

WorkshopPLUS- Networking Essentials

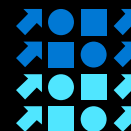
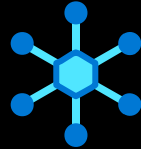
Module # 4
Monitor

CONNECT & EXTEND

Virtual Networks
Routing/NSGs
ExpressRoute/VPN
Virtual WAN

MONITOR

Azure Monitor
Azure Network Watcher



Azure Networking services

Adjust and strengthen
your Network

PROTECT

Bastion
Azure Firewall
DDoS Protection
Web Application Firewall
PrivateLink/Private Endpoints

DELIVER

DNS, Azure Load Balancer
Traffic Manager
Application Gateway
CDN/Azure Front Door

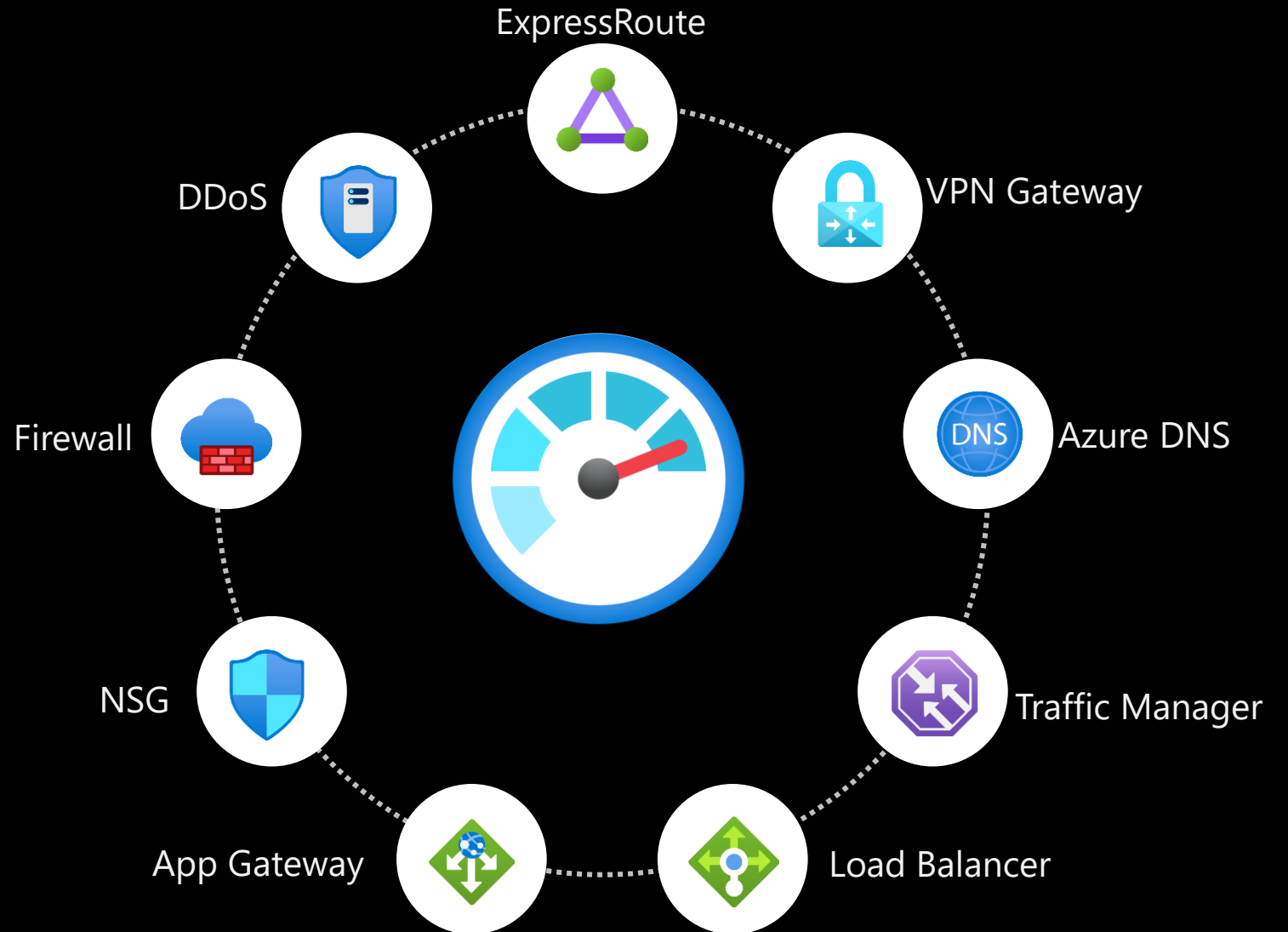
Azure Monitor



Azure Monitor

What's available

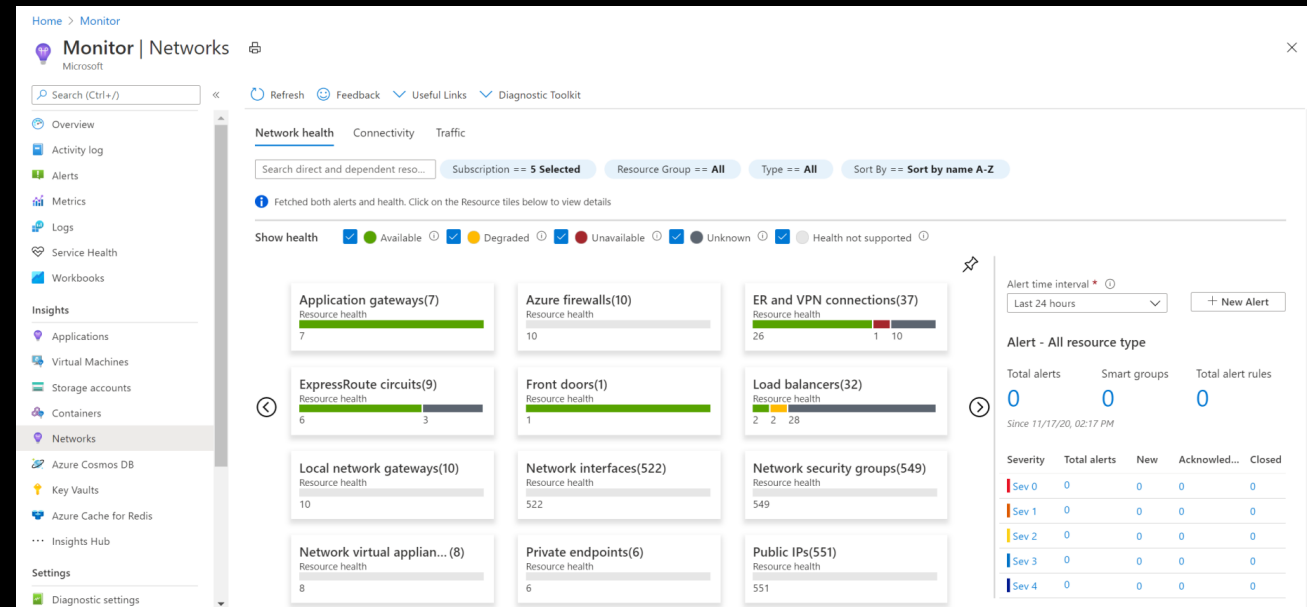
- ✓ Utilization
- ✓ Status (success/fail)
- ✓ Health
- ✓ Operating metrics
- ✓ Logs



What is Azure Monitor?

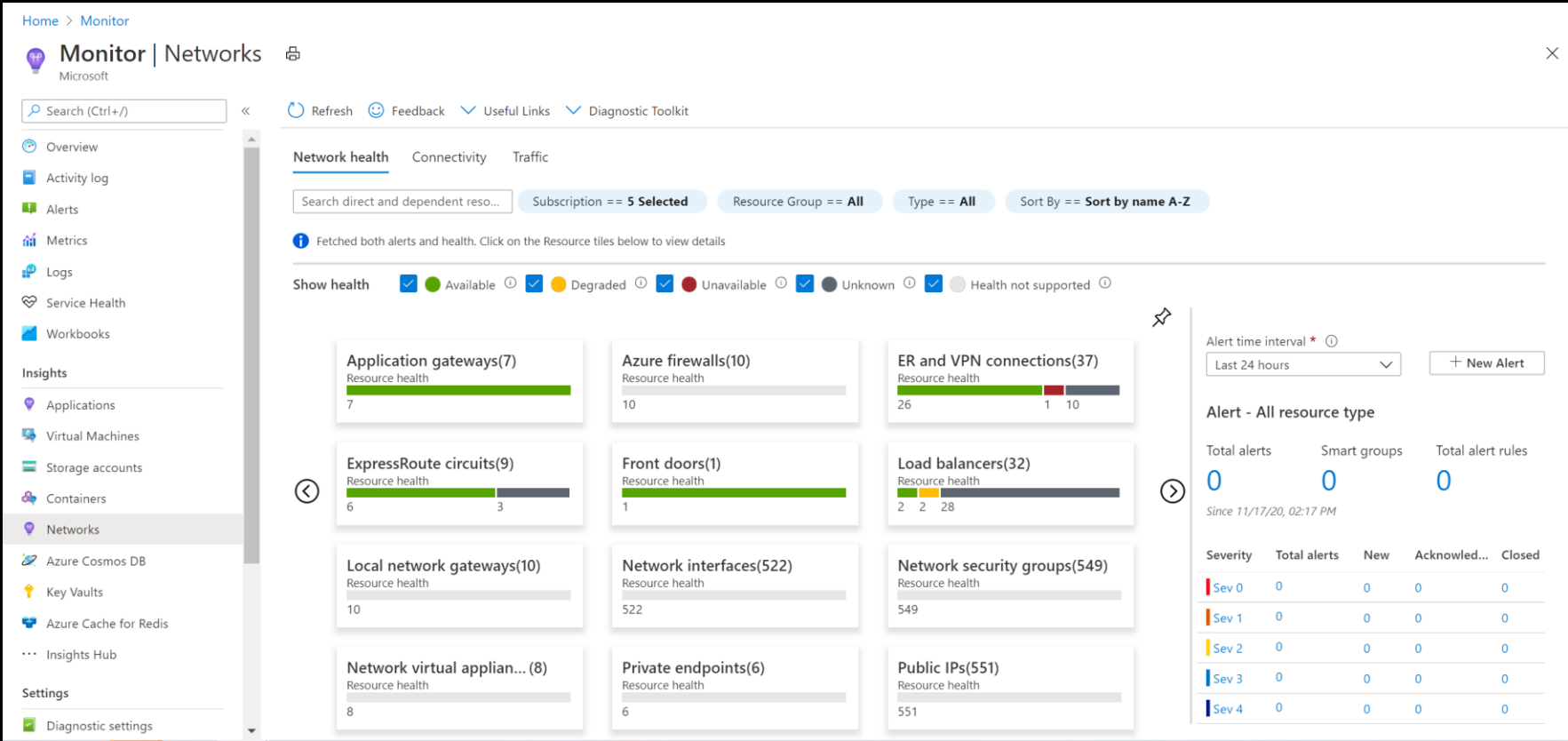
- Azure Monitor for Networks is structured around:

