NETSCOUT®

| WHITE PAPER |

Ensuring Business Continuity

Assuring Remote Worker User Experience Across VPN

ENTERPRISE

The virtual private network (VPN) has been a key enabling remote-work technology during the COVID-19 pandemic. For many enterprises, its use increased many-fold overnight to accommodate their entire workforce, something VPN was never designed for. ZDNet reported a rapid rise of VPN in many countries on March 23, 2020, in an article titled, "VPN Use Surges as Coronavirus Outbreak Prompts Huge Rise in Remote Working." Also, in March 2020, 451 Research conducted a flash survey of 802 IT decision makers to assess the impact of coronavirus pandemic on the way we work. Some of the findings are explained in a research note published on March 26, 2020, titled, "Coronavirus Quick Fixes Aren't Scalable; Business Leaders Must Rethink Work Itself." The report states that 62 percent of respondents have already experienced a fall in employee productivity or expect to in the next three months. And, 88 percent are spending less on business travel, while 78 percent of businesses believe expanded work-from-home (WFH) has already had a negative operational impact.

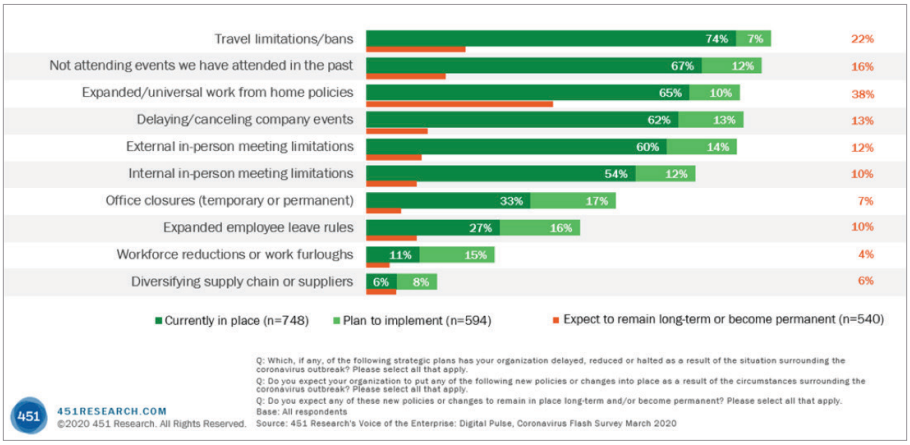

Figure 1: Source - 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey March 2020.

According to the report however, "The standouts are the 75 percent that already have or will be implementing expanded work-from-home policies in response to the crisis, and the 38 percent that think those policies will be long-term or made permanent. This is startling data, given that for most businesses remote work (if supported it at all) has typically meant only for some employees and only some of the time." This is a clear indication that expanded remote work is a post pandemic reality for many enterprises, not only as a means of meeting employee job satisfaction but also as a fiduciary risk-mitigation responsibility.

However, these radical changes are not without their challenges. One respondent, a Senior Manager of a 1-249 employees, $1M-9.99M company writes, "Remote access infrastructure enabling work-from-home is overwhelmed at primary client. Not enough capacity for everyone to work from home. This is affecting productivity and will likely result in delayed project timelines and increased project costs."

The standouts are the 75 percent that already have or will be implementing expanded work-from-home policies in response to the crisis, and the 38 percent that think those policies will be long-term or made permanent.

