Microsoft

Module 8

AZ-700T00A Design and Implement Network Monitoring

Module Overview

LA KQL → Dashboard → Alert

- Monitor your networks using Azure Monitor
- Exercise – Monitor a load balancer resource using Azure Monitor
- Use Azure Network Watcher to troubleshoot and analyze your network

Monitor your networks using Azure Monitor

Learning Objectives – Monitor your networks using Azure Monitor

- What is Azure Monitor?
- Metrics explorer
- Azure Monitor Network Insights
- Learning Recap

Azure Monitor

Built In

30 Tage

LA Log Analytics

Portal
Workbooks
KQL
Perf |

Perf Table

Data Lake

Kusto Query Lang

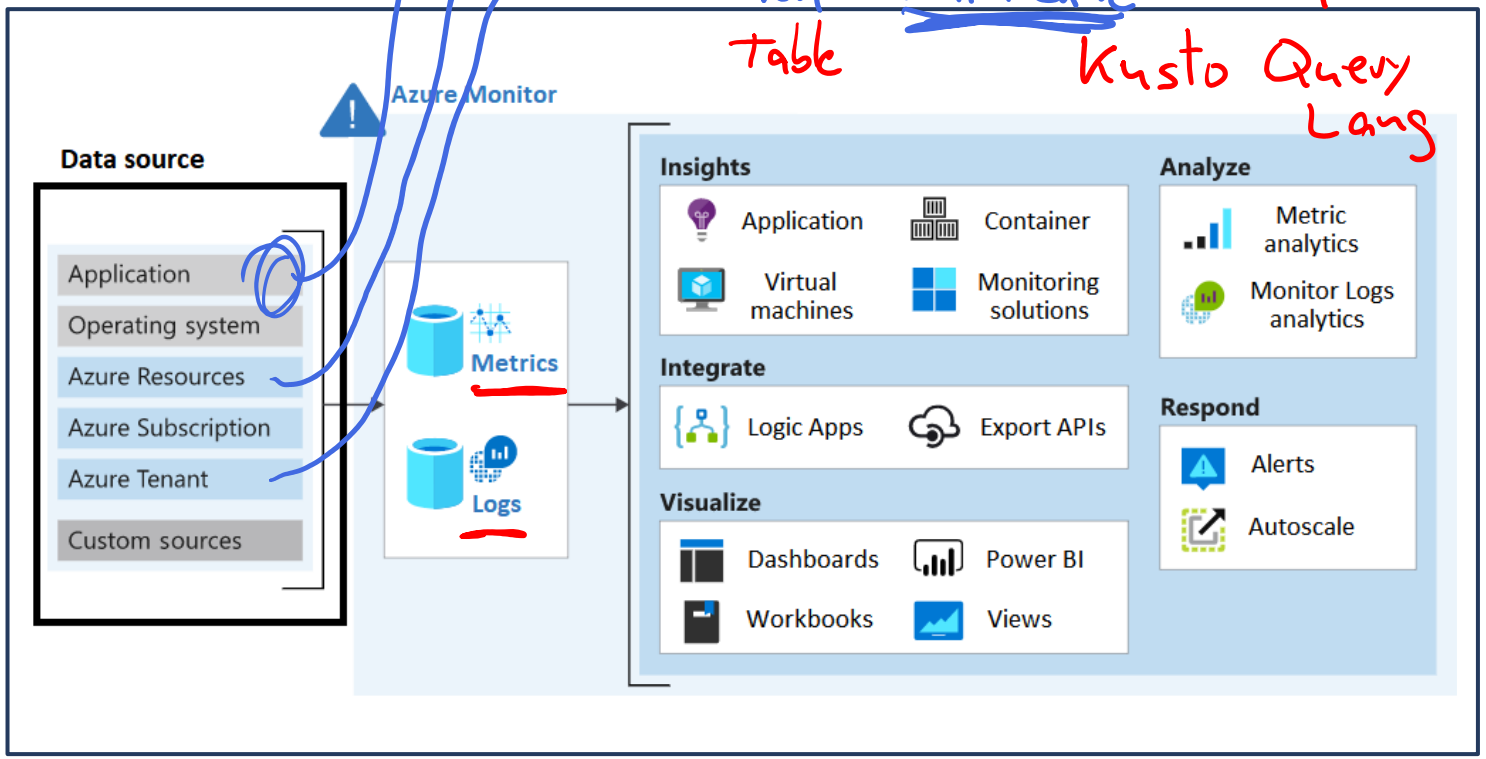
Monitoring data types: Metrics & Logs

Metrics are numerical values that describe some aspect of a system at a point in time

They are lightweight and capable of supporting near real-time scenarios

Logs contain different kinds of data organized into records with different sets of properties for each type

Telemetry (events, traces) and performance data can be combined for analysis



MS Sentinel
SIEM

~~Wins~~

Metrics explorer

VM

Agent
old: MMA
new: AMA — DCR — LA
Data Collection Rule

All services > All resources > CoreServicesVnet

All resources
Flexible Road LLC (skillup.tech)

Create | Manage view

Filter for any field...

Name

- Contoso-LB-AS
- Contoso-Public-IP
- Contoso-TMprofile
- Contoso-TMprofile-SR
- contoso.com
- CoreServicesVnet
- ManufacturingVM
- ManufacturingVM-ip
- ManufacturingVM-nsg
- manufacturingvm489
- ManufacturingVM_OsDisk_1_b3c65a...
- ManufacturingVnet
- myAppServicePlanEastUS
- myAppServicePlanWestEurope
- myAvailabilitySet
- myBastionHost
- myBastionIP
- myLoadBalancer
- myNSG
- myPublicIP

CoreServicesVnet | Metrics
Virtual network

Search (Ctrl+/)

- Subnets
- DDoS protection
- Firewall
- Security
- DNS servers
- Peerings
- Service endpoints
- Private endpoints
- Properties
- Locks

Monitoring

- Alerts
- Metrics
- Diagnostic settings
- Logs
- Connection monitor (classic)
- Diagram

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

New chart | Refresh | Share | Feedback | Local Time: Last 24 hours (Automatic - 5 minutes)

Max Inbound UDP packets DDoS for CoreServicesVnet

Add metric | Add filter | Apply splitting | Line chart | Drill into Logs | New alert rule | Pin to dashboard

Scope	Metric Namespace	Metric	Aggregation
CoreServicesVnet	Standard metrics	Inbound UDP packets ...	Max

- Inbound UDP bytes DDoS
- Inbound UDP bytes dropped DDoS
- Inbound UDP bytes forwarded DDoS
- Inbound UDP packets DDoS
- Inbound UDP packets dropped DDoS
- Inbound UDP packets forwarded DDoS
- Inbound UDP packets to trigger DDoS miti...

