# Inspecting Azure Hybrid Cloud Network Traffic

**Tim Warner**

AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim TechTrainerTim.com

MVP
Microsoft®
Most Valuable Professional

Microsoft
CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT

# Overview

**Use Network Performance Monitor**

- Monitor on-premises connectivity
- Monitor ExpressRoute connections

**Troubleshoot external networking**

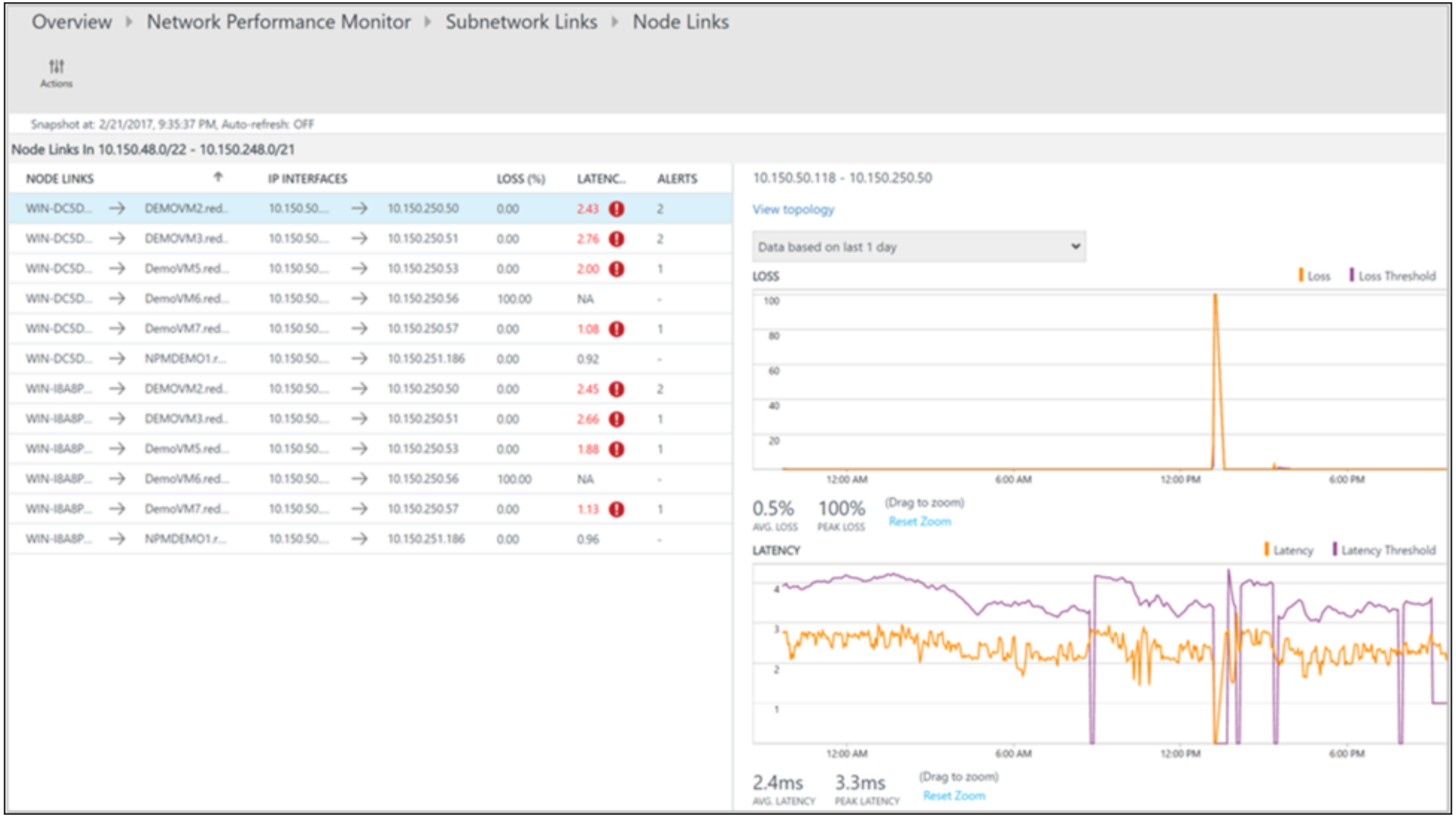
- Monitor Azure VPN Gateway
- Monitor public IP addresses

"In Azure network troubleshooting, visibility is the name of the game."

