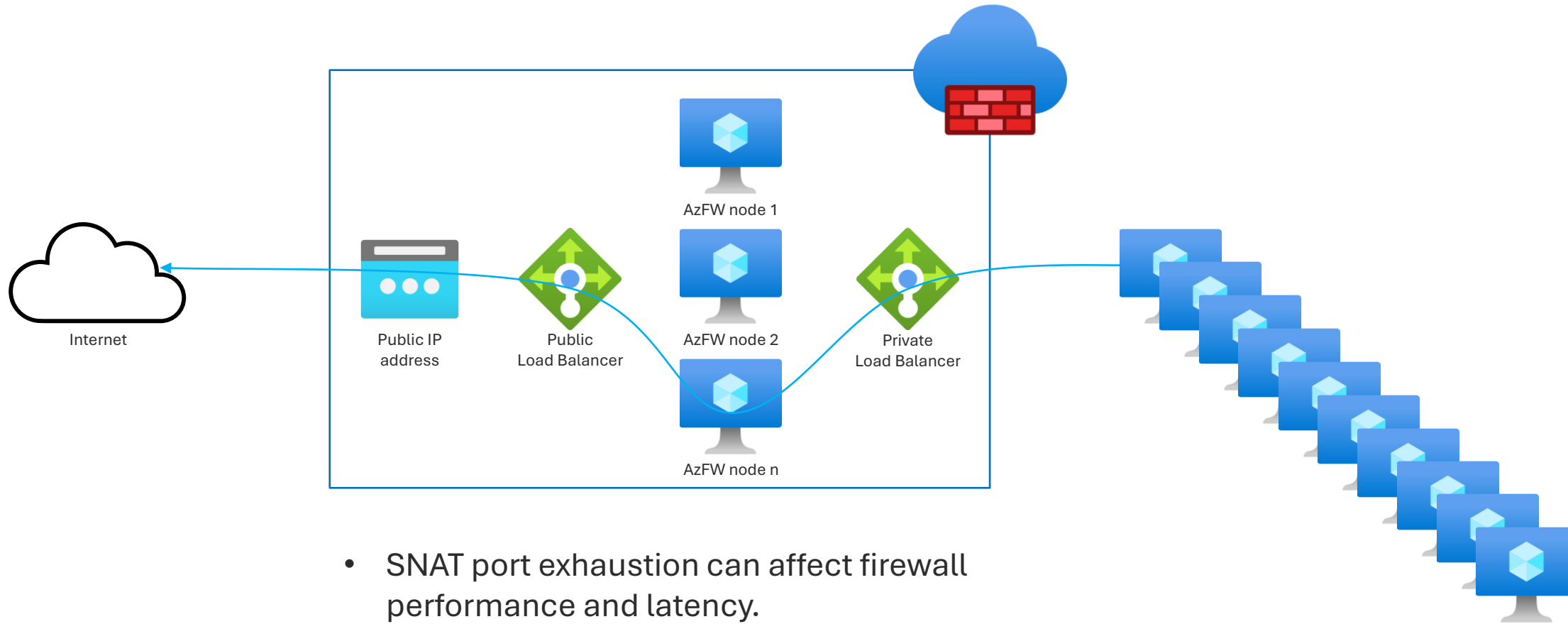
SOURCE NETWORK ADDRESS TRANSLATION

SNAT



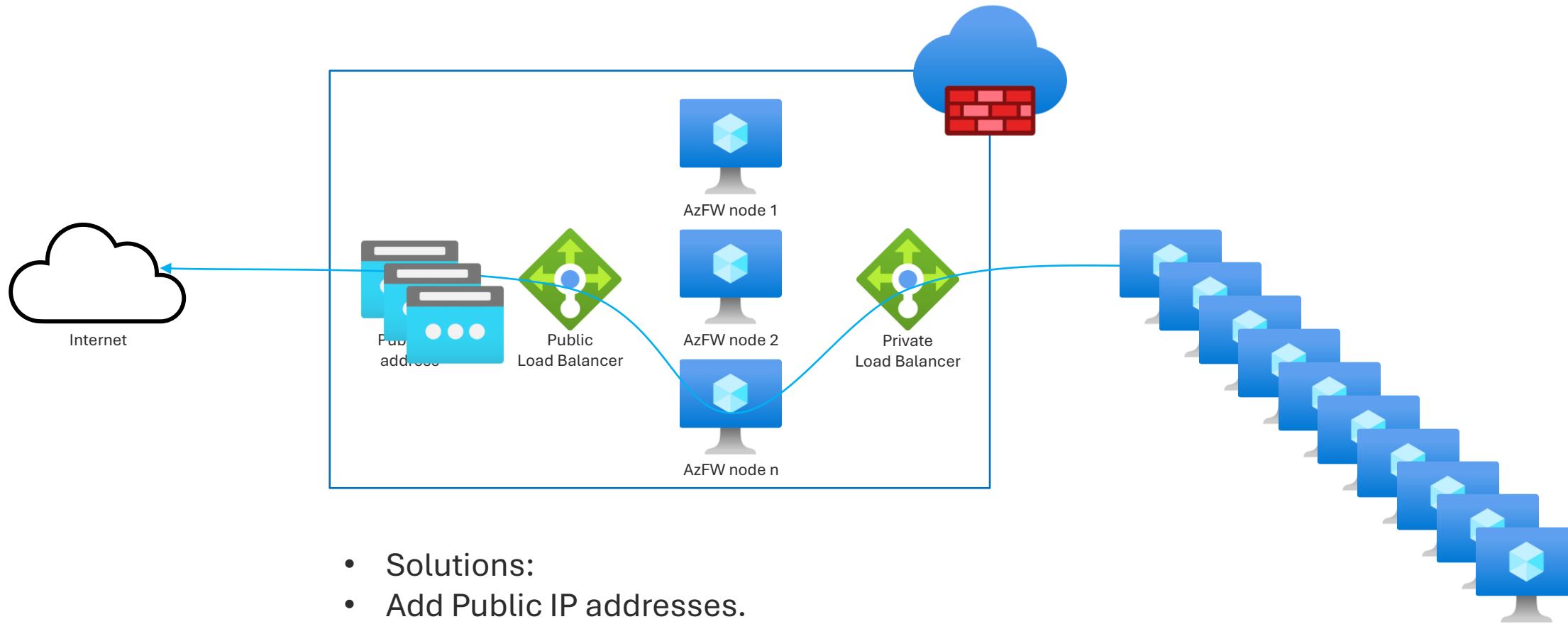
- Azure Firewall SNAT ports are limited to 2496 ports per Public IP and not 65K.

SNAT



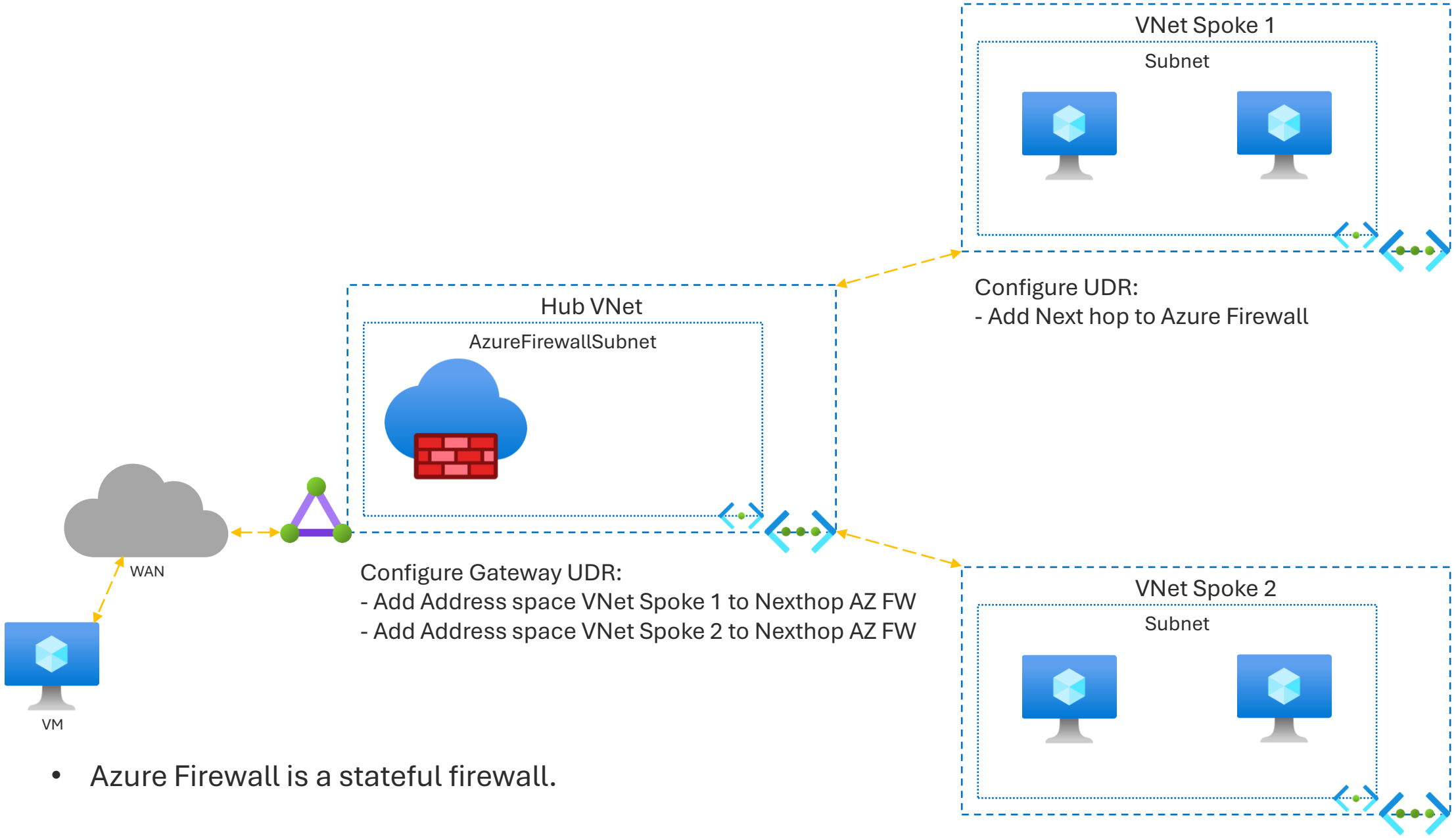
- SNAT port exhaustion can affect firewall performance and latency.
- AVD's are SNAT intensive.
- Monitor SNAT port Metric.

SNAT

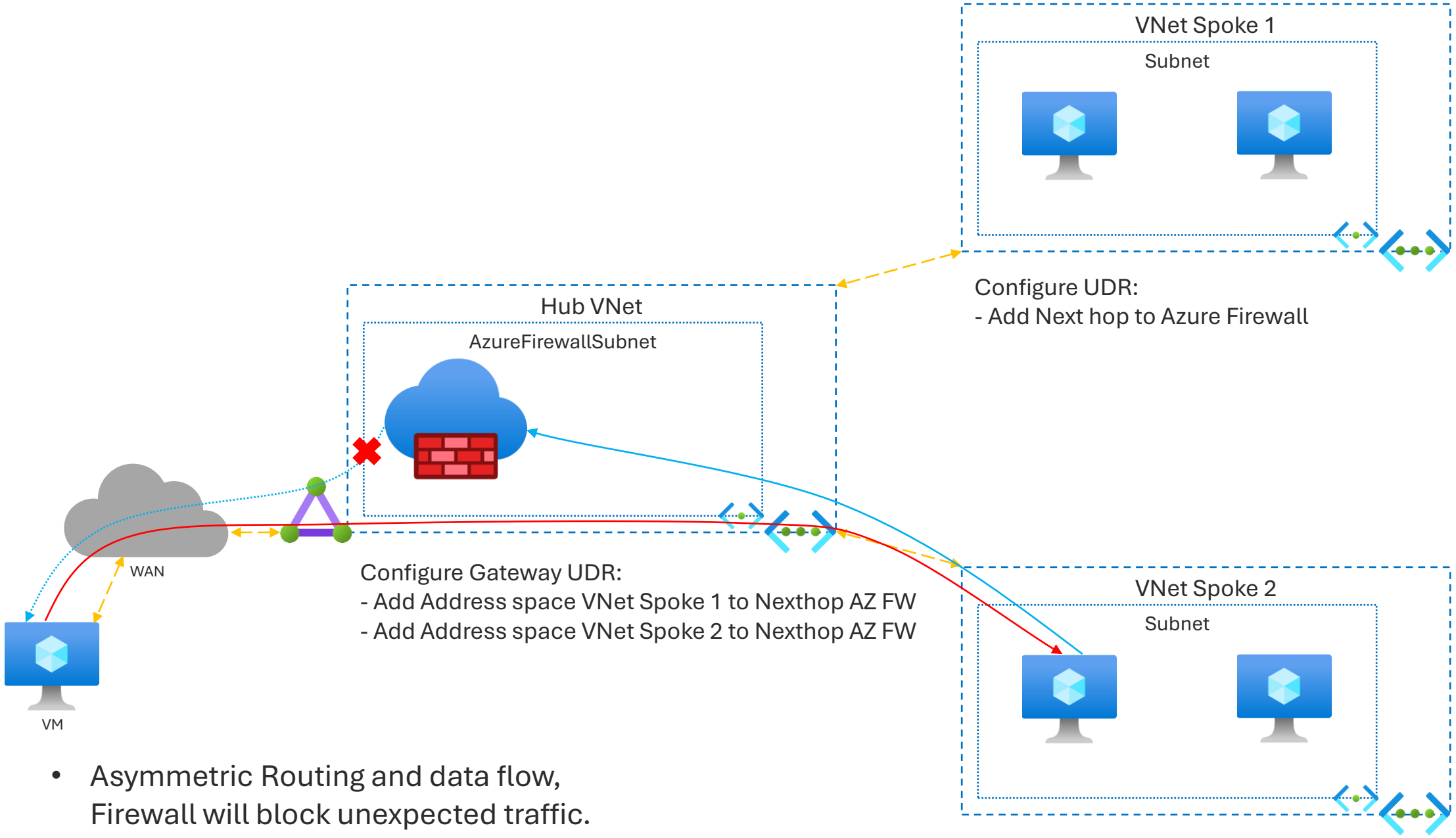


- Solutions:
- Add Public IP addresses.
- “Azure NAT Gateway”.

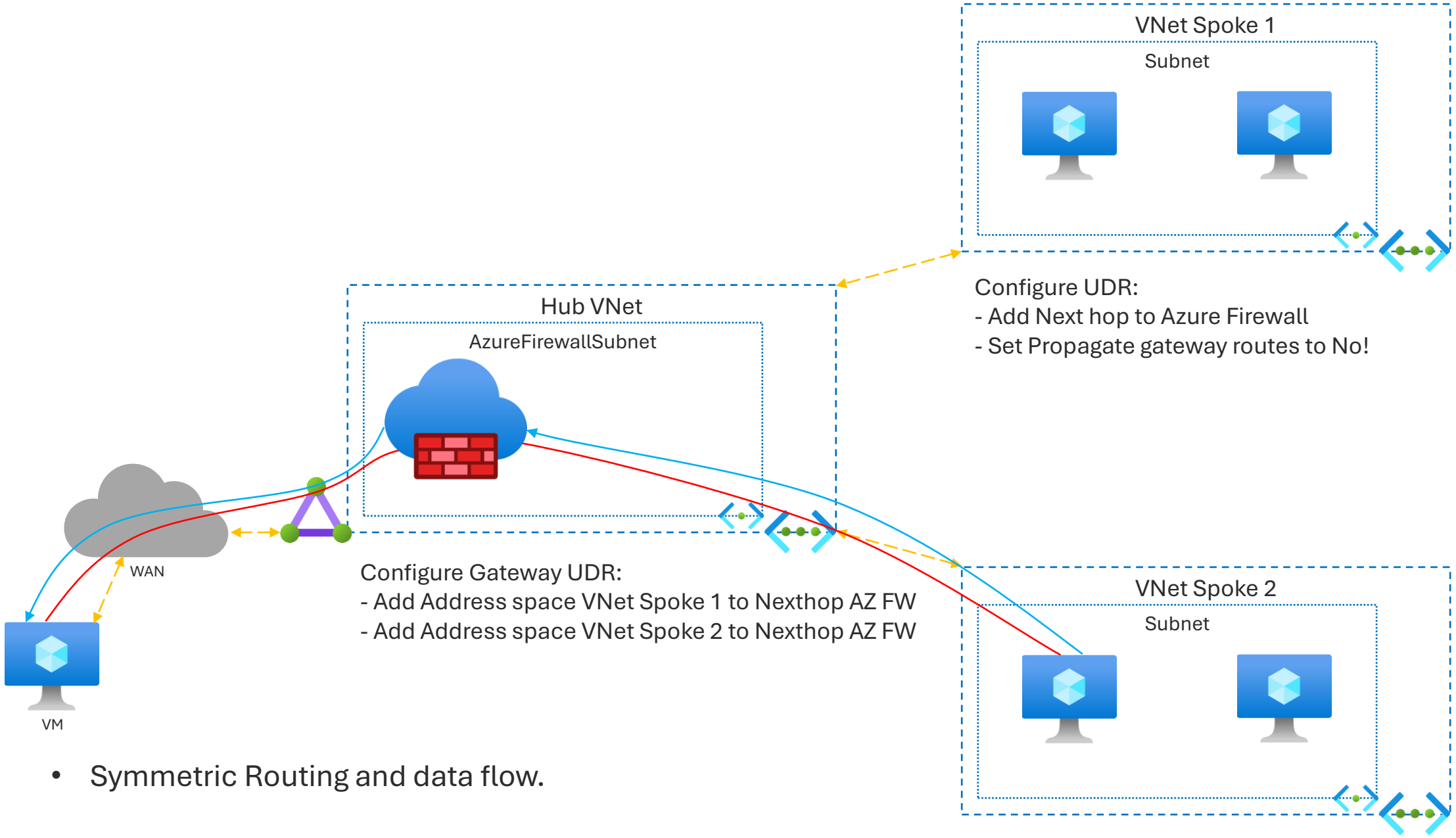
SYMMETRIC VS ASYMMETRIC ROUTING



- 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

```
1 // Network rule log data
2 // Parses the network rule log data.