100/s, 90/s, 80/s, 70/s, 60/s, 50/s, 40/s, 30/s, 20/s, 10/s, 0/s

12 PM, 6 PM, Mon 21, 6 AM, UTC+01:00

Diag. Settings — LA

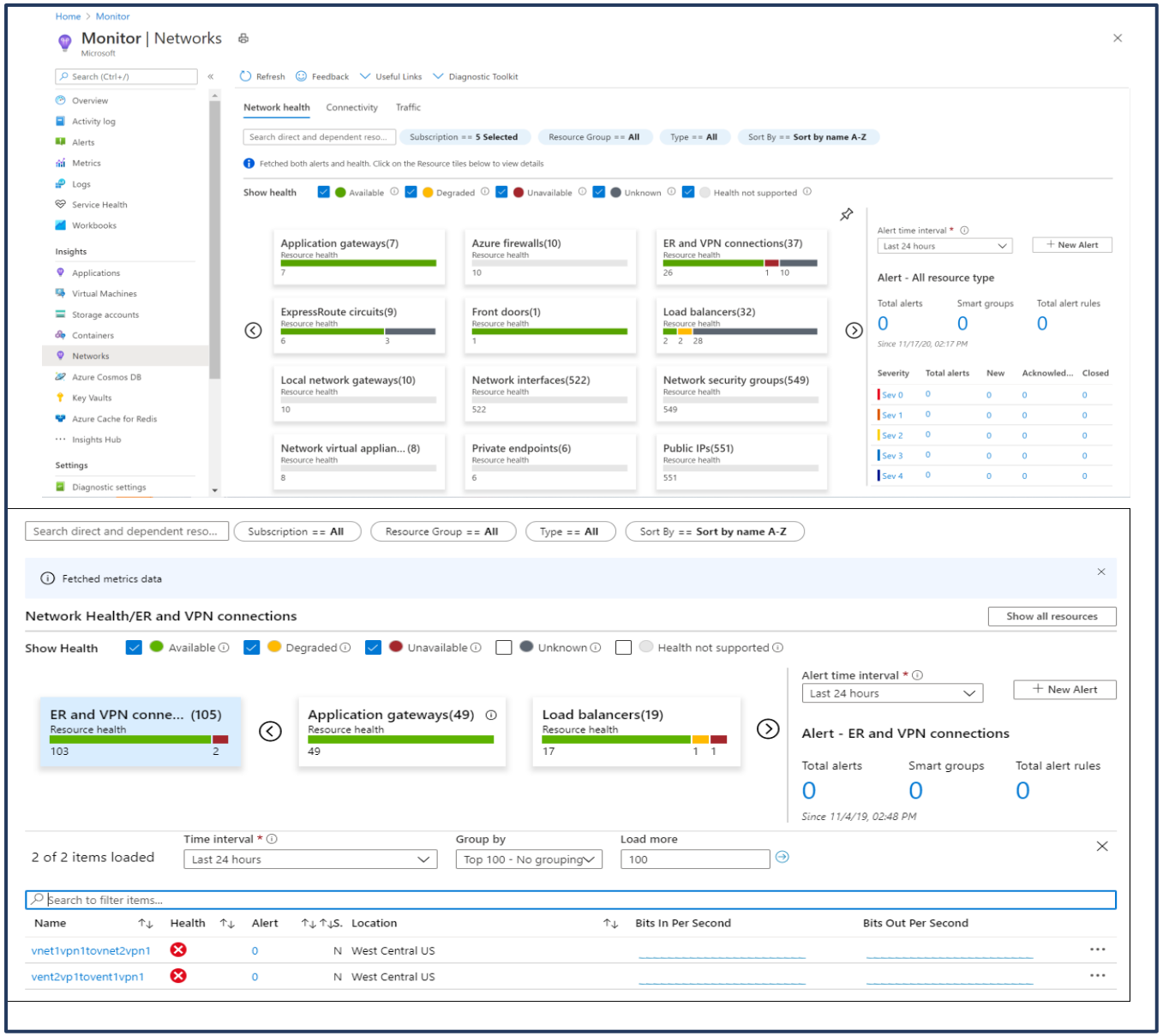
Azure Monitor Network Insights

Network health and metrics

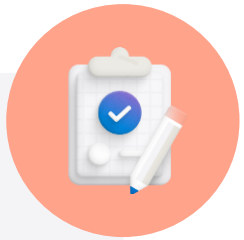
Connectivity

Traffic

Diagnostic Toolkit



Learning Recap – Monitor your networks using Azure Monitor



Check your knowledge questions and additional study

[Azure Monitor Network Insights - Azure Monitor | Microsoft Docs]

Monitor your networks using Azure Network Watcher

wireshark ← .pcap

Learning Objectives – Monitor your networks using Azure Network Watcher

Blob

- Azure Network Watcher
- Topology ←
- Connection Monitor $ → Alert ↳ Event
- IP Flow Verify
- NSG Diagnostics ←
- Next Hop tracert
- Effective Security Rules
- VPN Troubleshoot ?
- Packet Capture
- Connection Troubleshoot
- NSG Flow logs
- Traffic Analytics
- Learning Recap

VM + Agent

ping
telnet :80
Test-Netconnection
tnc

Network Watcher

RG

A **regional service** that provides various network diagnostic and monitoring tools