**Your humble instructor**

# Network Performance Monitor, Revisited

# NPM Performance Monitor



Overview ▸ Network Performance Monitor ▸ Subnetwork Links ▸ Node Links

Snapshot at: 2/21/2017, 9:35:37 PM, Auto-refresh: OFF

Node Links In 10.150.48.0/22 - 10.150.248.0/21

| NODE LINKS | | ↑ | IP INTERFACES | | | LOSS (%) | LATENC... | ALERTS |
|---|---|---|---|---|---|---|---|---|
| WIN-DC5D... | → | DEMOVM2.red... | 10.150.50.... | → | 10.150.250.50 | 0.00 | 2.43 ❗ | 2 |
| WIN-DC5D... | → | DEMOVM3.red... | 10.150.50.... | → | 10.150.250.51 | 0.00 | 2.76 ❗ | 2 |
| WIN-DC5D... | → | DemoVM5.red... | 10.150.50.... | → | 10.150.250.53 | 0.00 | 2.00 ❗ | 1 |
| WIN-DC5D... | → | DemoVM6.red... | 10.150.50.... | → | 10.150.250.56 | 100.00 | NA | - |
| WIN-DC5D... | → | DemoVM7.red... | 10.150.50.... | → | 10.150.250.57 | 0.00 | 1.08 ❗ | 1 |
| WIN-DC5D... | → | NPMDEMO1.r... | 10.150.50.... | → | 10.150.251.186 | 0.00 | 0.92 | - |
| WIN-I8A8P... | → | DEMOVM2.red... | 10.150.50.... | → | 10.150.250.50 | 0.00 | 2.45 ❗ | 2 |
| WIN-I8A8P... | → | DEMOVM3.red... | 10.150.50.... | → | 10.150.250.51 | 0.00 | 2.66 ❗ | 1 |
| WIN-I8A8P... | → | DemoVM5.red... | 10.150.50.... | → | 10.150.250.53 | 0.00 | 1.88 ❗ | 1 |
| WIN-I8A8P... | → | DemoVM6.red... | 10.150.50.... | → | 10.150.250.56 | 100.00 | NA | - |
| WIN-I8A8P... | → | DemoVM7.red... | 10.150.50.... | → | 10.150.250.57 | 0.00 | 1.13 ❗ | 1 |
| WIN-I8A8P... | → | NPMDEMO1.r... | 10.150.50.... | → | 10.150.251.186 | 0.00 | 0.96 | - |

10.150.50.118 - 10.150.250.50

View topology

Data based on last 1 day

LOSS

0.5% AVG. LOSS

100% PEAK LOSS

(Drag to zoom)

