Maximizing VPN Remote Access for Business Continuity

Remote and mobile workforces have been commonplace for years. With the COVID-19 outbreak, organizations around the world suddenly needed to securely transition entire employee workforces to remote home offices. As a result, over the course of just a few business days, the use of Virtual Private Network (VPN) technology expanded from select remote users to entire employee populations. And overnight, VPNs became the lifeblood of today's business operations, critical to keeping alive commercial, government, and healthcare organizations.

If your VPN isn't functioning, your whole business is offline.

Issue

The current situation with VPN usage has changed all IT operations from a centralized data center network to thousands of remote offices.

The conversion to all-remote workforces using wide-ranging mobile devices to access business resources has led to quick saturation of VPN bandwidth. Beyond adding VPN bandwidth to cure the problem, IT teams now need to factor how the wide-ranging applications and services are consuming those resources - very quickly, they need to separate services essential to business from those that are now "nice to have."

The NETSCOUT® nGeniusONE® Service Dashboard example provided in Figure 1 shows how quickly VPN bandwidth was consumed in the early days of the pandemic.

Figure 1: This nGeniusONE, Service Dashboard view shows a clear spike in VPN utilization occurring in a three-day span, corresponding to the COVID-19 progression timeline.

Impact

For enterprise, commercial, government, and service providers alike, the influx of remote workers will inevitably lead to points of congestion, as users of certain systems (e.g., Cisco virtual desktop infrastructures, UC applications) must employ VPN for access. If the VPN resources are overwhelmed, then remote worker productivity will dramatically decline.

Similarly, Cisco WebEx, Microsoft, and Zoom video conferencing application usage rates are on the rise, with even first-time users now turning to these meeting apps to replace collaborative, face-to-face sessions formerly occurring in the workplace. These video conferencing apps fill a critical void in the workplace, but they now consume VPN bandwidth, as well. Likewise, employees are now likely to call into conference calls using VPN-connected laptops, which also consume bandwidth in a manner not envisioned in earlier network designs.

Companies will therefore need end-to-end visibility across their network and real-time performance monitoring to analyze the impact of increased competition for these resources. With the nGeniusONE platform, traffic monitoring metrics can be viewed by a range of keys, such as locations, user communities, servers, and applications. This granular nGeniusONE data is critical for accurately diagnosing issues, better allocating bandwidth, or building specific services to alleviate those issues. For example, with additional bandwidth not immediately accessible in some cases, nGeniusONE can help IT determine how voice and video services are consuming bandwidth, and whether disabling video for non-essential business is a viable, less-costly workaround to VPN upgrades. For those organizations with extensive Citrix VDI services running applications, nGeniusONE can pinpoint whether frozen screens or timeouts relate to the VDI or VPN, or another service dependency, assuring the right remediation is being applied to the problem at hand.

Triage / Troubleshooting

The nGeniusONE platform provides IT teams with real-time monitoring and trending analysis required for preventive service assurance and effective troubleshooting.

In the Service Dashboard provided in Figure 2, we see a relationship between the rise in usage and sessions aligning to the timeouts and delayed response times. New session timeouts rose by 18 percent – as the volume of VPN usage increases, so does the problem.

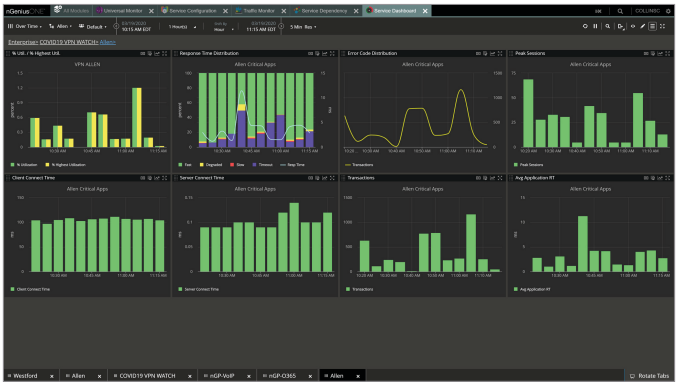

Figure 2: nGeniusONE Service Dashboard analytics providing single-pane views into error code distribution, as well as degraded and slow response times.