- Network Health/Metrics
- Connectivity
- Traffic



Network Insights

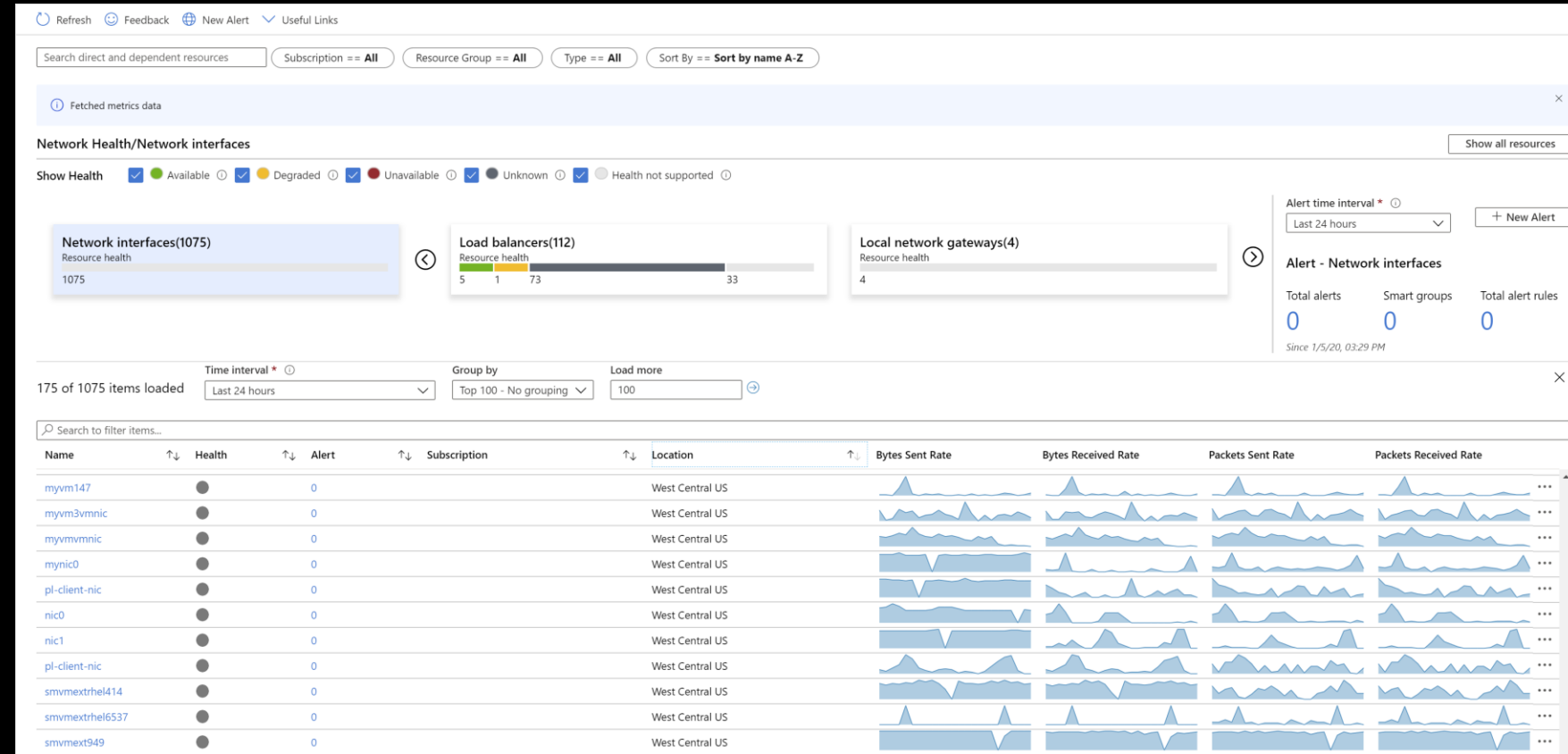
Single health, metric and alert console for your entire cloud network.



Network Insights

Single health, metric and alert console for your entire cloud network.