3 AzureDiagnostics
4 | where Category == "AzureFirewallNetworkRule"
5 | where OperationName == "AzureFirewallNatRuleLog" or OperationName == "AzureFirewallNetworkRuleLog"
6 //case 1: for records that look like this:
7 //PROTO request from IP:PORT to IP:PORT.
8 | parse msg_s with Protocol " request from " SourceIP ":" SourcePortInt:int " to " TargetIP ":" TargetPortInt:int *
9 //case 1a: for regular network rules
10 | parse kind=regex flags=U msg_s with * ". Action\\: " Action1a "\\."
11 //case 1b: for NAT rules
12 //TCP request from IP:PORT to IP:PORT was DNAT'ed to IP:PORT
13 | parse msg_s with * " was " Action1b:string " to " TranslatedDestination:string ":" TranslatedPort:int *
14 //Parse rule data if present
15 | parse msg_s with * ". Policy: " Policy ". Rule Collection Group: " RuleCollectionGroup "." *
16 | parse msg_s with * " Rule Collection: " RuleCollection ". Rule: " Rule
17 //case 2: for ICMP records
18 //ICMP request from 10.0.2.4 to 10.0.3.4. Action: Allow
19 | parse msg_s with Protocol2 " request from " SourceIP2 " to " TargetIP2 ". Action: " Action2
20 | extend
21 SourcePort = toString(SourcePortInt),
22 TargetPort = toString(TargetPortInt)
23 | extend
24 Action = case(Action1a == "", case(Action1b == "", Action2, Action1b), split(Action1a, ".")[0]),
25 Protocol = case(Protocol == "", Protocol2, Protocol),
26 SourceIP = case(SourceIP == "", SourceIP2, SourceIP),
27 TargetIP = case(TargetIP == "", TargetIP2, TargetIP),
28 //ICMP records don't have port information
29 SourcePort = case(SourcePort == "", "N/A", SourcePort),
30 TargetPort = case(TargetPort == "", "N/A", TargetPort),
31 //Regular network rules don't have a DNAT destination
32 TranslatedDestination = case(TranslatedDestination == "", "N/A", TranslatedDestination),
33 TranslatedPort = case(isnull(TranslatedPort), "N/A", toString(TranslatedPort)),
34 //Rule information
35 Policy = case(Policy == "", "N/A", Policy),
36 RuleCollectionGroup = case(RuleCollectionGroup == "", "N/A", RuleCollectionGroup),
37 RuleCollection = case(RuleCollection == "", "N/A", RuleCollection),
38 Rule = case(Rule == "", "N/A", Rule)
39 | 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-prd-fw	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-prd-fw	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-prd-fw	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-fw	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-prd-fw	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-prd-fw	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: FirewallPolicy_ev-hub-prd-fw	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: FirewallPolicy_ev-hub-prd-fw	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.

