Troubleshooting End-User, VPN, and Network Path Performance Issues With NETSCOUT

By now, enterprises, government agencies, and service providers all recognize the indispensable role that virtual private networks (VPNs) serve in their hybrid workforce environments. Simply put, Information Technology (IT) Operations cannot assure high-quality end-user experience or reliable business service performance without dependable VPN performance.

However, as evidenced in this Use Case, even expert-level IT Operations resources can be surprised by how NETSCOUT's Visibility Without Borders approach helps identify unexpected dependencies in the network path essential for troubleshooting, root cause analysis, and service restoration.

Issue

This centralized government IT team faced a not-unusual scenario as agency workforces transitioned to work-from-home (WFH) environments – VPN login delays experienced at the start of their workdays prompted employees to contact their respective Help Desk resources for support. These service tickets were subsequently relayed to the centralized IT Operations team for troubleshooting and resolution.

When thousands of government users concurrently attempted to login around 9 a.m. each day, IT Operations easily determined VPN performance was sluggish but could not identify root cause.

These reports troubled IT Operations, as they had just deployed new VPN concentrators to support WFH users, as well as additional firewall and proxy technologies.

Impact

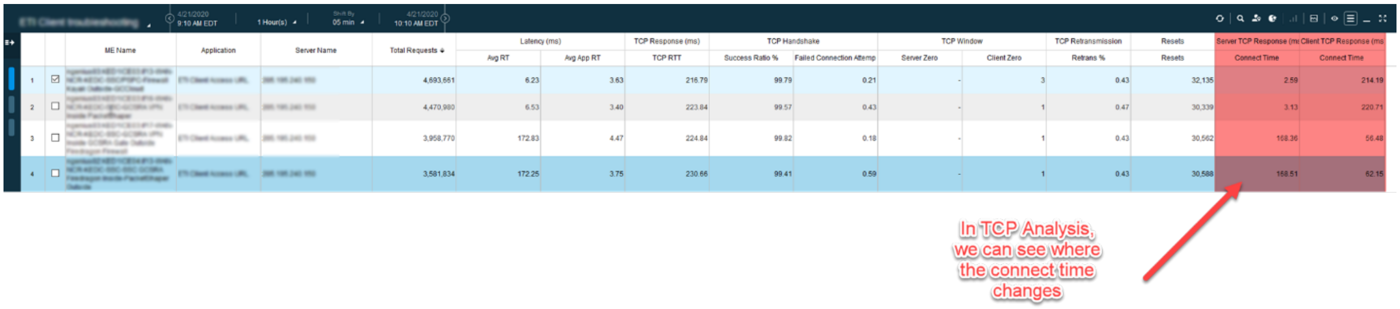
In this case, these VPN performance delays impacted government technologists providing mission-critical business services support to other agencies.

With numerous users experiencing these VPN performance delays, this was an issue that need to be addressed quickly, both to ensure employee productivity and efficient government operations, as well as protect the IT organization's reputation for quality service delivery.

As changes to the network can trigger unexpected performance issues, uncovering the true nature of this degradation was a priority. Beyond needing to improve performance and service access to WFH users, IT Operations was determined to find whether the root cause was related to new VPN concentrators, which were added to provide additional virtual network bandwidth, or the recent investments in firewall and proxy technologies.

Troubleshooting

The agency's IT Operations team collaborated with their contracted NETSCOUT® Engineer to leverage nGeniusONE® analytics and service edge visibility provided by installed InfiniStreamNG® (ISNG) appliances with integrated NETSCOUT Adaptive Service Intelligence® (ASI) technology to begin quick troubleshooting of this VPN performance issue. In making use of ASI-generated smart data that fueled nGeniusONE analytics, IT Operations employed a standard workflow to provide a single-screen view into network links along the VPN service path. With contextual drill-down to the Universal Monitor, IT Operations selected a "TCP Analysis" view to determine whether any TCP-level issues were responsible for the delays, such as TCP Server/Client and retransmission percentages or Server/Client duplicate acknowledgments.