No agent/configuration required

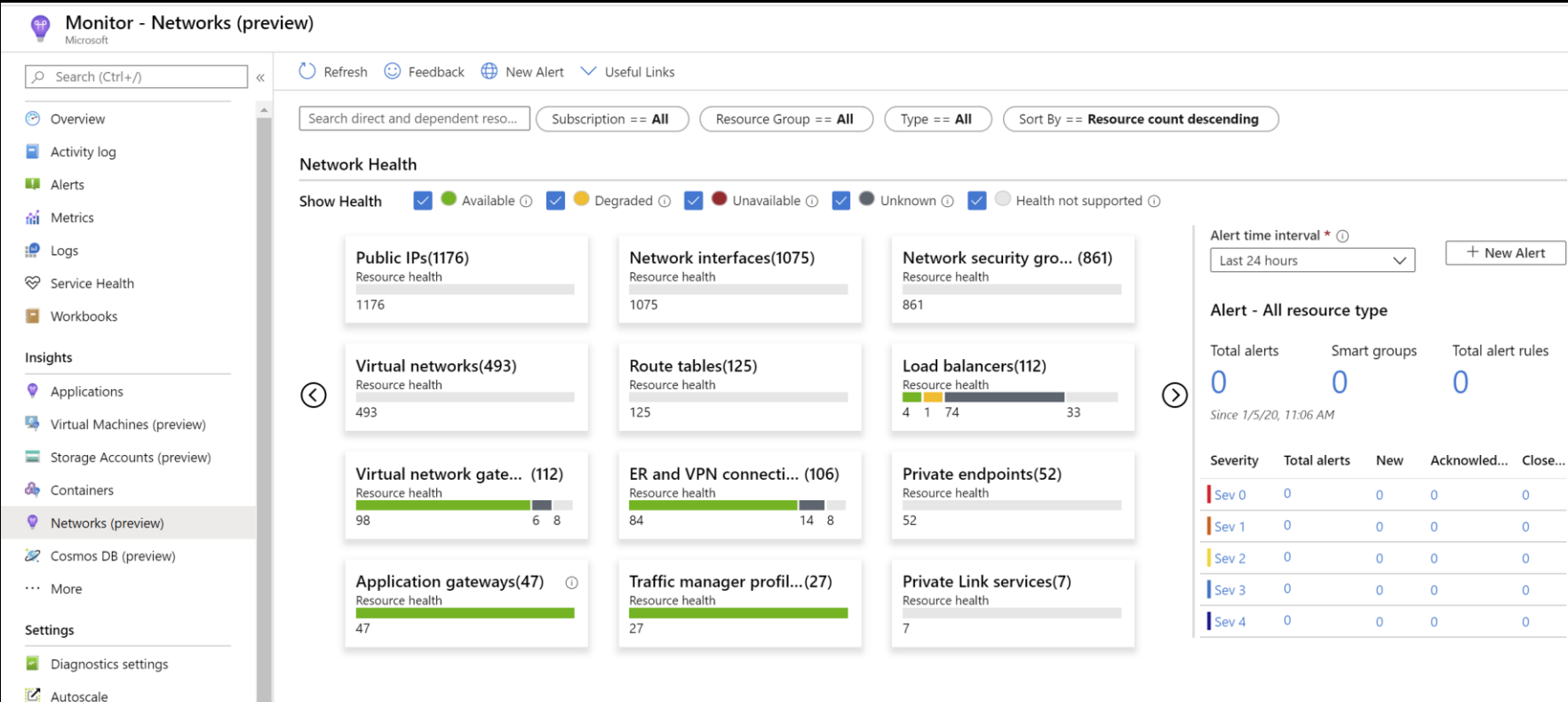


Network Insights

Single health, metric and alert console for your entire cloud network.

No agent/configuration required

Search resource properties for associated resources and dependencies



Network Insights

Single health, metric and alert console for your entire cloud network.

No agent/configuration required

Search resource properties for associated resources and dependencies

The screenshot displays the Microsoft Azure Network Insights dashboard. At the top, there are navigation links: Refresh, Feedback, New Alert, and Useful Links. Below these is a search bar containing the text 'hrweb', followed by filter buttons for Subscription (All), Resource Group (All), Type (All), and Sort By (Sort by name A-Z). A status bar indicates 'Search operation completed'. The main section is titled 'Network Health/ Searched results' and includes a 'Show Health' toggle and a legend for resource health: Available (green), Degraded (yellow), Unavailable (red), Unknown (grey), and Health not supported (light grey). The results are presented in five cards: 'Application gateways(1)' with a green health bar and count of 1; 'Network interfaces(21)' with a grey health bar and count of 21; 'Network security groups(3)' with a grey health bar and count of 3; 'Public IPs(3)' with a grey health bar and count of 3; and 'Virtual networks(2)' with a grey health bar and count of 2.