Reset Zoom

LATENCY

2.4ms AVG. LATENCY

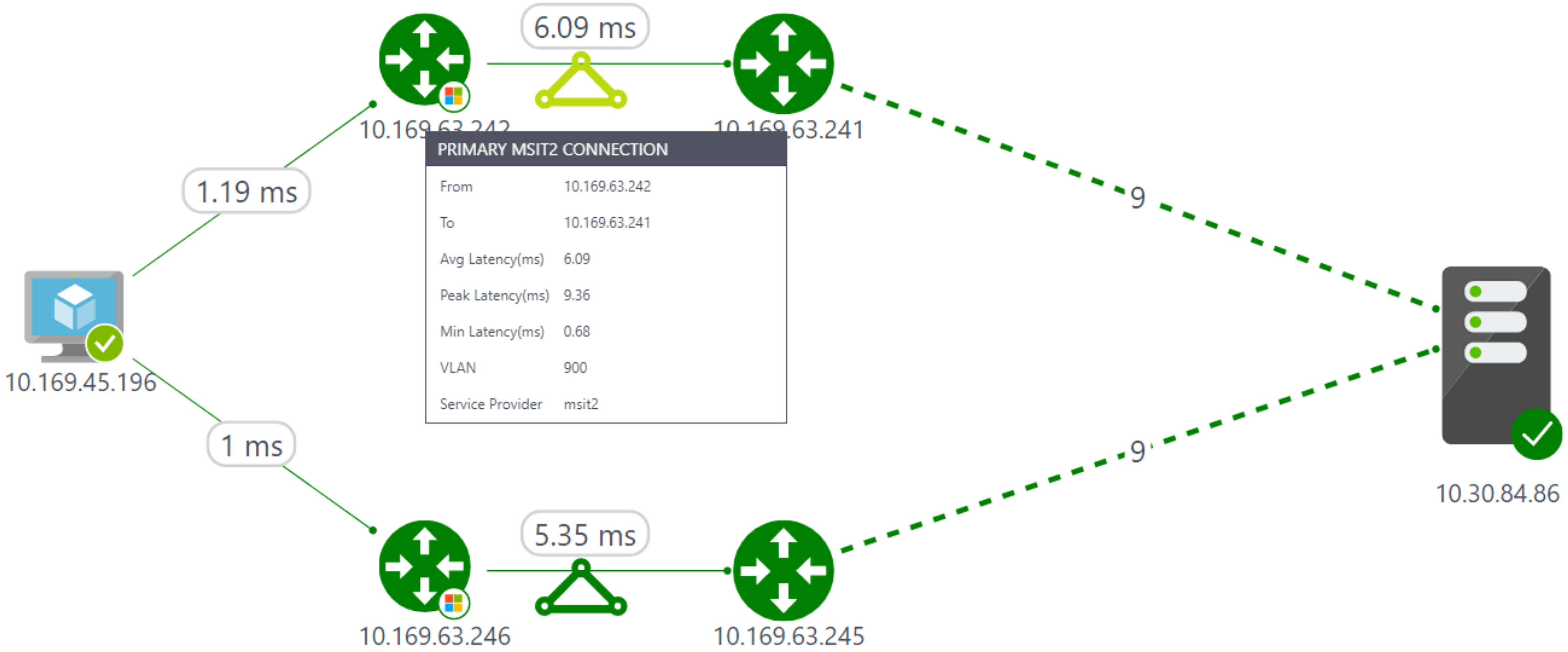
3.3ms PEAK LATENCY

(Drag to zoom)