By combining these performance metrics into a single Service Dashboard customized for VPN monitoring, nGeniusONE provides a range of diagnostic views that allows IT teams (e.g., NetOps, SecOps) to recommend changes and institute best practices to alleviate performance issues.

With nGeniusONE, IT can pinpoint mission-critical applications and identify those having performance issues over VPN by looking into timeouts, slow response times, and retransmissions. We can then see the application affected by these issues and look for the root source of the problem. Using nGeniusONE to analyze session timeout instances, IT can see boundaries of response time, which can add value by showing that front-end servers rather than bandwidth may be the problem, for example. Similarly, nGeniusONE contextual analysis can show that retransmissions could also be linked to out-of-order packets or oversaturation of network links.

By contextually drilling down from the VPN Service Dashboard view, IT users can then access a corresponding nGeniusONE Traffic Monitor providing information regarding the Top 10 applications running on VPN.

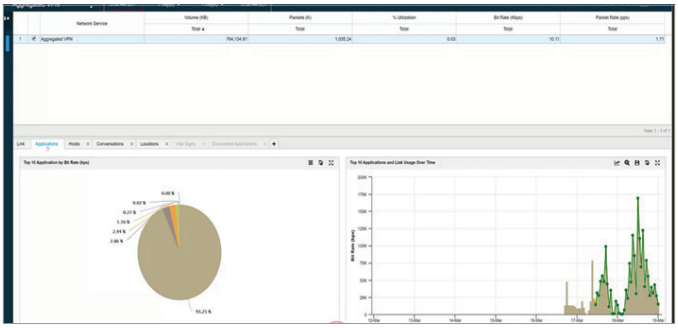

Figure 3: nGeniusONE Traffic Monitor view showing Top 10 applications running on the aggregated VPN. This view helps IT visualize how employees are consuming VPN resources, differentiating business application use from non-essential internet steaming services that consume valuable bandwidth.

For IT teams looking to monitor VPN user experience by location or communities, the Service Dashboard provides a single-pane, real-time view into overall performance.

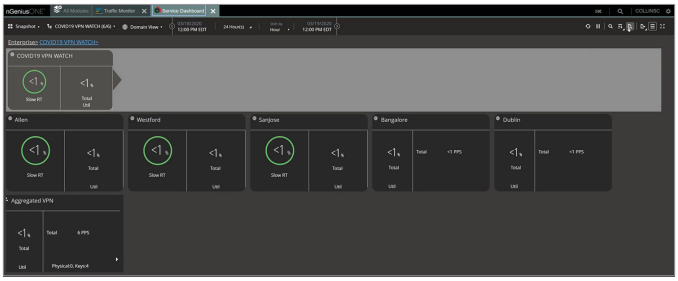

Figure 4: Using the Service Dashboard to look at communities of users also helps quickly isolate which sites may be having trouble with VPN services. In this example, less than 1% of users are experiencing VPN response time issues.

Remediation / Restoration

Using nGeniusONE traffic metrics allows organizations to make better-informed decisions on adding VPN capacity or configuring technology such as split-tunnel-VPN, which directs all internet traffic through local home networks.

It also helps companies hone and articulate remote access policies. For example, something as simple as constant communication about what applications require access via VPN and which do not can have a positive effect.

Summary

The COVID-19 pandemic has highlighted the criticality of visibility of both incoming bandwidth and VPN gateway resources to the health of today's business operations. Those organizations equipped to manage consumption of these VPN resources also require real-time monitoring and single-pane views into business application performance and user experience to ensure that the business is continuing to operate as seamlessly as possible during this new reality.

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

EUC_021_EN-2002 04/2020