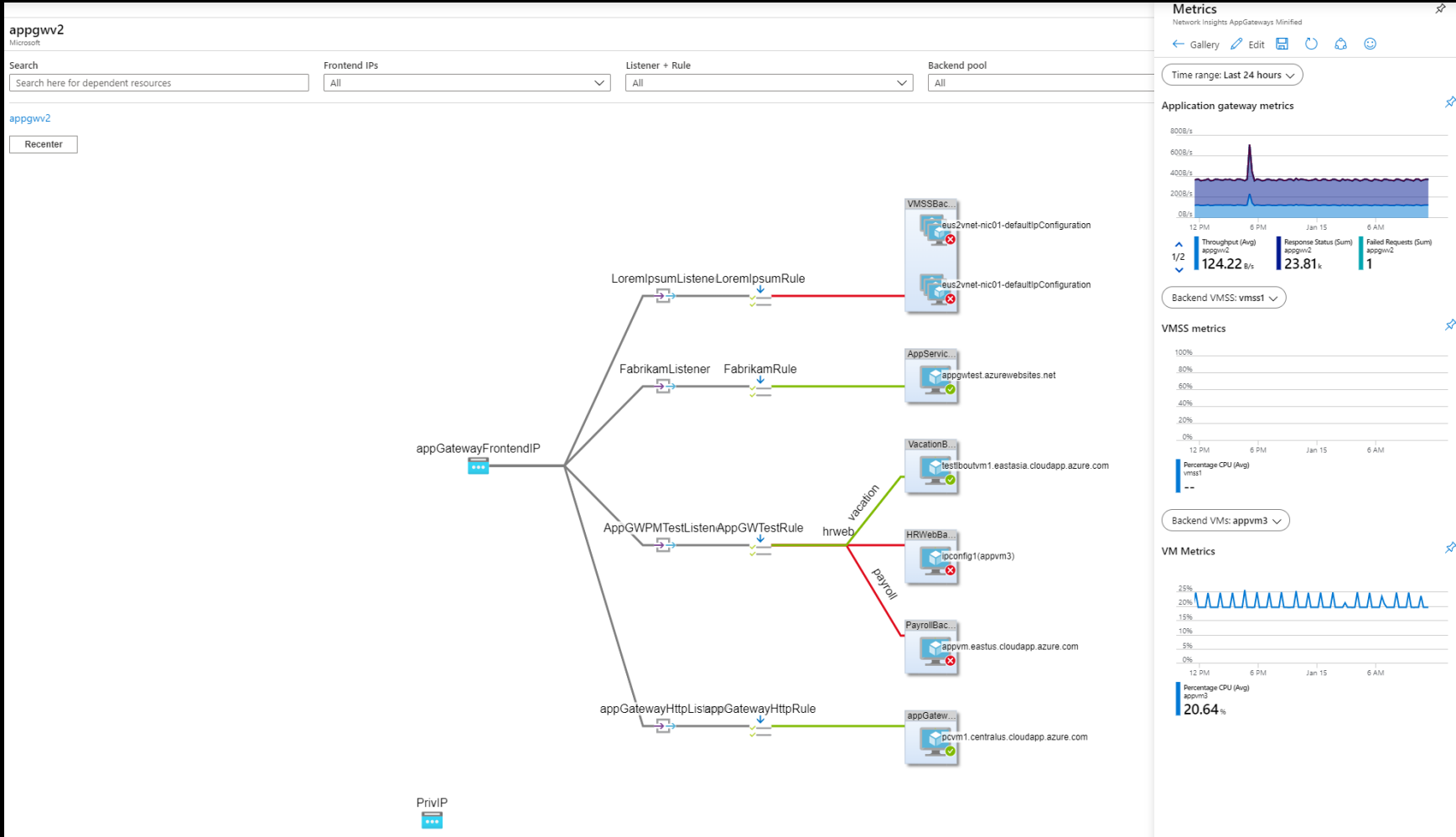
Network Insights

Single health, metric and alert console for your entire cloud network.

No agent/configuration required

Search resource properties for associated resources and dependencies

Visualize the structure and functional dependencies of network resources



Network Insights

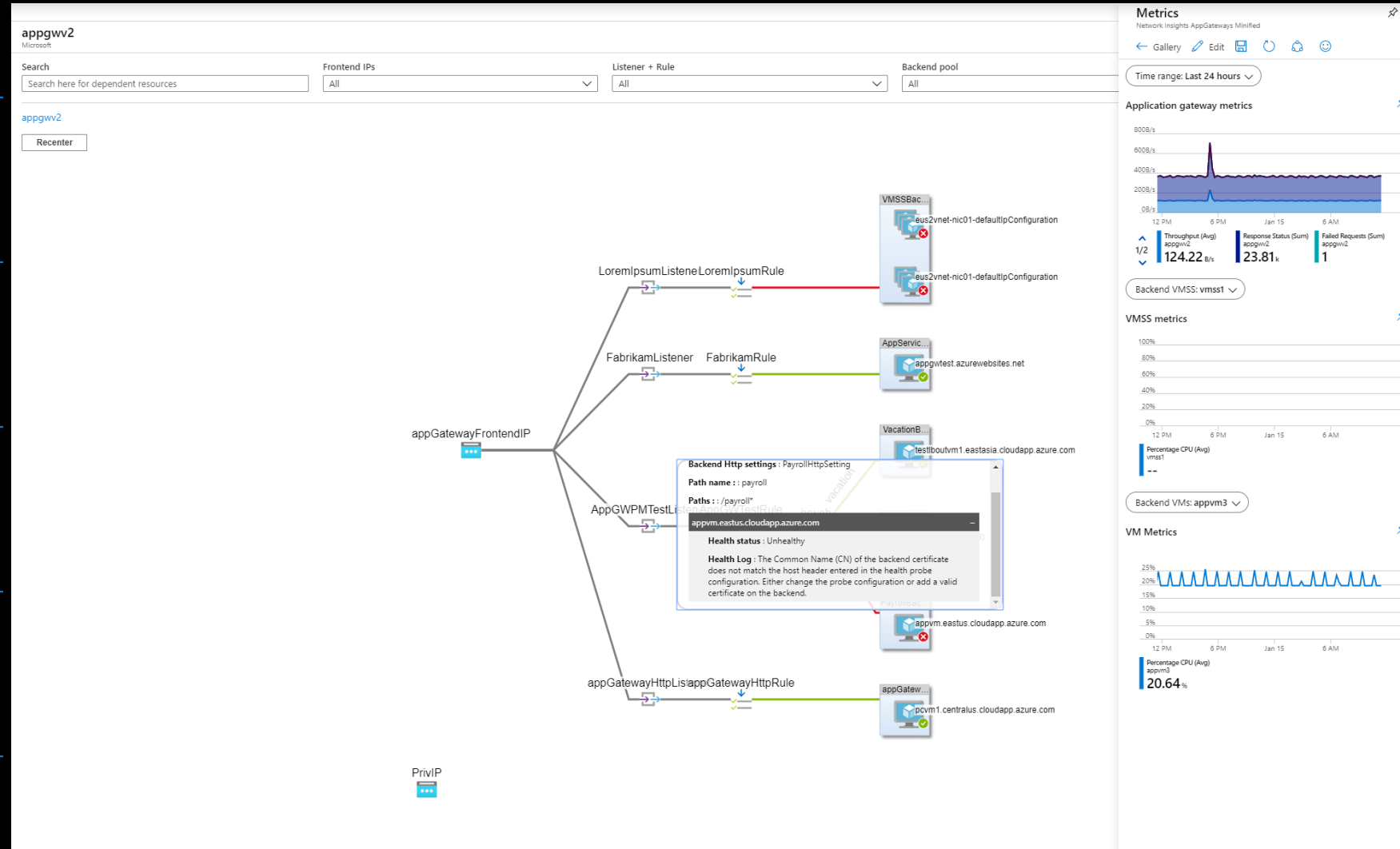
Single health, metric and alert console for your entire cloud network.