Reset Zoom

https://timw.info/a11c7

# ExpressRoute Monitor

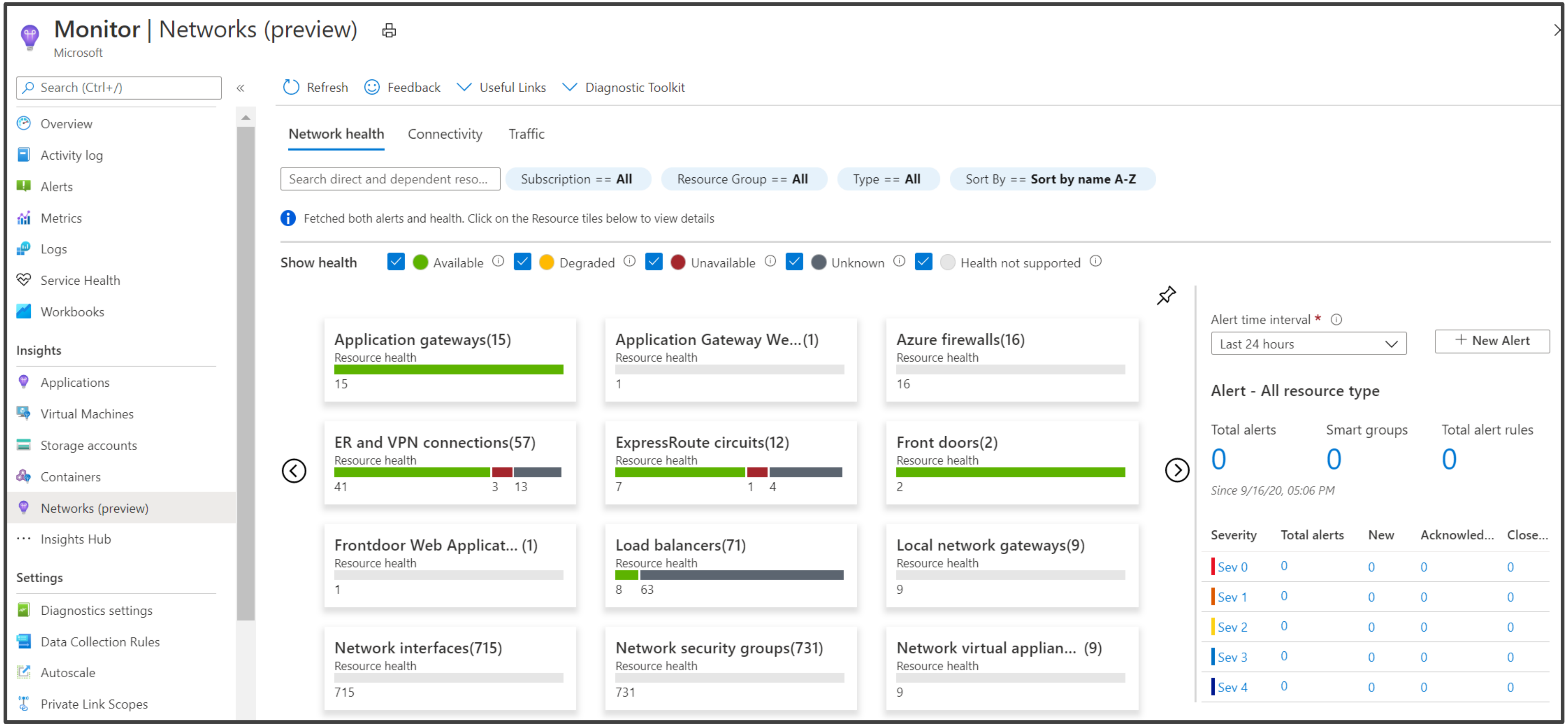


PRIMARY MSIT2 CONNECTION

| | |
|---|---|
| From | 10.169.63.242 |
| To | 10.169.63.241 |
| Avg Latency(ms) | 6.09 |
| Peak Latency(ms) | 9.36 |
| Min Latency(ms) | 0.68 |
| VLAN | 900 |
| Service Provider | msit2 |

https://timw.info/edd4

# Azure Monitor for Networks (Insights)



**Monitor** | Networks (preview)

Microsoft

Search direct and dependent reso...

Subscription == **All**

Resource Group == **All**

Type == **All**

Sort By == **Sort by name A-Z**

Fetched both alerts and health. Click on the Resource tiles below to view details

Show health ☑ ● Available ⓘ ☑ ● Degraded ⓘ ☑ ● Unavailable ⓘ ☑ ● Unknown ⓘ ☑ ○ Health not supported ⓘ

Application gateways(15)
Resource health
15

Application Gateway We...(1)
Resource health
1

Azure firewalls(16)
Resource health
16

ER and VPN connections(57)
Resource health
41 3 13

ExpressRoute circuits(12)
Resource health
7 1 4

Front doors(2)
Resource health
2

Frontdoor Web Applicat... (1)
Resource health
1

Load balancers(71)
Resource health
8 63

Local network gateways(9)
Resource health
9

Network interfaces(715)
Resource health
715

Network security groups(731)
Resource health
731

Network virtual applian... (9)
Resource health
9

Alert time interval * ⓘ

Last 24 hours

+ New Alert

Alert - All resource type

| Total alerts | Smart groups | Total alert rules |
|---|---|---|
| 0 | 0 | 0 |

*Since 9/16/20, 05:06 PM*

| Severity | Total alerts | New | Acknowled... | Close... |
|---|---|---|---|---|
| Sev 0 | 0 | 0 | 0 | 0 |
| Sev 1 | 0 | 0 | 0 | 0 |
| Sev 2 | 0 | 0 | 0 | 0 |
| Sev 3 | 0 | 0 | 0 | 0 |
| Sev 4 | 0 | 0 | 0 | 0 |