IP Flow Verify diagnoses connectivity issues

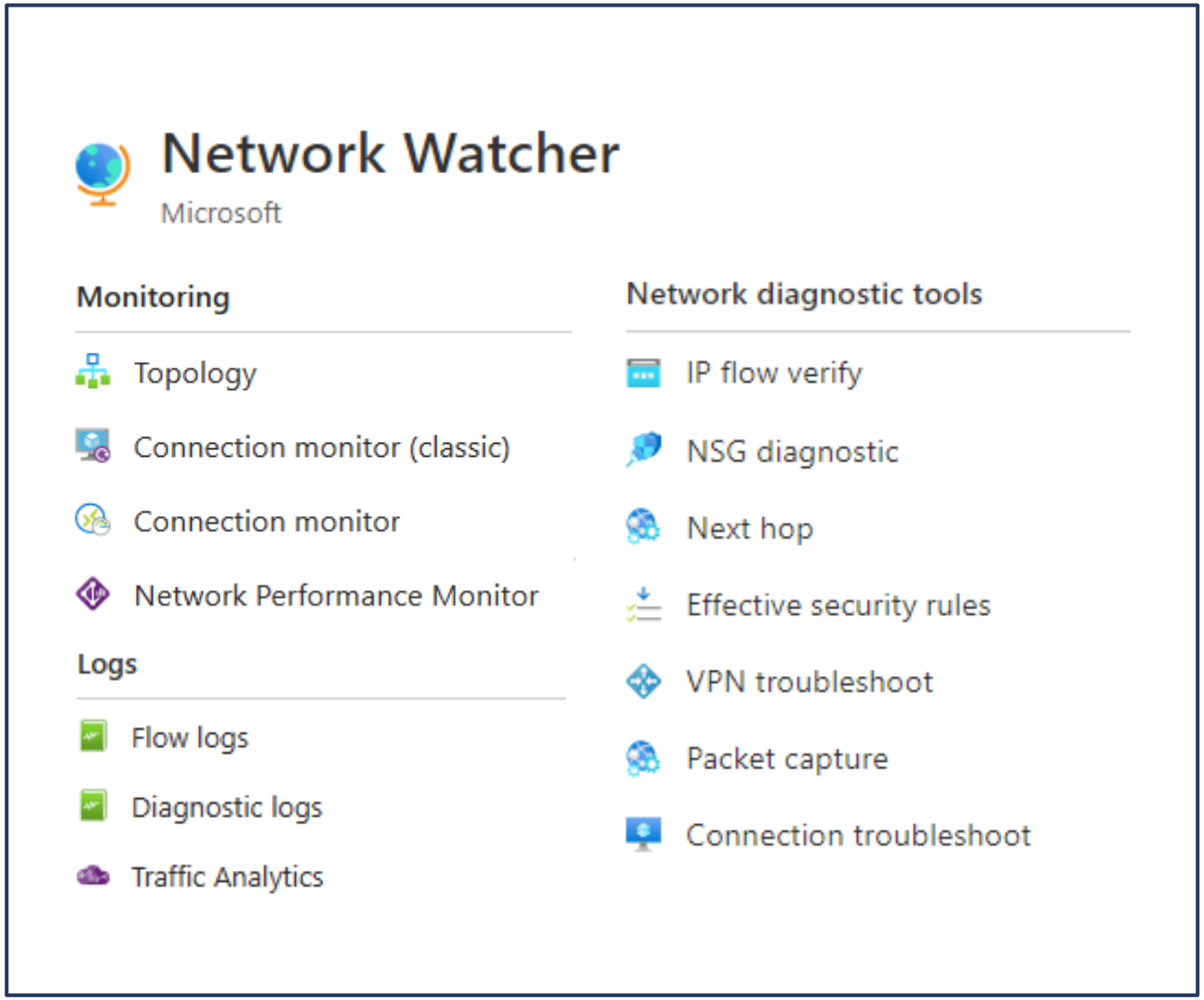
Next Hop determines if traffic is being correctly routed

VPN Diagnostics troubleshoots gateways and connections

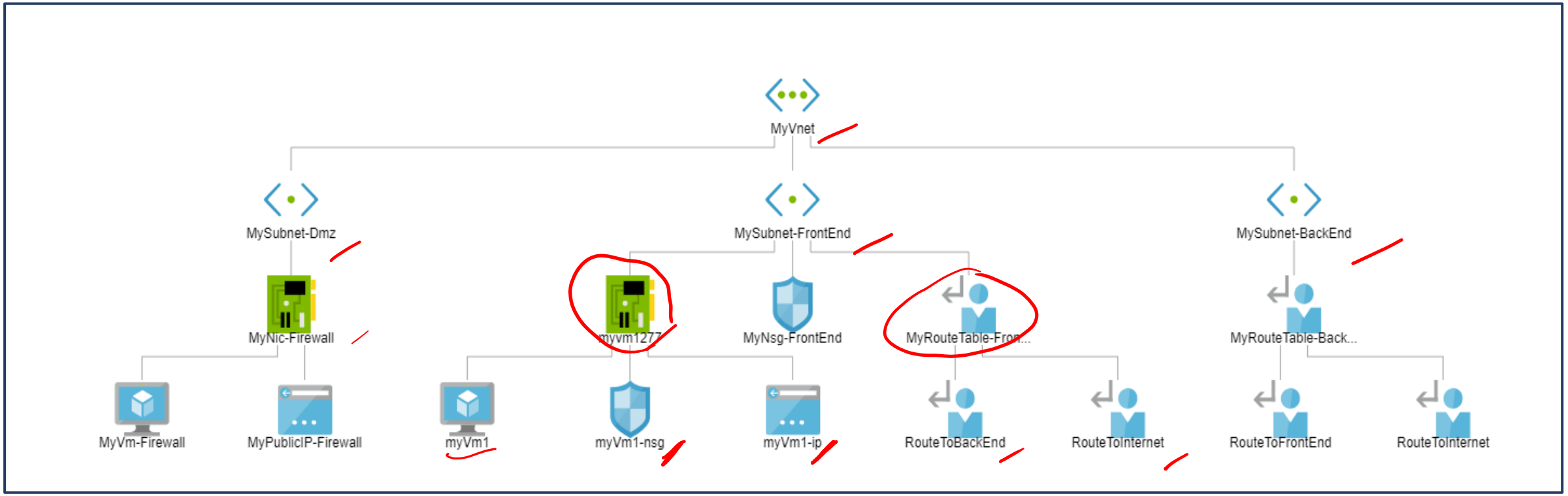
NSG Flow Logs maps IP traffic through a network security group

Connection troubleshoot shows connectivity between source VM and destination

Topology generates a visual diagram of resources



Topology



Provides a visual representation of your networking elements

View all the resources in a virtual network, resource to resource associations, and relationships between the resources