No agent/configuration required

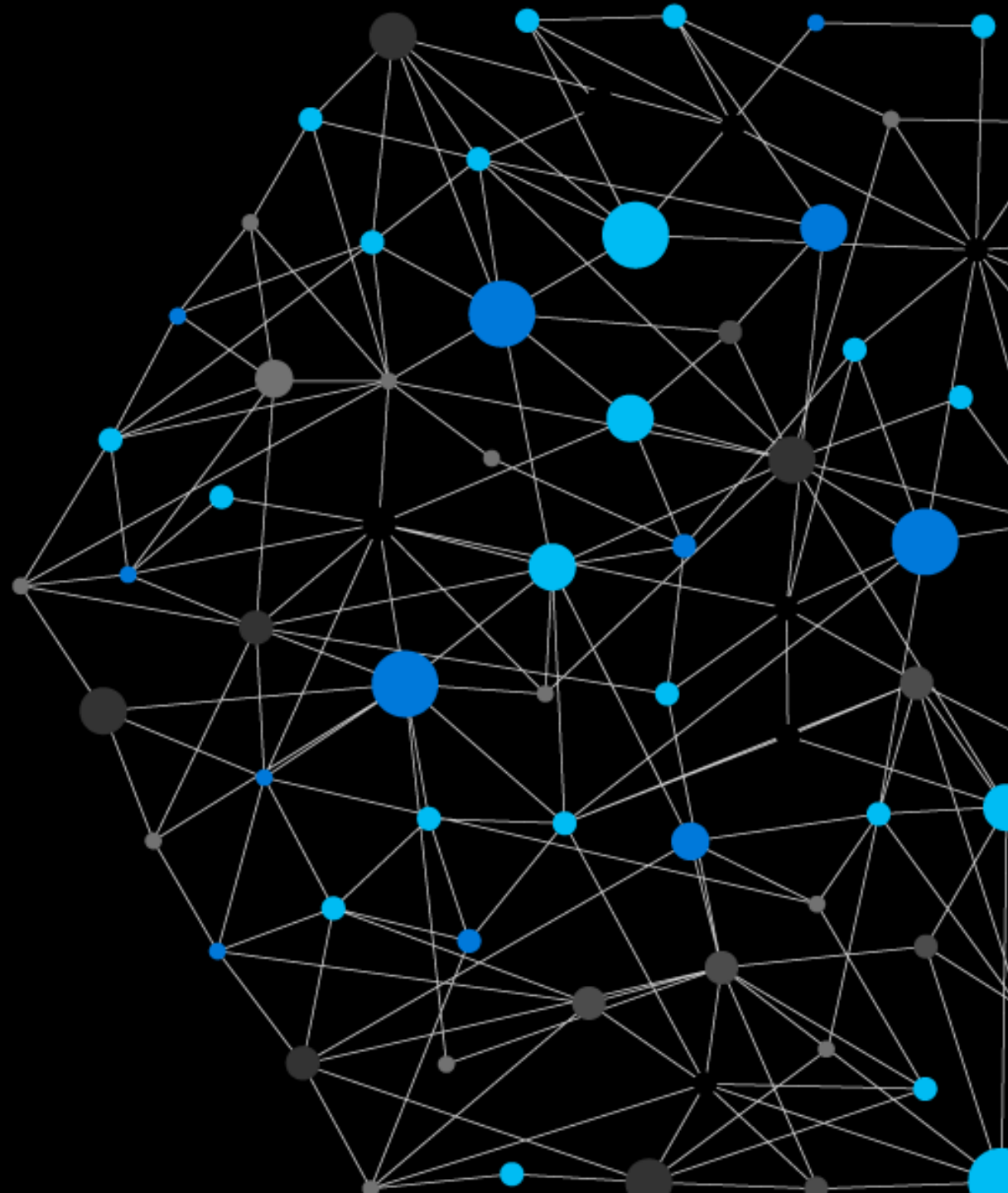
Search resource properties for associated resources and dependencies

Visualize the structure and functional dependencies for Application Gateway

Get resource-specific diagnostic and troubleshooting help

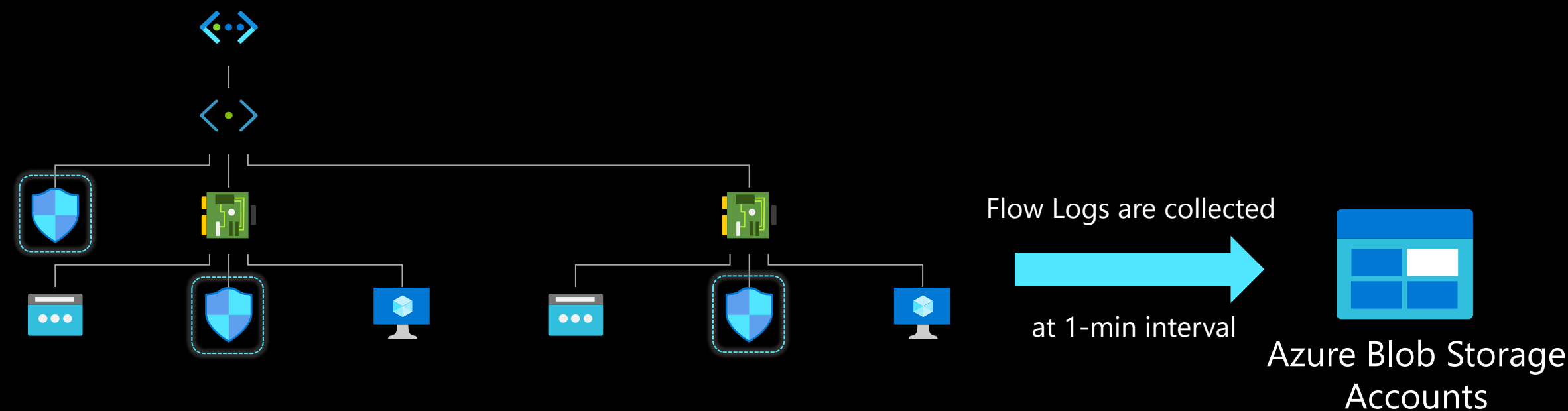


Traffic Monitoring



NSG Flow logs

NSG Flow logs are a record of NSG behavior



NSG Flow logs



Multi-subscription support for flow log storage



All traffic reaching NSGs is captured



No impact on network performance or bandwidth

5 tuple flows for traffic allowed/denied with bytes and packets

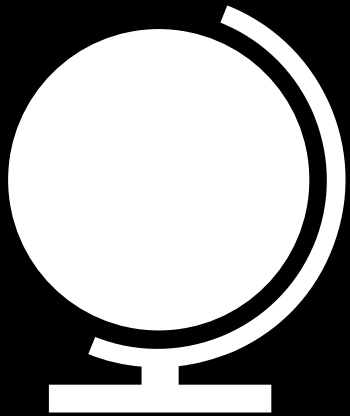
"1584032449,10.0.0.5,20.45.123.90,37848,443,T,O,A,C,14,3564,16,10115",

