VIAVI Solutions

Brochure

Don’t Get Lost In Translation

Restore End-to-End Visibility – without collecting packets or deploying agents

Are you:

- Troubleshooting network or application performance? Investigating potential security threats?
- Trying to get an accurate end-to-end view of conversations?

If so:

You’re probably noticing that network and port address translations (NAT/PAT) introduce significant complexity in carrying out these tasks.

What do we mean by NAT & PAT?

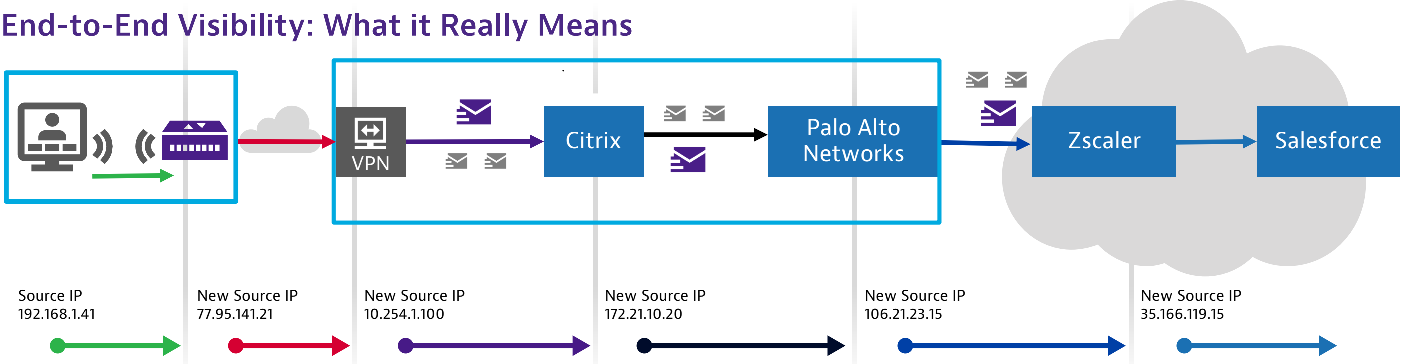
Modern network and service architectures cause source and destination IP addresses and ports to change frequently, making it a challenge to understand and follow an end-to-end conversation. For example: Load balancers make it difficult to determine which server is responding to a user’s request.

Challenges created by NAT & PAT?

- Allowing remote users access to corporate resources through VPN concentrators and firewalls involves address and port translations that make it difficult to see the end-user’s original IP address as their packets traverse through these network elements
- Migrations from on-premises to hybrid application architectures and cloud-based services completely re-shape end-to-end conversations as the packets travel through cloud-based proxies and many other NAT/PAT network elements

The figure below shows the number of IP address variations as user requests traverse the various network components for access to a service like Salesforce.com.

End-to-End Visibility: What it Really Means

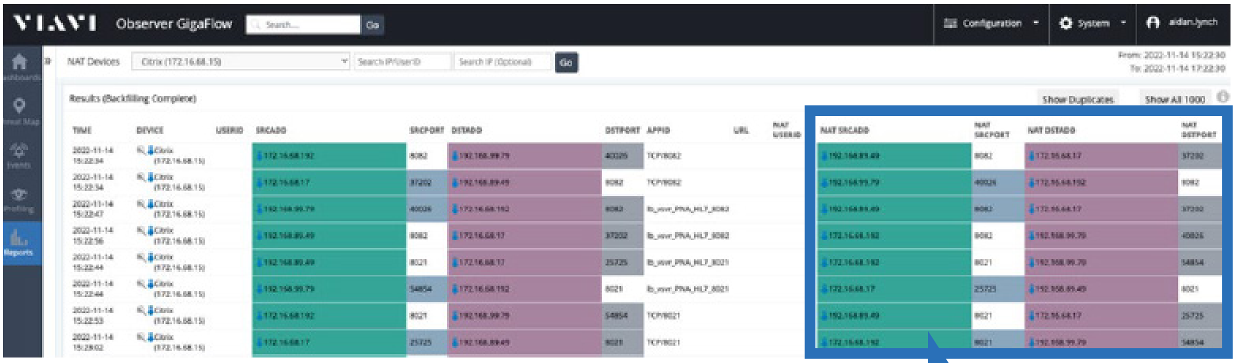

VPN
Citrix
Palo Alto Networks
Zscaler
Salesforce
Source IP 192.168.1.41
New Source IP 77.95.141.21
New Source IP 10.254.1.100
New Source IP 172.21.10.20
New Source IP 106.21.23.15
New Source IP 35.166.119.15

Source and Destination IP address and port visibility from end-to-end

Observer restores visibility by revealing how infrastructure devices modify IP conversations from source to destination and back again

VIAVI Observer utilizes NAT/PAT data from all address translating devices in the network to construct an end-to-end view of each transaction (or flow) – no packet collection or agent deployment required. This provides visibility into how end-user requests are being reshaped by firewalls, load balancers, VPN concentrators, web proxies, and other address translating devices.