The Network Watcher instance is in the same region as the virtual network

Connection Monitor

$

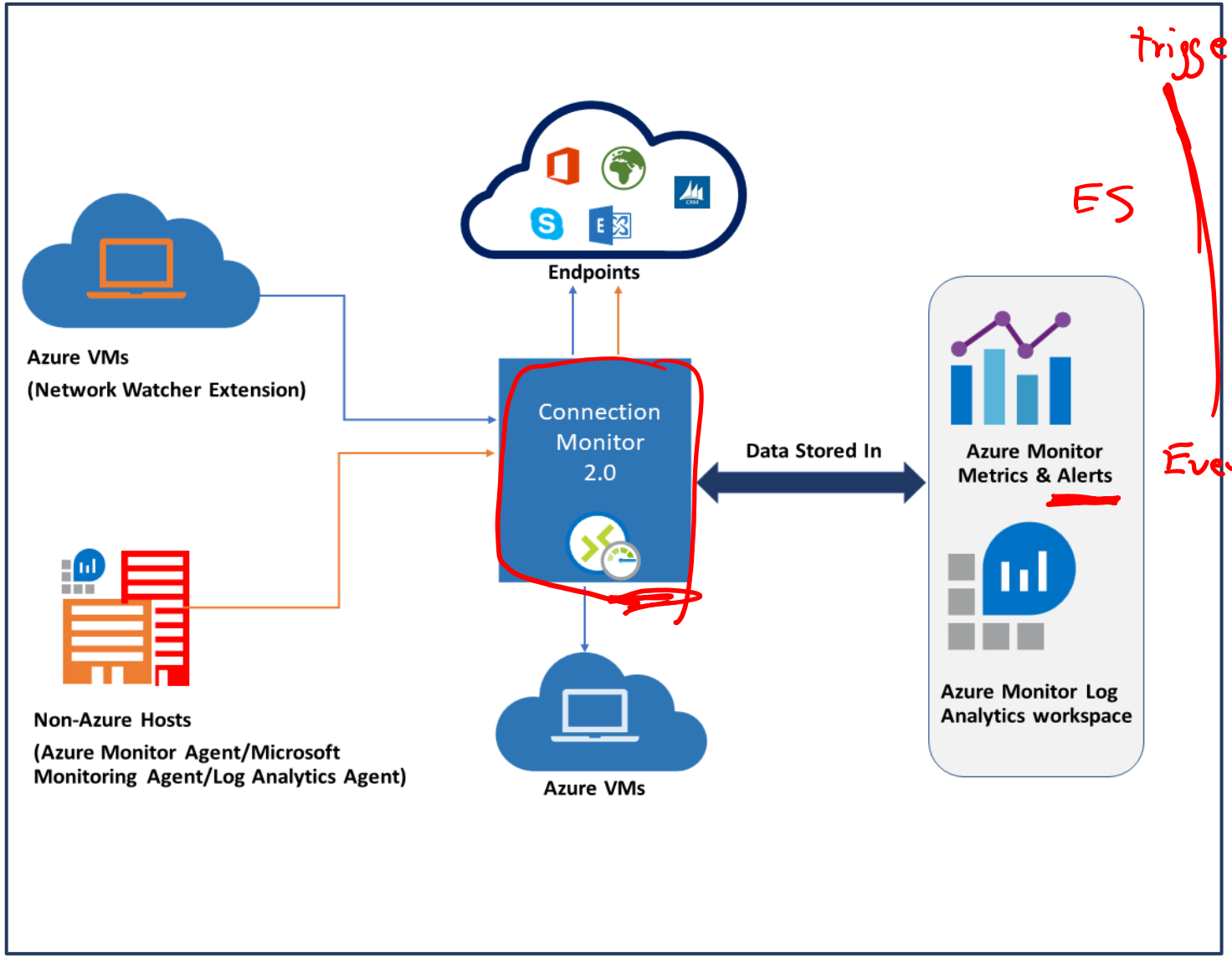
Azure Function
code

Check network connectivity between the two VMs

Compare cross-region network latencies.

Compare the latencies of the on-premises site to the latencies of the Azure application.

Check the connectivity between your on-premises setups and the Azure VMs that host your cloud application