1584032449	10.0.0.5	20.45.123.90	37848	443	T	O	A	C	14	3564	16	10115
Timestamp UNIX epoch	Source IP	Destination IP	Source Port	Destination Port	Protocol T = TCP U = UDP	Traffic Flow I = Inbound O = Outbound	Traffic Decision A = Allowed D = Denied	Flow State B = Begin C = Continue E = End	Packets Source to Destination	Bytes Source to Destination	Packets Destination to Source	Bytes Destination to Source

Version 1

Version 2

NSG Flow logs Use cases



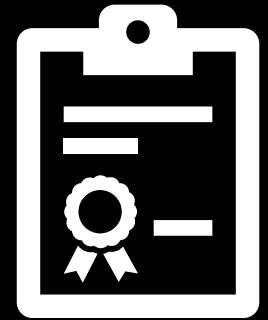
**Traffic Pattern
Analysis**



**Usage monitoring
& optimization**



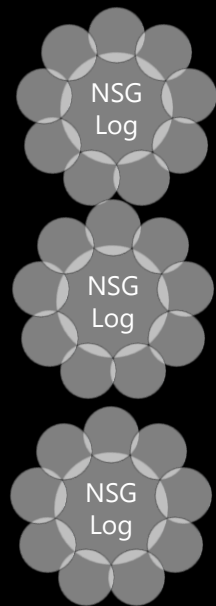
Compliance



**Network forensics
& Security analysis**

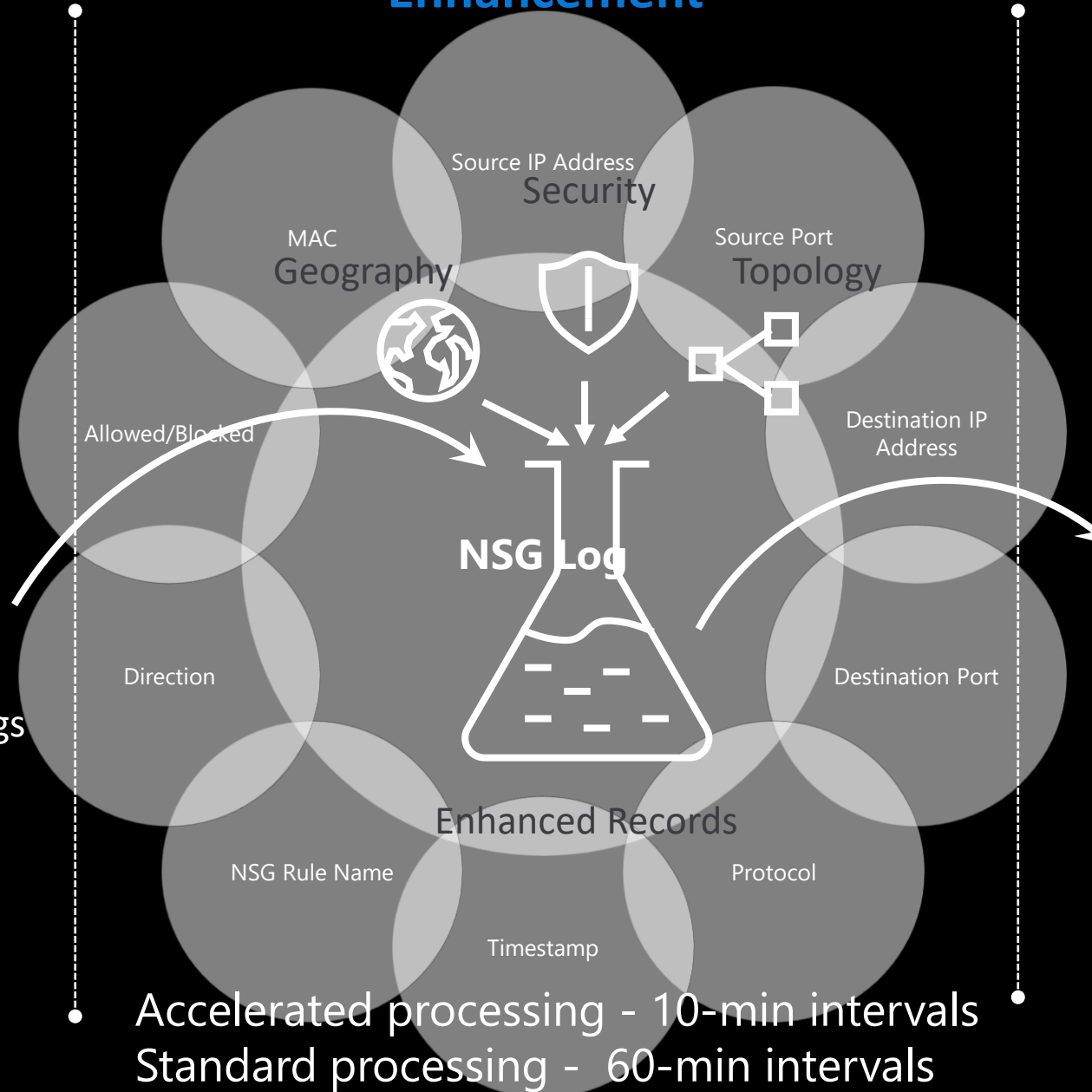
Traffic Analytics

Aggregation



Reduced Logs

Enhancement



Analytics

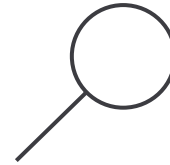


Traffic Analytics Capabilities



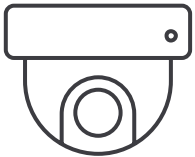
Traffic Distribution

- Geo Region and Country
- Azure datacenter
- Virtual Network



Network Telemetry

- NSG Rule hit count
- VPN Gateway utilization
- Allowed/Blocked traffic



Network Security

- Identify Malicious flows
- Ports Active on Internet
- Host Trying to Access Internet



Traffic Hotspots

- Top talking hosts
- Top accessed ports/protocols
- Most frequent conversations
- Virtual Networks with most traffic

Azure Network Watcher



What is Azure Network Watcher?