Performance experts and SecOps teams can use this same data to keep authorized users performing and minimize dwell time for the bad actors that may have penetrated external defences.



NAT Devices Citrix (172.16.68.15) Search IP/UserID Search IP (Optional) Go

From: 2022-11-14 15:22:30
To: 2022-11-14 17:22:30

Results (Backfilling Complete)

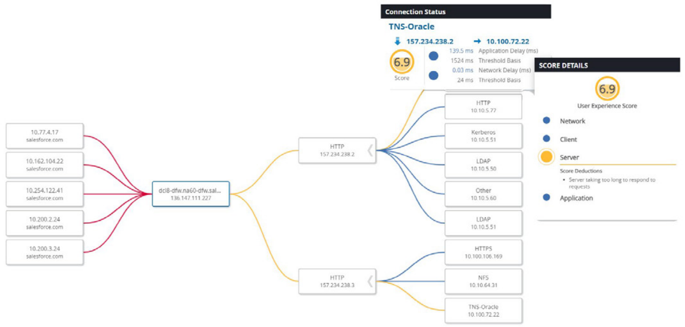
Show Duplicates Show All 1000

TIME	DEVICE	USERID	SRCADD	SRCPORT	DSTADD	DSTPORT	APPID	URL	NAT USERID	NAT SRCADD	NAT SRCPORT	NAT DSTADD	NAT DSTPORT
2022-11-14 15:22:34	Citrix (172.16.68.15)		172.16.68.192	8082	192.168.99.79	40025	TCP/8082			192.168.89.49	8082	172.16.68.17	37202
2022-11-14 15:22:34	Citrix (172.16.68.15)		172.16.68.17	37202	192.168.89.49	8082	TCP/8082			192.168.99.79	40026	172.16.68.192	8082
2022-11-14 15:22:47	Citrix (172.16.68.15)		192.168.99.79	40026	172.16.68.192	8082	lb_vsvr_PNA_HL7_8082			192.168.89.49	8082	172.16.68.17	37202
2022-11-14 15:22:56	Citrix (172.16.68.15)		192.168.89.49	8082	172.16.68.17	37202	lb_vsvr_PNA_HL7_8082			172.16.68.192	8082	192.168.99.79	40026
2022-11-14 15:22:44	Citrix (172.16.68.15)		192.168.89.49	8021	172.16.68.17	25725	lb_vsvr_PNA_HL7_8021			172.16.68.192	8021	192.168.99.79	54854
2022-11-14 15:22:44	Citrix (172.16.68.15)		192.168.99.79	54854	172.16.68.192	8021	lb_vsvr_PNA_HL7_8021			172.16.68.17	25725	192.168.89.49	8021
2022-11-14 15:22:53	Citrix (172.16.68.15)		172.16.68.192	8021	192.168.99.79	54854	TCP/8021			192.168.89.49	8021	172.16.68.17	25725
2022-11-14 15:28:02	Citrix (172.16.68.15)		172.16.68.17	25725	192.168.89.49	8021	TCP/8021			172.16.68.192	8021	192.168.99.79	54854

VIAVI Observer's easy to use navigation provides quick access to NAT/PAT data

Translation + Application Dependency and Performance

In addition to understanding and visualizing end-to-end conversations, NetOps and SecOps teams benefit greatly from Observer's ability to created automated, accurate depictions of how users interact with applications and how the application components interact and perform.



SecOps teams can immediately identify potential exposures and vulnerabilities while NetOps can leverage performance overlays and end-user experience scoring to automate problem domain isolation and root cause identification.

VIAVI Observer Provides:

- The ability to visualize end-to-end IP conversations as network addresses and ports are translated
- A clear understanding of how network devices are handling and impacting end-user requests
- Forensic-level analysis of suspicious and malicious traffic
- On-demand application dependency mapping based on actual network traffic
- Automated End-User Experience scoring and problem domain identification

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

viavisolutions.com