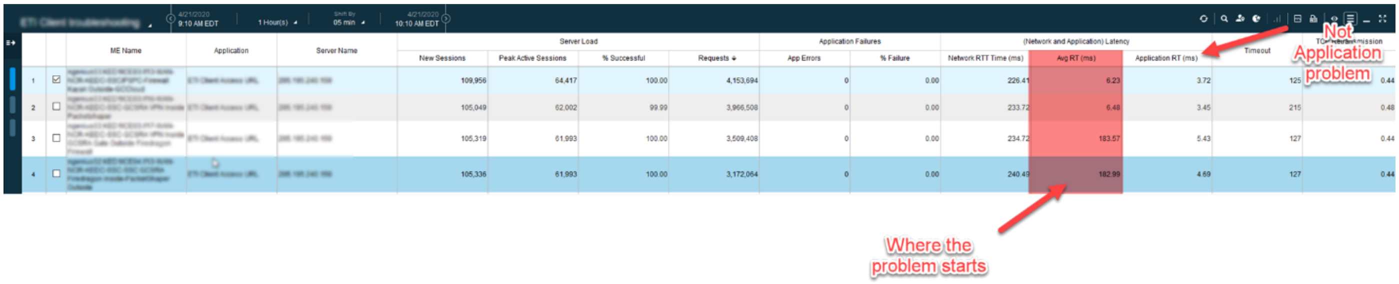


[redacted] 4/21/2020 9:10 AM EDT | 1 Hour(s) | Shift By 05 min | 4/21/2020 10:10 AM EDT

		ME Name	Application	Server Name	Total Requests	Latency (ms)		TCP Response (ms)	TCP Handshake		TCP Window		TCP Retransmission	Resets	Server TCP Response (ms	Client TCP Response (ms
						Avg RT	Avg App RT	TCP RTT	Success Ratio %	Failed Connection Attemp	Server Zero	Client Zero	Retrans %	Resets	Connect Time	Connect Time
1	☑	[redacted]	[redacted]	[redacted]	4,693,661	6.23	3.63	216.79	99.79	0.21	-	3	0.43	32,135	2.59	214.19
2	☐	[redacted]	[redacted]	[redacted]	4,470,980	6.53	3.40	223.84	99.57	0.43	-	1	0.47	30,339	3.13	220.71
3	☐	[redacted]	[redacted]	[redacted]	3,958,770	172.83	4.47	224.84	99.82	0.18	-	1	0.43	30,562	168.36	56.48
4	☐	[redacted]	[redacted]	[redacted]	3,581,834	172.25	3.75	230.66	99.41	0.59	-	1	0.43	30,588	168.51	62.15

In TCP Analysis, we can see where the connect time changes

Figure 1: nGeniusONE TCP Analysis provided evidence regarding where server connection responsiveness was delayed.



[redacted] 4/21/2020 9:10 AM EDT | 1 Hour(s) | Shift By 05 min | 4/21/2020 10:10 AM EDT

		ME Name	Application	Server Name	Server Load				Application Failures		(Network and Application) Latency			Timeout	TCP Retransmission
					New Sessions	Peak Active Sessions	% Successful	Requests	App Errors	% Failure	Network RTT Time (ms)	Avg RT (ms)	Application RT (ms)		
1	☑	[redacted]	[redacted]	[redacted]	109,956	64,417	100.00	4,153,694	0	0.00	226.41	6.23	3.72	125	0.44
2	☐	[redacted]	[redacted]	[redacted]	105,049	62,002	99.99	3,966,508	0	0.00	233.72	6.48	3.45	215	0.48
3	☐	[redacted]	[redacted]	[redacted]	105,319	61,993	100.00	3,509,408	0	0.00	234.72	183.57	5.43	127	0.44
4	☐	[redacted]	[redacted]	[redacted]	105,336	61,993	100.00	3,172,064	0	0.00	240.49	182.99	4.69	127	0.44

Not Application problem

Where the problem starts

Figure 2: nGeniusONE provided clear evidence that the Web server connect times were the root cause of this issue.

Using nGeniusONE in this workflow, IT Operations also viewed detailed response time metrics between five different devices along the network path, ranging from the VPN client onto the data center. IT Operations also viewed detailed response time metrics between five different devices along the communications path, including the VPN client at the client edge, to the VPN gateway at the network edge, through to the data center service edge, where the government applications were located.

As exhibited in Figure 1, nGeniusONE's TCP Analysis identified a proxy server was causing connect time delays.

As exhibited in Figure 2, TCP Analysis also identified where the problem originated along the network path and ruled out application performance as the root cause of this issue.

Remediation

As a result of nGeniusONE's root cause analysis, IT Operations remediated the identified performance delays by upgrading their proxy server environment.

Summary

With many of these agencies themselves tasked with delivering financial and medical services to residents, it would only have been a matter of time until these performance delays adversely impacted constituents, government business, as well as the IT Operations' reputation. Restoring VPN service performance quickly and effectively with nGeniusONE analytics and NETSCOUT smart visibility helped IT Operations avoid these unwanted levels of scrutiny.

NETSCOUT.

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us