Diagnostic setting ...

 Save  Discard  Delete  Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name AzureFWLogs

Logs

Category groups ⓘ

☐ allLogs

Categories

- ☒ Azure Firewall Network Rule
- ☒ Azure Firewall Application Rule
- ☒ Azure Firewall Nat Rule
- ☒ Azure Firewall Threat Intelligence
- ☒ Azure Firewall IDPS Signature
- ☒ Azure Firewall DNS query
- ☒ Azure Firewall FQDN Resolution Failure
- ☒ Azure Firewall Fat Flow Log
- ☒ Azure Firewall Flow Trace Log
- ☒ Azure Firewall Network Rule Aggregation (Policy Analytics)
- ☒ Azure Firewall Application Rule Aggregation (Policy Analytics)
- ☒ Azure Firewall Nat Rule Aggregation (Policy Analytics)

Destination details

☒ Send to Log Analytics workspace

Subscription

Cloud & Cybersecurity testomgeving

Log Analytics workspace

ev-LogAnalytics (westeurope)

Destination table ⓘ

☐ Azure diagnostics ☒ Resource specific

☐ Archive to a storage account

☐ Stream to an event hub

☐ Send to partner solution

STRUCTURED AZURE FIREWALL LOGS

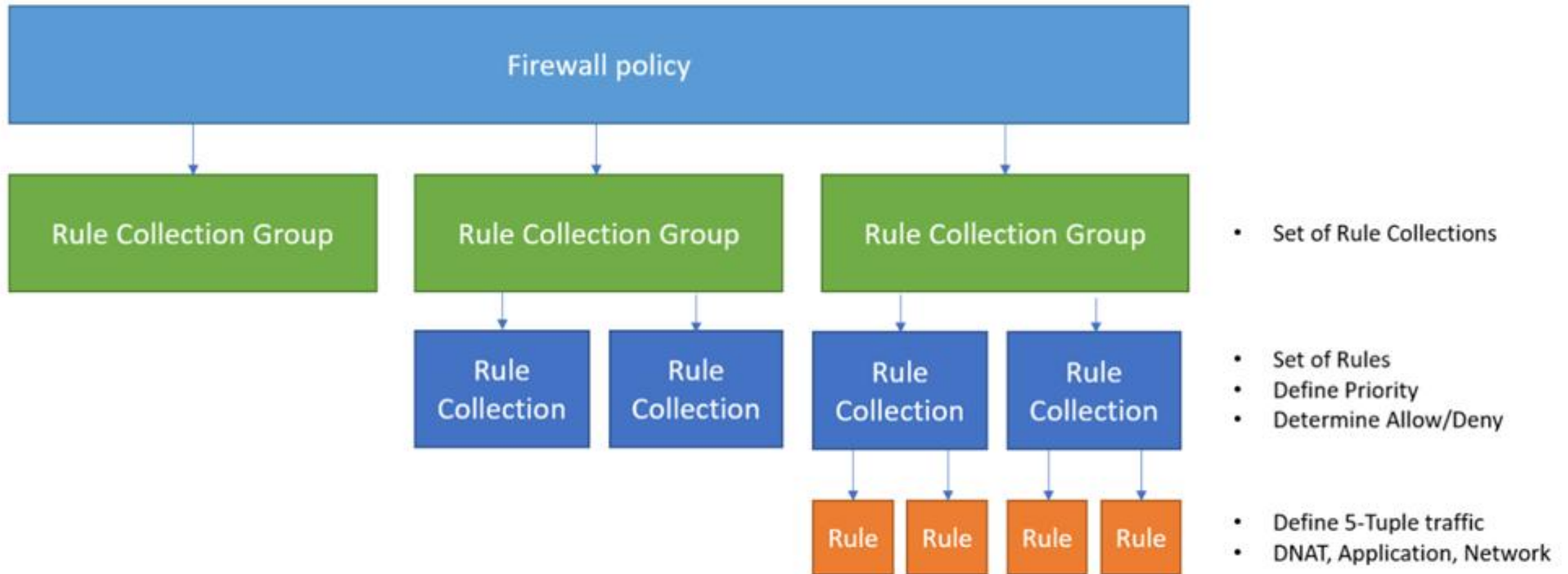
```
1 // Network rule logs
2 // Packets that matched Network rules. Both packet and rule metadata is displayed.