https://timw.info/5c537

# Demo

1

Set up NPM

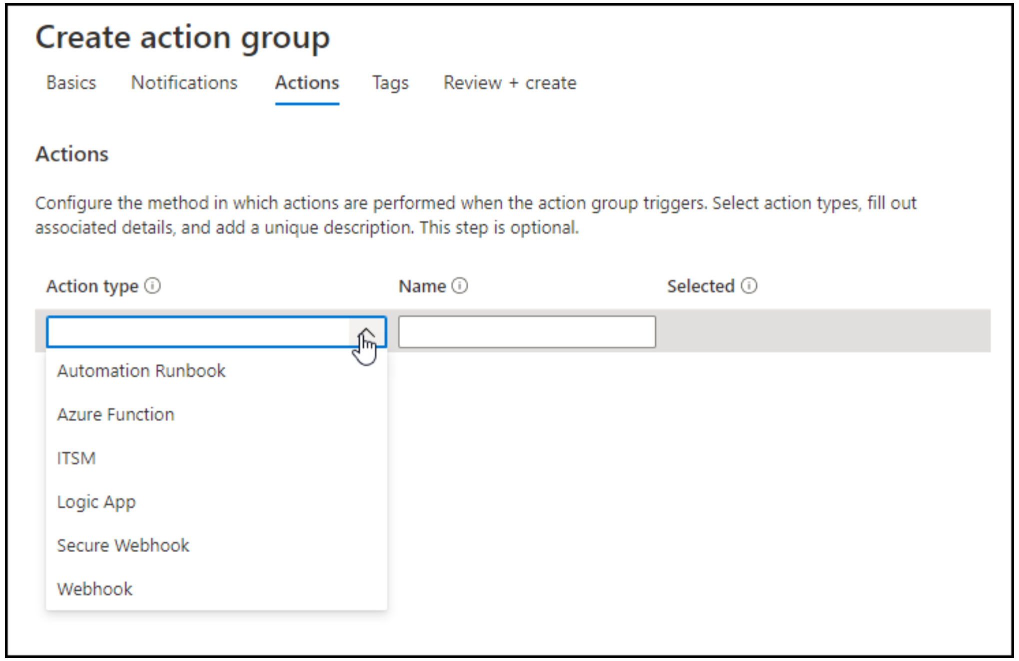
View network data

Tour Azure Monitor Network Insights

# Troubleshoot Azure VPN Gateway

# Azure VPN Gateway Diagnostic Log Alerts

```
AzureDiagnostics
| where Category == "TunnelDiagnosticLog"
| where _ResourceId == tolower("<RESOURCEID OF GATEWAY>")
| where TimeGenerated > ago(5m)
| where remoteIP_s == "<REMOTE IP OF TUNNEL>"
| where status_s == "Disconnected"
| project TimeGenerated, OperationName, instance_s, Resource,
ResourceGroup, _ResourceId
| sort by TimeGenerated asc
```



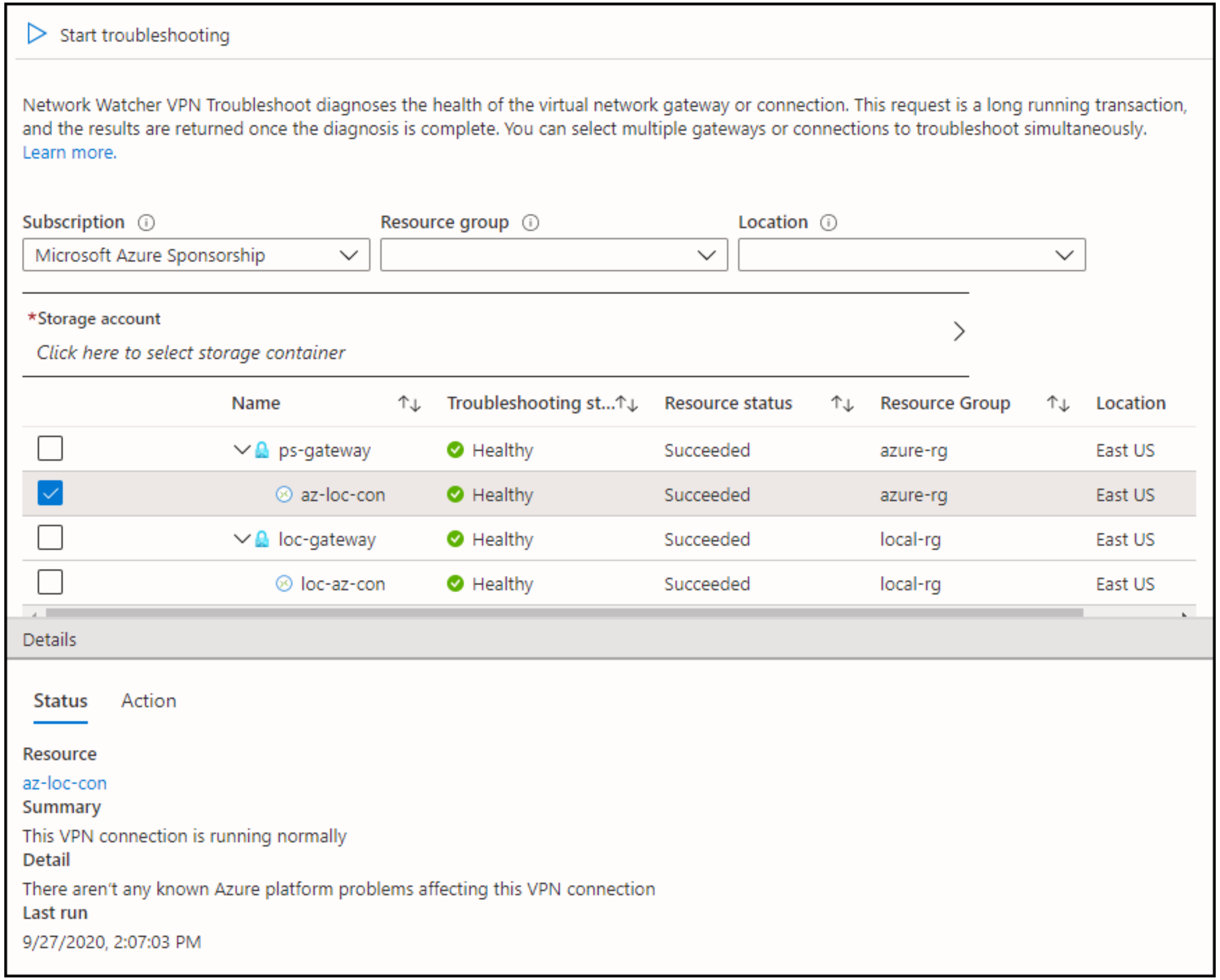
Create action group

Actions

Configure the method in which actions are performed when the action group triggers. Select action types, fill out associated details, and add a unique description. This step is optional.

https://timw.info/e969

# Network Watcher VPN Troubleshoot



Network Watcher VPN Troubleshoot diagnoses the health of the virtual network gateway or connection. This request is a long running transaction, and the results are returned once the diagnosis is complete. You can select multiple gateways or connections to troubleshoot simultaneously. Learn more.