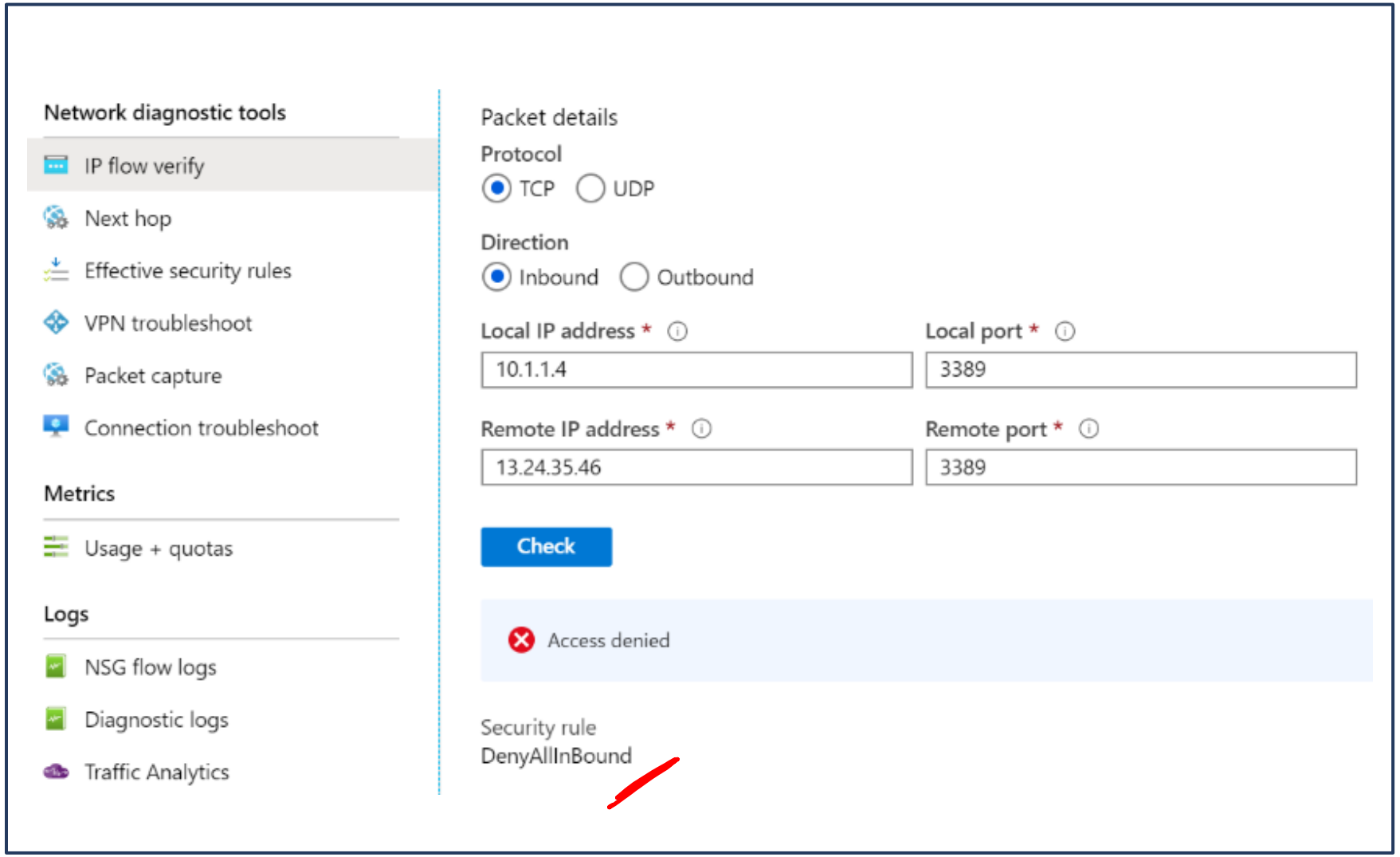
trigger

ES

Event

IP Flow Verify

Checks if a packet is allowed or denied to or from a virtual machine



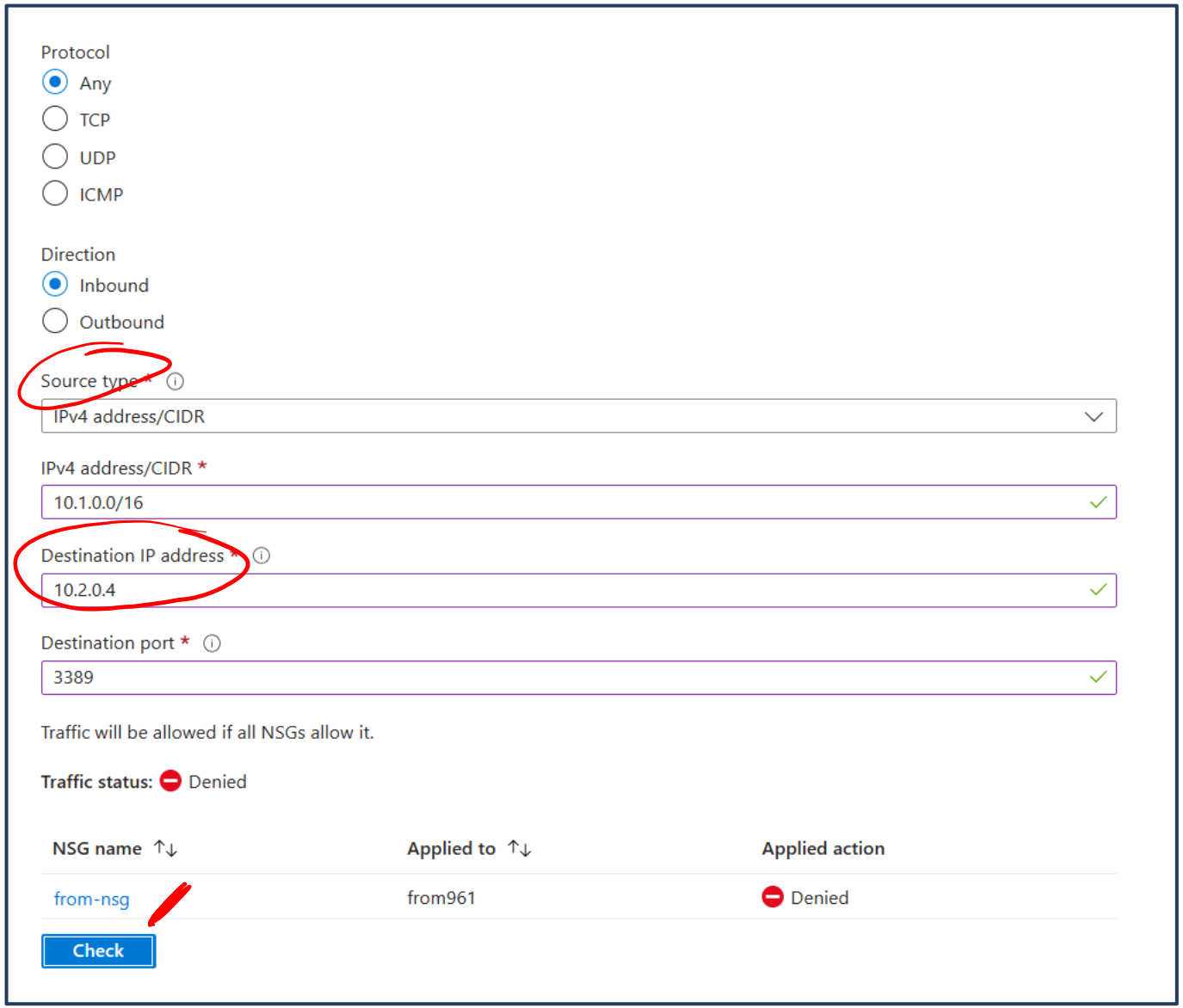
NSG Diagnostics

Used to understand which traffic flows will be allowed or denied in your Azure Virtual Network

Tool outputs whether traffic was allowed or denied

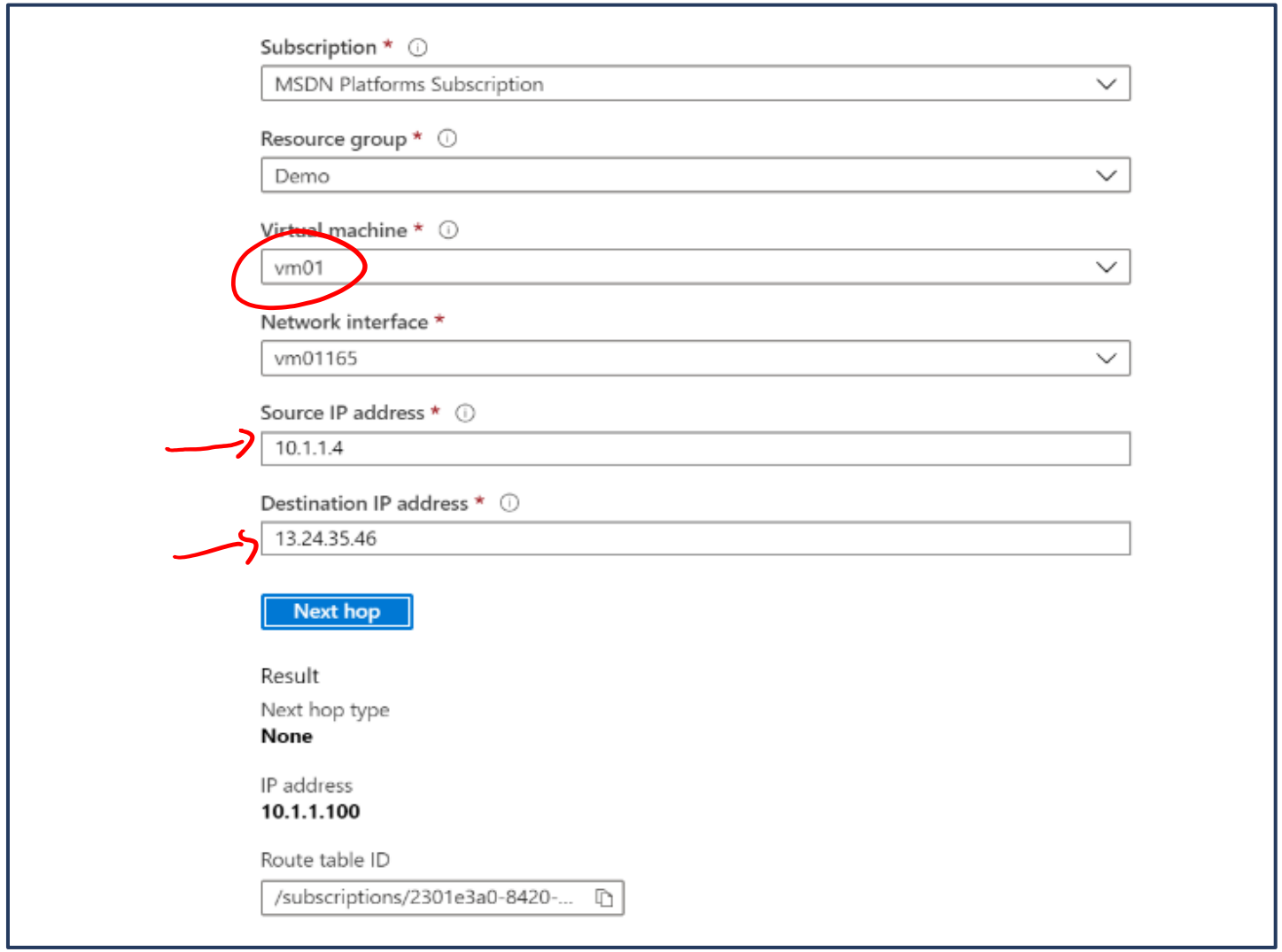
Outputs the NSG rules that were evaluated for the specified flow