3 AZFWNetworkRule
4 | take 100
```

ResultsChart

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

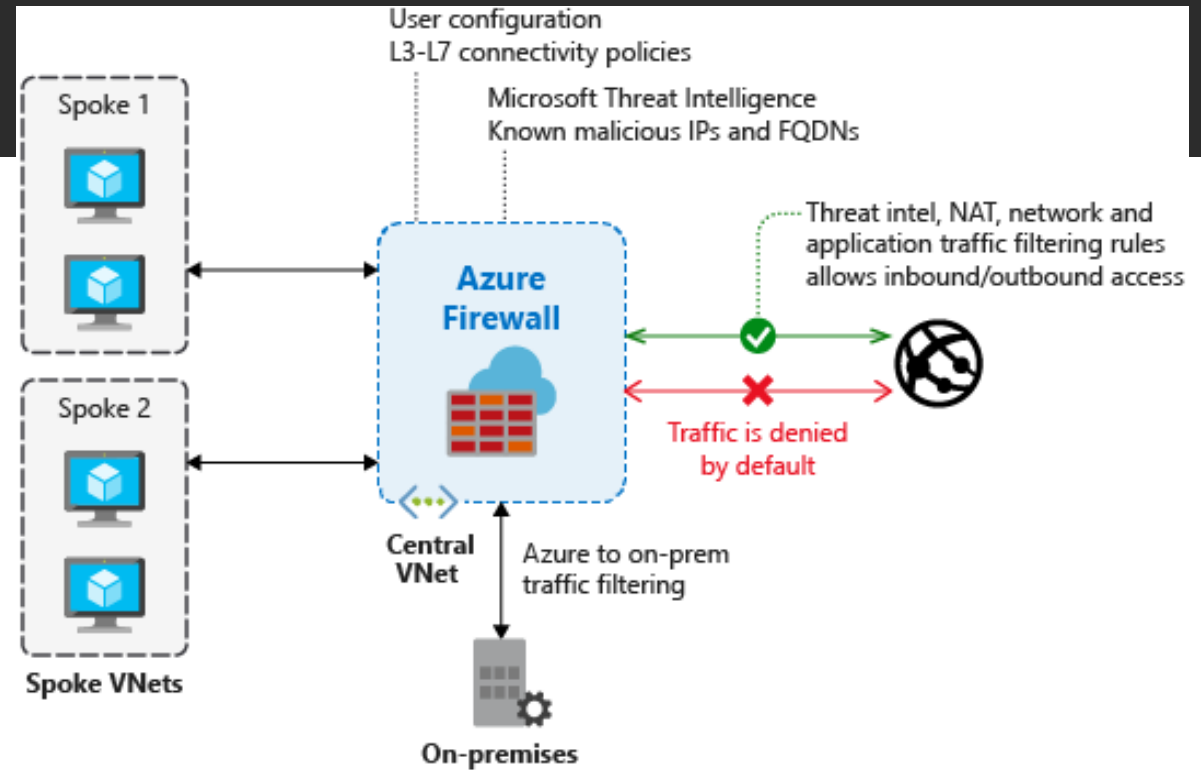
CLASSIC VS POLICY



- 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

default-prd-afwp | Policy Analytics

Firewall Policy

Search

Overview

Activity log

Access control (IAM)

Tags

Management

Rules

- Rule collections
- DNAT rules
- Network rules
- Application rules

Settings

- Parent policy
- DNS
- Threat Intelligence
- TLS inspection
- IDPS
- Private IP ranges (SNAT)
- Secured virtual hubs
- Secured virtual networks
- Web categories
- Explicit proxy (preview)

Monitoring

- Policy Analytics
- Properties
- Locks
- Automation
- Help

Insights

DNAT rules

Network rules

Application rules

Traffic flows

Single-rule analysis

Refresh

Configure Workspaces

See all recommendations

Policy limits

2,045 Rules

5,548 Unique source/destination

1 IP groups

20,000 Max

200 Max

Rules with multiple IP addresses

11 Rules with more than 10 source IPs

21 Rules with more than 10 destination IPs

2,045 Total