Subscription: Microsoft Azure Sponsorship

Resource group:

Location:

*Storage account

*Click here to select storage container*

| | Name | Troubleshooting st... | Resource status | Resource Group | Location |
|---|---|---|---|---|---|
| □ | ps-gateway | ✓ Healthy | Succeeded | azure-rg | East US |
| ☑ | az-loc-con | ✓ Healthy | Succeeded | azure-rg | East US |
| □ | loc-gateway | ✓ Healthy | Succeeded | local-rg | East US |
| □ | loc-az-con | ✓ Healthy | Succeeded | local-rg | East US |

Details

**Resource**

az-loc-con

**Summary**

This VPN connection is running normally

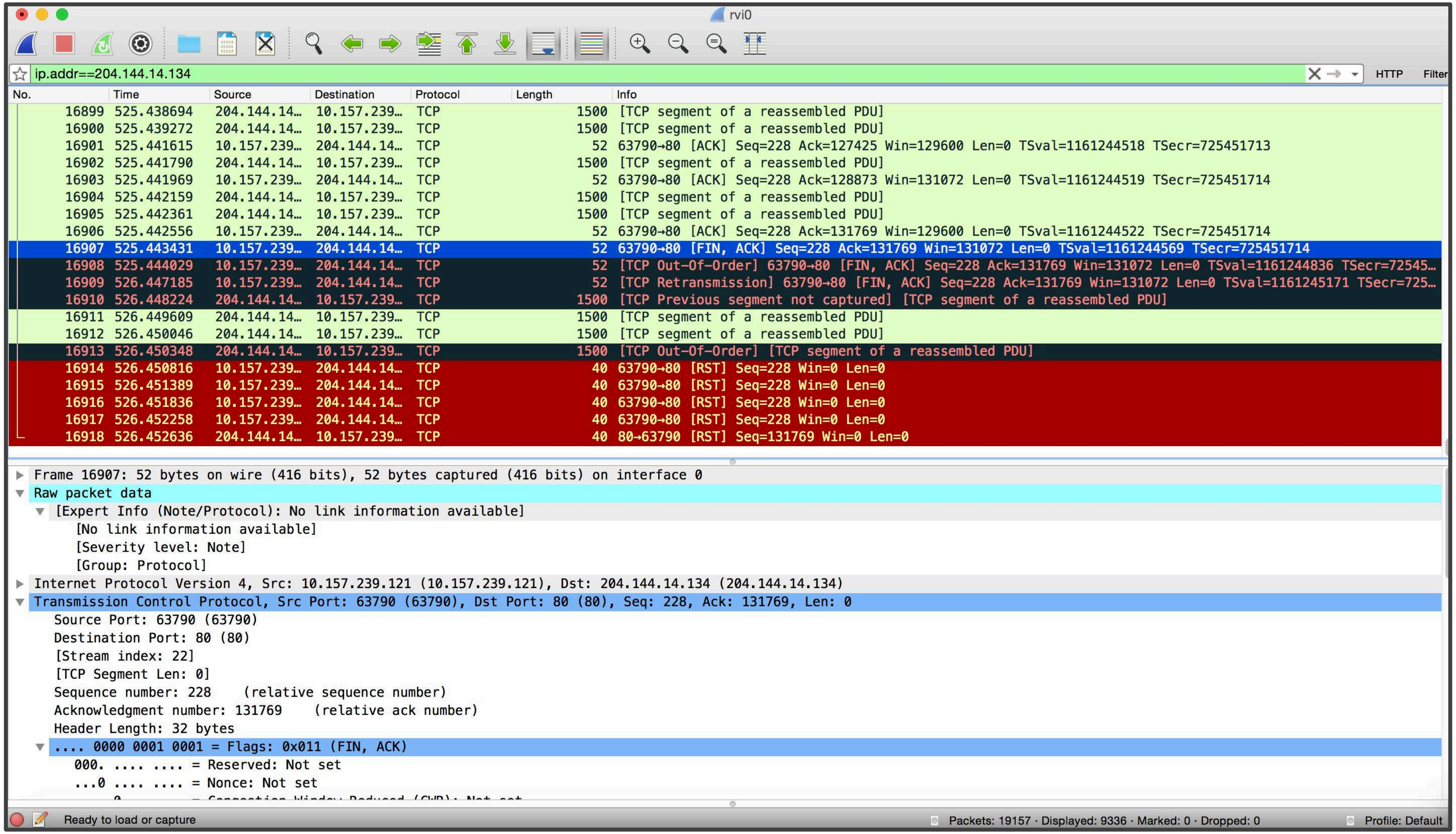
**Detail**

There aren't any known Azure platform problems affecting this VPN connection

**Last run**

9/27/2020, 2:07:03 PM

# Network Watcher Packet Capture



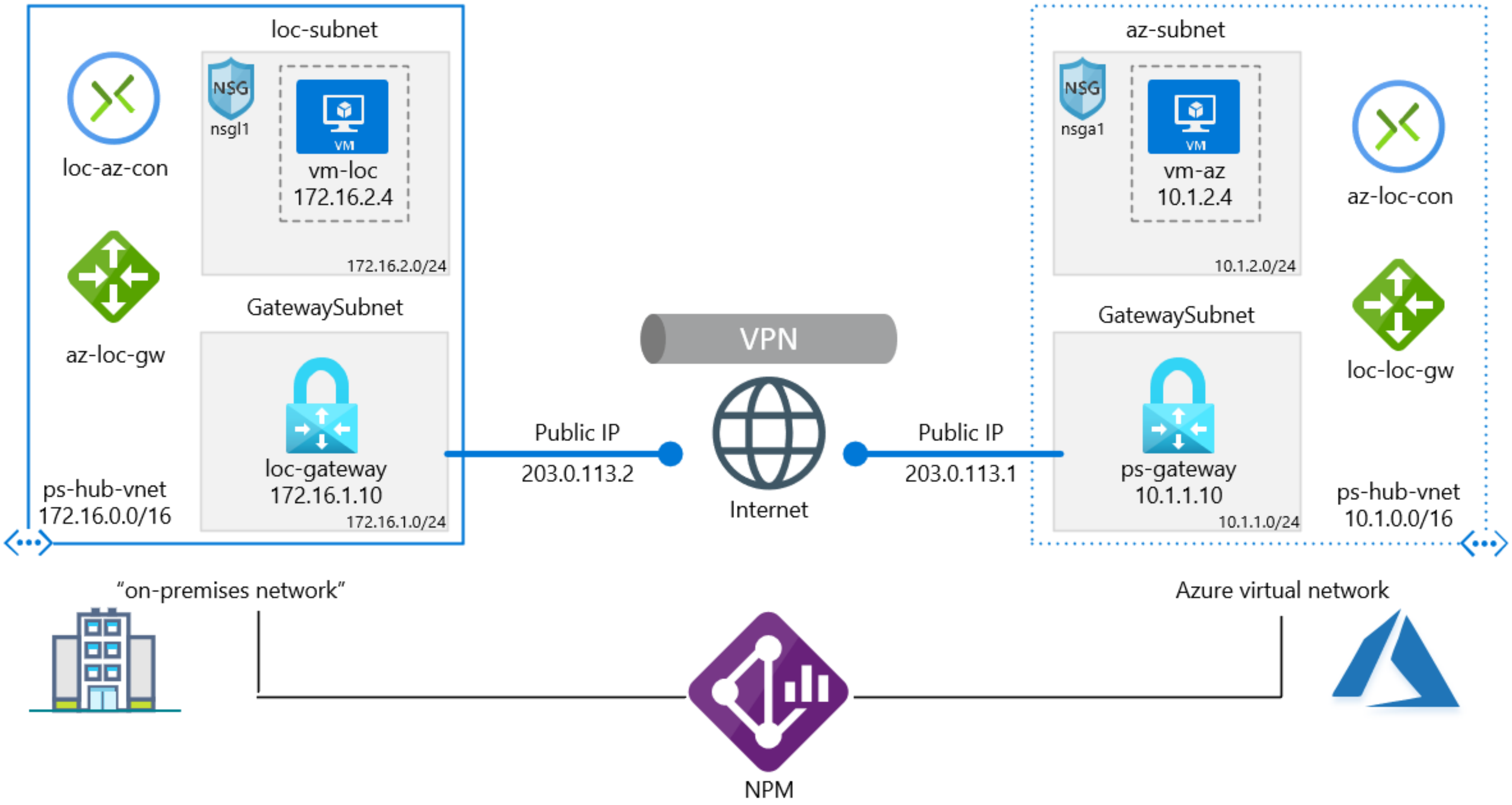
```
ip.addr==204.144.14.134                                                     HTTP   Filter

No.     Time        Source          Destination     Protocol   Length   Info
16899   525.438694  204.144.14…    10.157.239…    TCP          1500   [TCP segment of a reassembled PDU]
16900   525.439272  204.144.14…    10.157.239…    TCP          1500   [TCP segment of a reassembled PDU]
16901   525.441615  10.157.239…    204.144.14…    TCP            52   63790→80 [ACK] Seq=228 Ack=127425 Win=129600 Len=0 TSval=1161244518 TSecr=725451713
16902   525.441790  204.144.14…    10.157.239…    TCP          1500   [TCP segment of a reassembled PDU]
16903   525.441969  10.157.239…    204.144.14…    TCP            52   63790→80 [ACK] Seq=228 Ack=128873 Win=131072 Len=0 TSval=1161244519 TSecr=725451714