Detailed information for debugging.



Next Hop

Helps with determining whether traffic is being directed to the intended destination by showing the next hop



Effective Security Rules

nsg01

Inbound rules

Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
RDP_Inbound	100	13.23.34.45/32	0-65535	0.0.0.0/0	3389-3389	TCP	Allow
AllowVnetInBound	65000	Virtual network (1 prefixes)	0-65535	Virtual network (1 prefixes)	0-65535	All	Allow
AllowAzureLoadBalancerInBound	65001	Azure load balancer (2 prefixes)	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Allow
DenyAllInBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

Outbound rules

Name	Priority	Source	Source Ports	Destination	Destination Ports	Protocol	Access
AllowVnetOutBound	65000	Virtual network (1 prefixes)	0-65535	Virtual network (1 prefixes)	0-65535	All	Allow
AllowInternetOutBound	65001	0.0.0.0/0,0.0.0.0/0	0-65535	Internet (216 prefixes)	0-65535	All	Allow
DenyAllOutBound	65500	0.0.0.0/0,0.0.0.0/0	0-65535	0.0.0.0/0,0.0.0.0/0	0-65535	All	Deny

Details the Effective Security Rules (inbound and outbound) of the Network Interface card of a Virtual Machine

VPN Troubleshoot

Subscription: MSDN Platforms Subscription

Resource group: Demo

Location: East US

*Storage account

https://samcteusvmdiagnostics.blob.core.windows.net/vpn

Name	Troubleshooting s...	Resource status	Resource Group	Location
vng01	Running	Succeeded	Demo	East US
cn01	-	Succeeded	Demo	East US

Helps you troubleshoot gateways and connections

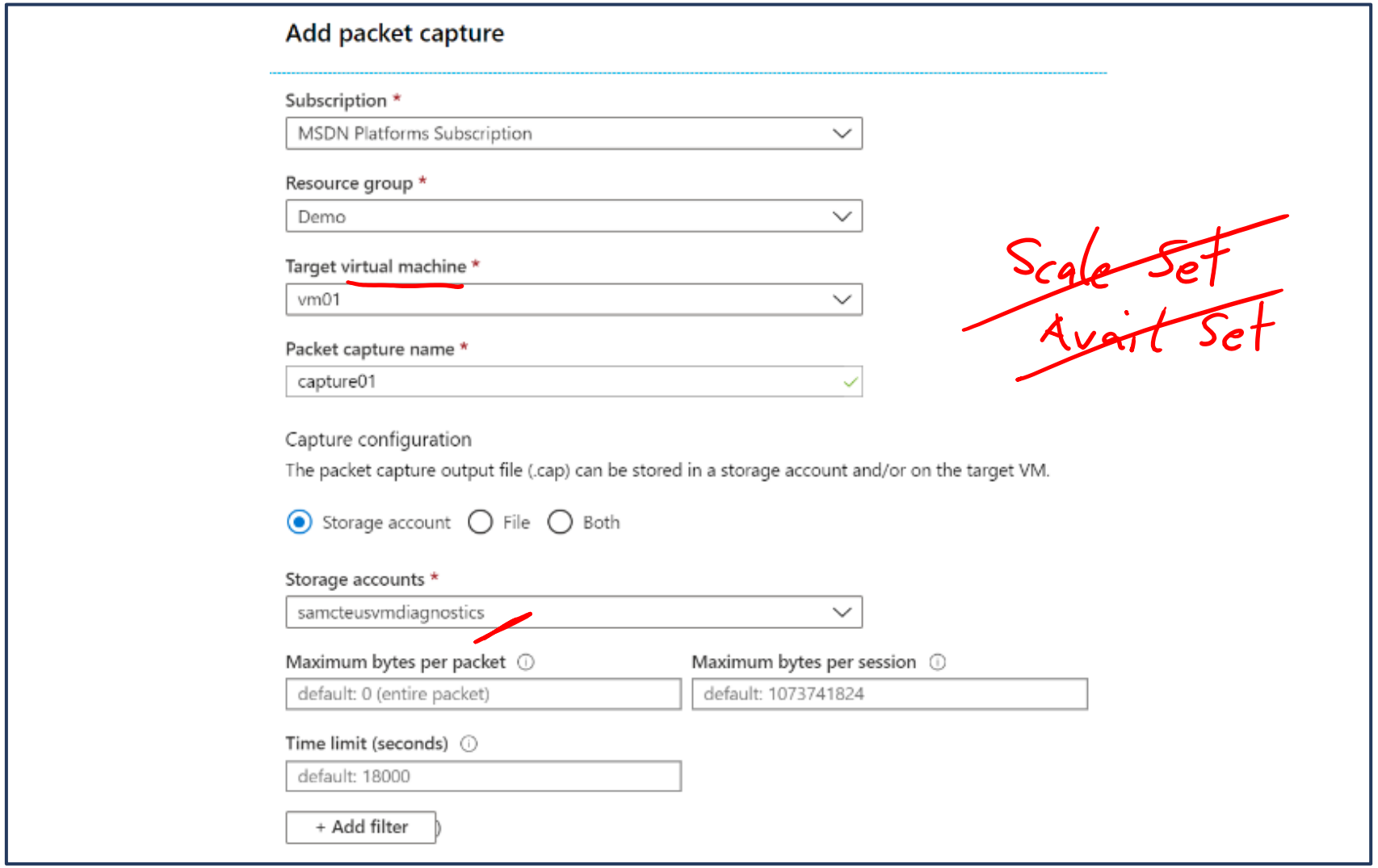
Provides summary information and detailed information