2,045 Total

Rules with low utilization

621 Rules with no hits

2,045 Total

Static analysis

22 Redundant rules

14 Duplicated IP addresses

2,045 Total

2,045 Total

Generic rules

2 Rules with a wildcard in the source

36 Rules with a wildcard in the destination

2,045 Total

2,045 Total

Potentially malicious sources

Threat Intelligence

IDPS

Diagnostic setting

Save

Discard

Delete

Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you and one or more destinations that you would stream them to. Normal usage charges for [more about the different log categories and contents of those logs](#)

Diagnostic setting name

LogsAndMetricsToLogAnalytics

Logs

Category groups

allLogs

Categories

☒ Azure Firewall Network Rule

☒ Azure Firewall Application Rule

☒ Azure Firewall Nat Rule

☒ Azure Firewall Network Rule Aggregation (Policy Analytics)

☒ Azure Firewall Application Rule Aggregation (Policy Analytics)

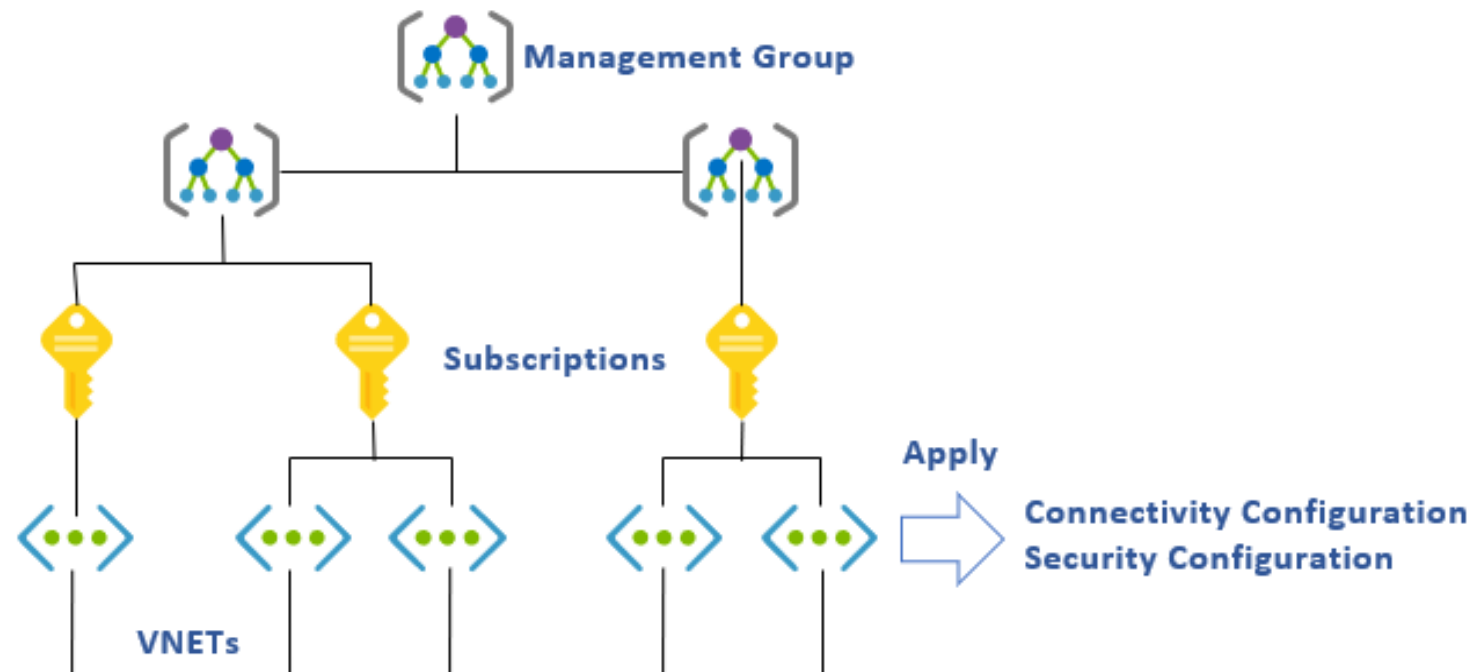
☒ Azure Firewall Nat Rule Aggregation (Policy Analytics)

- 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!