16904   525.442159  204.144.14…    10.157.239…    TCP          1500   [TCP segment of a reassembled PDU]
16905   525.442361  204.144.14…    10.157.239…    TCP          1500   [TCP segment of a reassembled PDU]
16906   525.442556  10.157.239…    204.144.14…    TCP            52   63790→80 [ACK] Seq=228 Ack=131769 Win=129600 Len=0 TSval=1161244522 TSecr=725451714
16907   525.443431  10.157.239…    204.144.14…    TCP            52   63790→80 [FIN, ACK] Seq=228 Ack=131769 Win=131072 Len=0 TSval=1161244569 TSecr=725451714
16908   525.444029  10.157.239…    204.144.14…    TCP            52   [TCP Out-Of-Order] 63790→80 [FIN, ACK] Seq=228 Ack=131769 Win=131072 Len=0 TSval=1161244836 TSecr=72545…
16909   526.447185  10.157.239…    204.144.14…    TCP            52   [TCP Retransmission] 63790→80 [FIN, ACK] Seq=228 Ack=131769 Win=131072 Len=0 TSval=1161245171 TSecr=725…
16910   526.448224  204.144.14…    10.157.239…    TCP          1500   [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
16911   526.449609  204.144.14…    10.157.239…    TCP          1500   [TCP segment of a reassembled PDU]
16912   526.450046  204.144.14…    10.157.239…    TCP          1500   [TCP segment of a reassembled PDU]
16913   526.450348  204.144.14…    10.157.239…    TCP          1500   [TCP Out-Of-Order] [TCP segment of a reassembled PDU]
16914   526.450816  10.157.239…    204.144.14…    TCP            40   63790→80 [RST] Seq=228 Win=0 Len=0
16915   526.451389  10.157.239…    204.144.14…    TCP            40   63790→80 [RST] Seq=228 Win=0 Len=0
16916   526.451836  10.157.239…    204.144.14…    TCP            40   63790→80 [RST] Seq=228 Win=0 Len=0