Can troubleshoot multiple gateways or connections simultaneously

Packet Capture

Captures inbound and outbound traffic from a Virtual Machine

Saves data to a storage account, a local file, or both



Connection Troubleshoot

ping
tnc

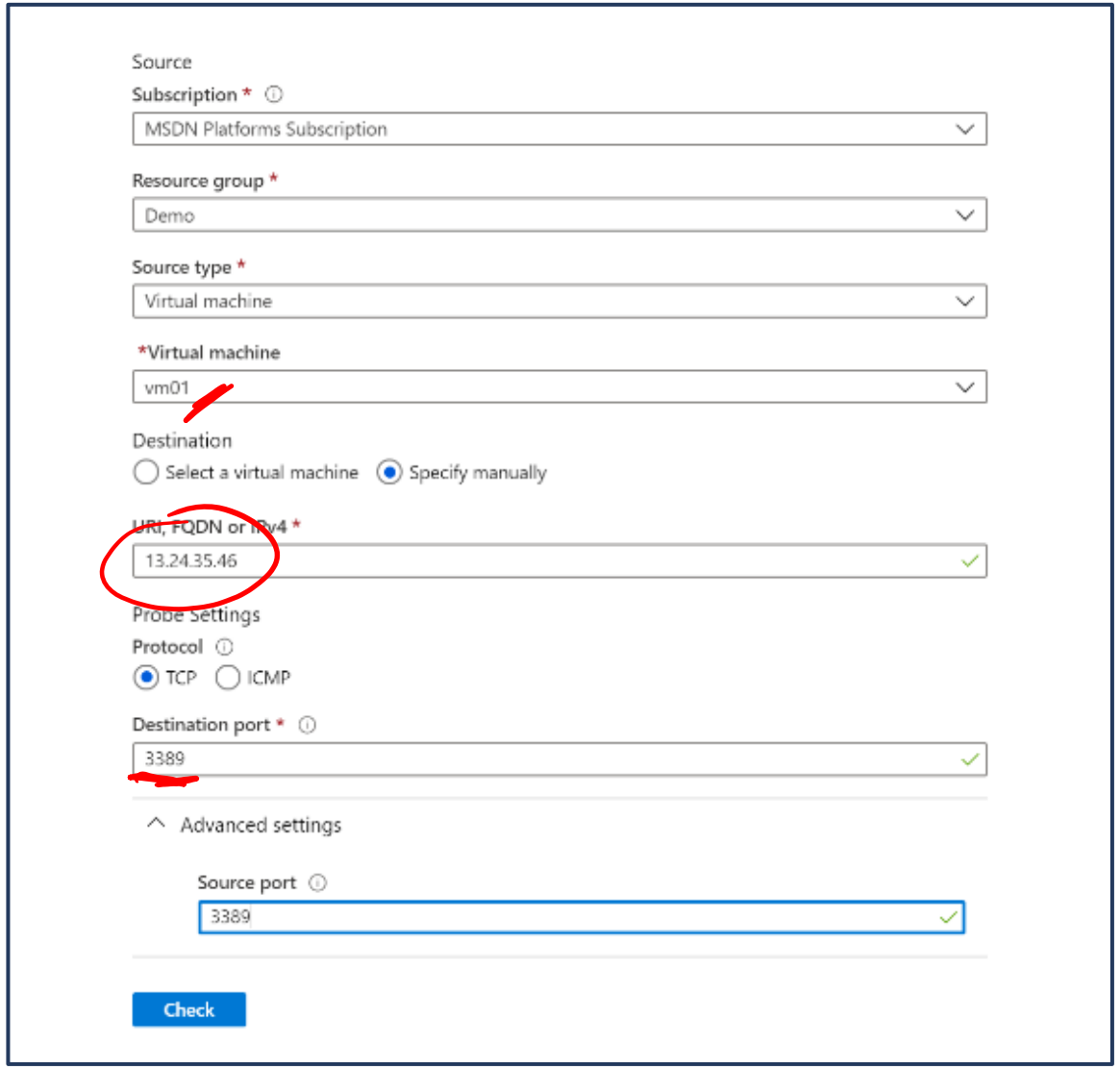
Check connectivity between source VM and destination

Identify configuration issues that are impacting reachability

Provide all possible hop by hop paths from the source to destination

Review hop by hop latency – min, max, and average between source and destination

View a graphical topology from your source to destination



NSG Flow Logs

View information about ingress and egress IP traffic through an NSG

Flow logs are written in JSON format and show outbound and inbound flows on a per rule basis

The JSON format can be visually displayed in Power BI or third-party tools like Kibana