Azure Network Watcher is a collection of tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.

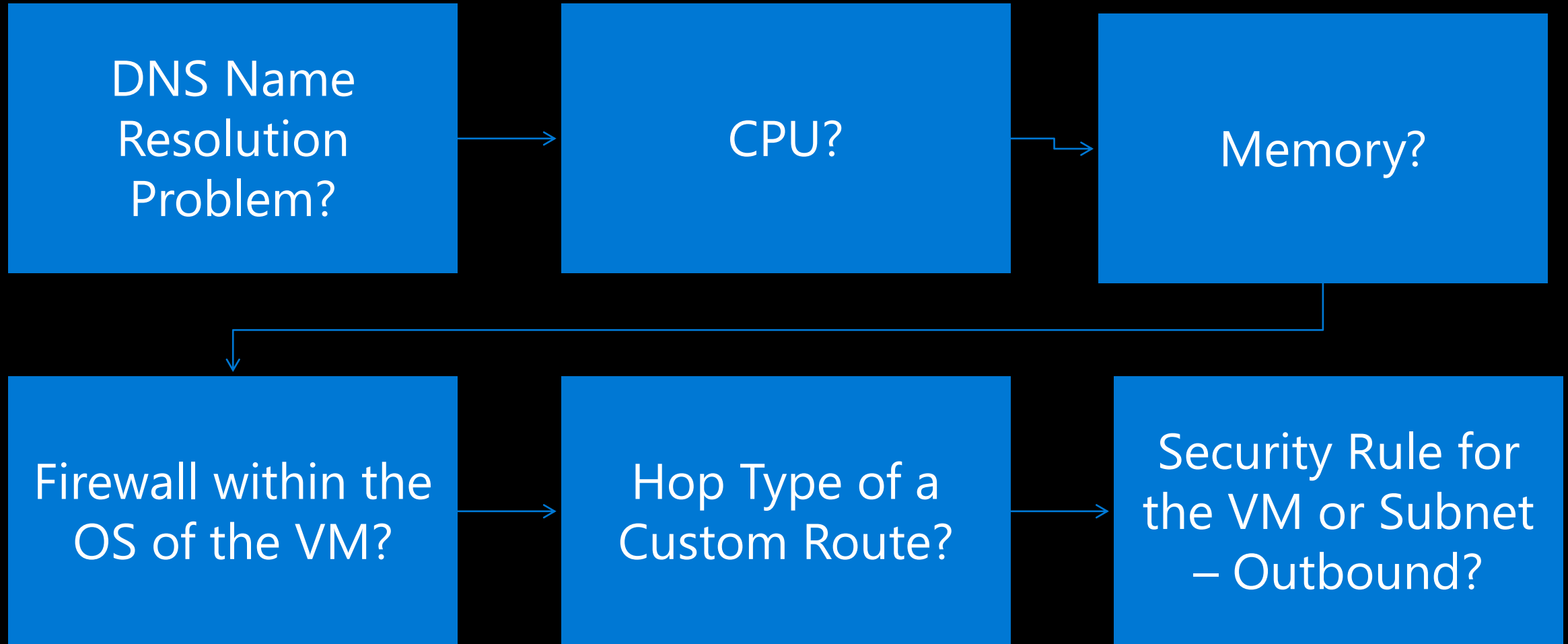


Monitoring Endpoints:

- Another Virtual Machine
 - A fully-qualified domain name (FQDN)
 - A Uniform Resource Identifier (URI)
 - IPv4 Address
-
- **Connection Monitor:** Allows the capability to monitor communication at a regular interval and inform you of reachability, latency, and network topology changes between the VM and the endpoint.



Why is an endpoint unreachable?



Network diagnostic tools: IP flow verify

Network Watcher
Microsoft

Search (Ctrl+/) <<

Overview

Monitoring

- Topology
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify**
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

Network diagnostic tools: Packet capture

Network Watcher
Microsoft

Search (Ctrl+*/*)

Overview

Monitoring

- Topology
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture**
- Connection troubleshoot

Metrics

- Usage + quotas

Logs

- NSG flow logs
- Diagnostic logs
- Traffic Analytics

Logs:

NSG Flow logs

Network Watcher


Microsoft




 Overview

Monitoring

 Topology


 Connection monitor


 Network Performance Monitor


Network diagnostic tools


 IP flow verify

 Next hop


 Effective security rules

 VPN troubleshoot

 Packet capture


 Connection troubleshoot

Metrics

 Usage + quotas

Logs

 NSG flow logs

 Diagnostic logs

 Traffic Analytics

Questions?