16917   526.452258  10.157.239…    204.144.14…    TCP            40   63790→80 [RST] Seq=228 Win=0 Len=0
16918   526.452636  204.144.14…    10.157.239…    TCP            40   80→63790 [RST] Seq=131769 Win=0 Len=0
```

```
▶ Frame 16907: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface 0
▼ Raw packet data
  ▼ [Expert Info (Note/Protocol): No link information available]
      [No link information available]
      [Severity level: Note]
      [Group: Protocol]
▶ Internet Protocol Version 4, Src: 10.157.239.121 (10.157.239.121), Dst: 204.144.14.134 (204.144.14.134)
▼ Transmission Control Protocol, Src Port: 63790 (63790), Dst Port: 80 (80), Seq: 228, Ack: 131769, Len: 0
    Source Port: 63790 (63790)
    Destination Port: 80 (80)
    [Stream index: 22]
    [TCP Segment Len: 0]
    Sequence number: 228    (relative sequence number)
    Acknowledgment number: 131769    (relative ack number)
    Header Length: 32 bytes
  ▼ .... 0000 0001 0001 = Flags: 0x011 (FIN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
```

Ready to load or capture    Packets: 19157 · Displayed: 9336 · Marked: 0 · Dropped: 0    Profile: Default

https://timw.info/8926

# Lab Topology



Demo

2

**Set up Azure VPN alerts**

- https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-setup-alerts-virtual-network-gateway-log

**NW VPN Troubleshoot**

**Packet Capture**

# Summary

Microsoft gives you the tools to visualize your hybrid cloud network performance

Learn KQL sooner rather than later

Be gentle with yourself - networking is a heavy lift

Thanks so much!

Courses: timw.info/ps

Twitter: @TechTrainerTim

Website: TechTrainerTim.com