Traffic Analytics

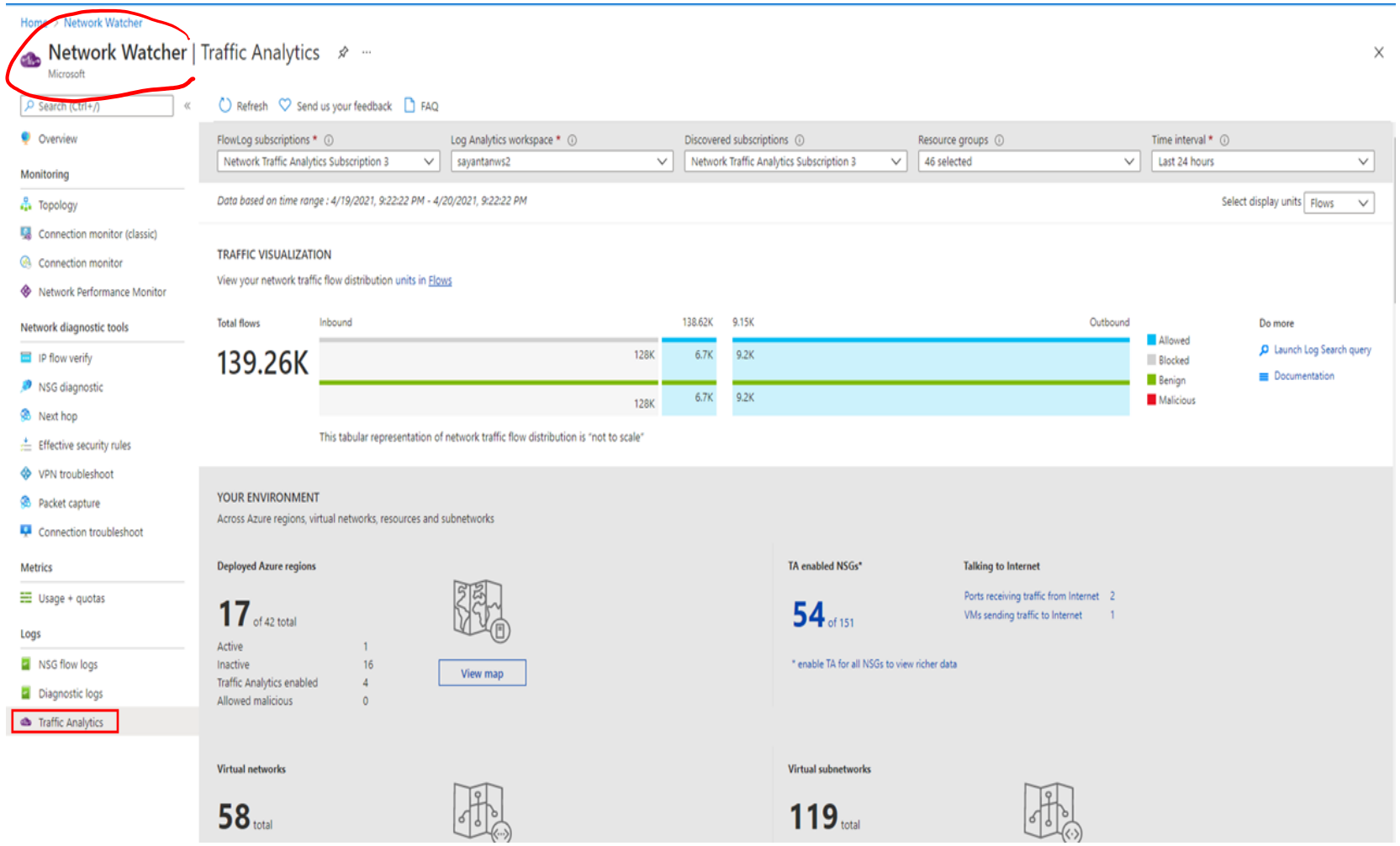
Network security group (NSG)

Network security group (NSG) flow logs

Log Analytics

Log Analytics workspace

Network Watcher

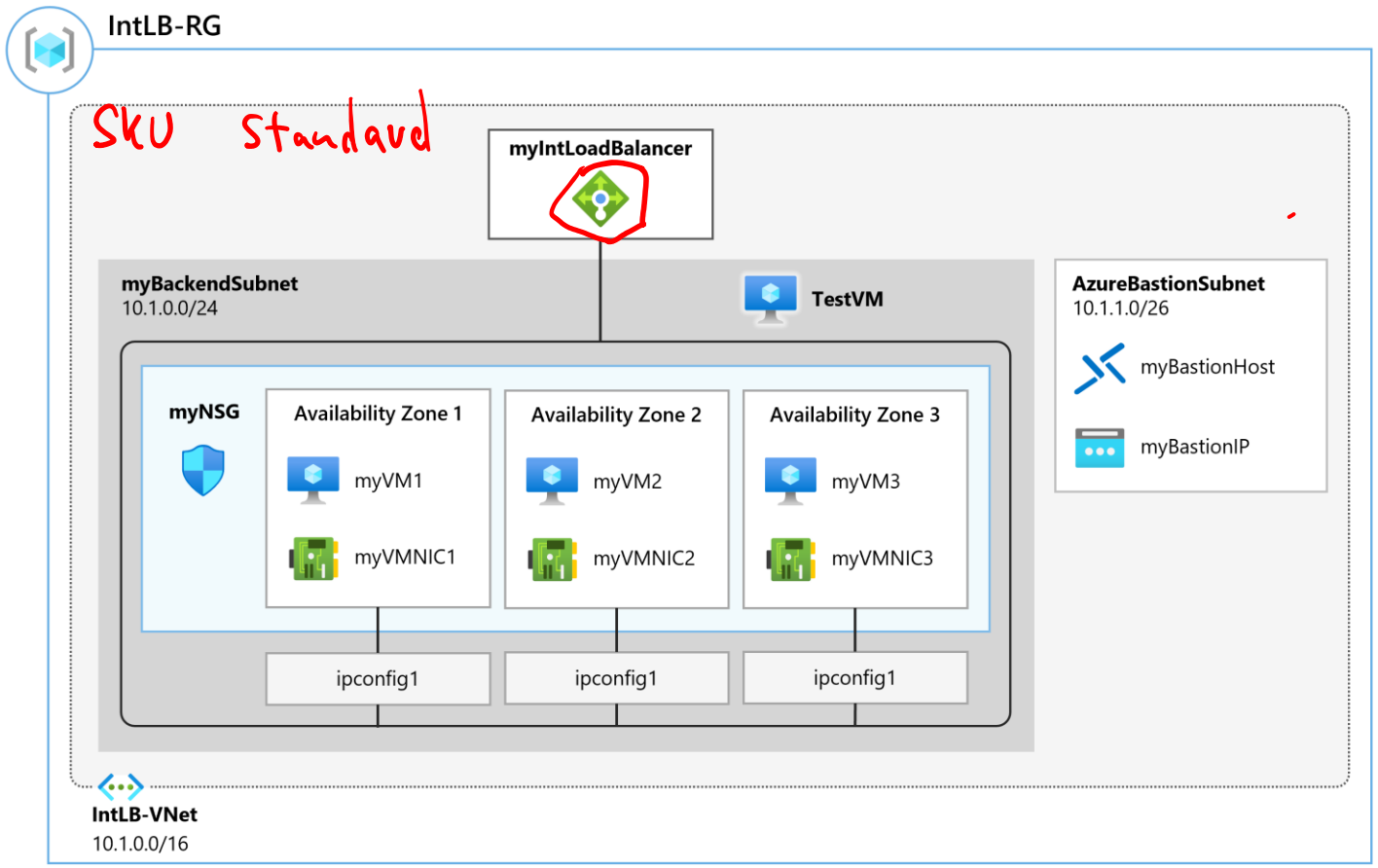


Exercise – Monitor a load balancer resource using Azure Monitor

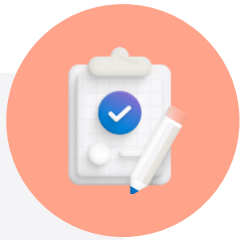
Exercise: Monitor a load balancer resource using Azure Monitor

Lab

- Create an internal load balancer
- Create a Log Analytics workspace
- Use Azure Monitor Insights
- Configure the load balancer's diagnostic settings
- Automation Account



Learning Recap – Monitor your networks using Azure Network Watcher



Check your knowledge questions and additional study

Azure Network Watcher Documentation | Microsoft Docs

Azure Network Watcher | Microsoft Docs

End of presentation