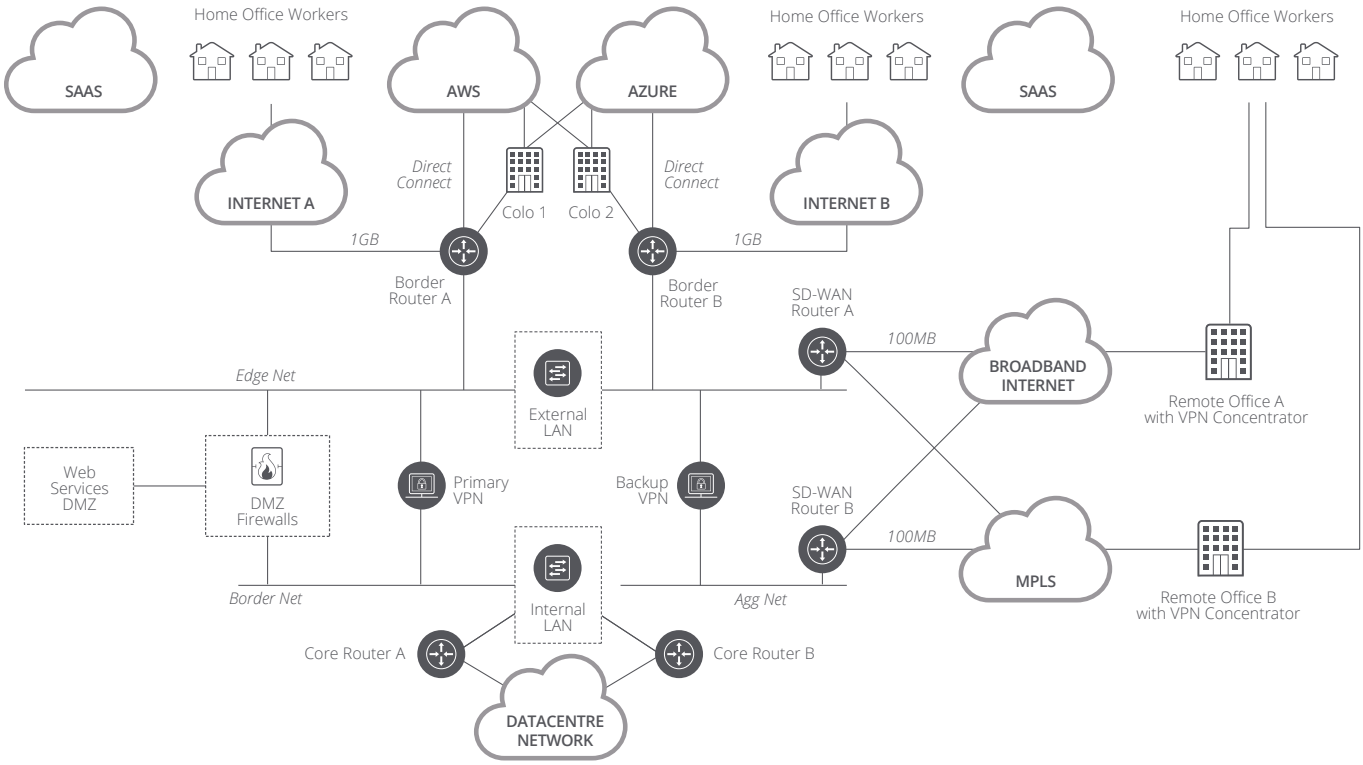

Figure 2: Typical network connectivity for remote branch and work-from-home employees.

While most IT departments have met the challenges of remote work, it has largely been a reactive scramble that has stressed both IT infrastructure and staff. According to an April 9, 2020 article by 451 Research titled, "Network-heavy Services are Coping with Coronavirus So Far," the picture "has not been universally rosy." Unified Communications as a Service (UCaaS), VPNs and related applications "appear to have encountered performance issues as traffic surged in early to mid-March," the report states. "Network provider Cogent experienced brief but noteworthy outages on March 11 and 18 (2020)."

Is the job done if employees can work remotely today? The answer is a resounding no. One of the first things beyond access that organizations must enact is visibility across the newly indispensable VPN infrastructure to ensure dependable operation, adequate capacity, and assure user experience.

Delays and unavailability are the last things you want your employees to cope with while scrambling to access enterprise resources in new and unfamiliar ways. Poor user experience is a productivity killer and a negative for IT. But what is user experience? At NETSCOUT®, we define user experience by its five tenets: availability, reliability, responsiveness, quality, and security.

The reactive nature of responses to the COVID-19 pandemic has created a period of more frequent changes to IT infrastructure under often lax (change management) oversight, leading to higher risks of errors and unintended consequences. Furthermore, these changes are likely to continue, while many enterprises evaluate enhancements to their remote work strategies going forward. Visibility is a prerequisite to planning, smooth running operations, and risk mitigation. It is a necessity, not a luxury.

While, visibility must be part of an overall end-to-end architecture, here we focus on three use cases to demonstrate the importance of maintaining visibility into your VPN infrastructure going forward:

- Right-sizing VPN hardware
- Enabling network engineering to meet demand with relevant data
- Assuring user experience in the new normal, especially for two other critical remote work technologies, unified communication and collaboration (UC&C) and virtual desktop interface (VDI), which are inherently sensitive to network jitter and delay.

For reference, Figure 2 shows a typical enterprise network in which the headquarters and several smaller data centers and remote locations are connected via an SD-WAN or an MPLS mesh network. The network at HQ provides redundant connectivity to the internet, co-lo, and cloud service providers. The HQ Network as well as remote branches house primary and backup VPN concentrators, which are located between edge and aggregation networks. (VPN concentrators can optionally be placed in the DMZ also as a design choice. Alternatively, VPN concentrators may be placed in co-lo in a similar configuration.) Home-based users will be connected to the closest VPN concentrator using GeoDNS to consume UC&C, VDI, and business services.

Prior to the COVID-19 pandemic, the typical VPN infrastructure was designed to accommodate work-from-home for a small percentage of the workforce some of the time. How those remote users accessed the internet (e.g., via routing remote VPN users' internet traffic through the corporate network or not) was a design choice and a trade-off between marginally increased bandwidth usage on the network and that of enforcement of network security policies. During the pandemic, social distancing orders across the globe forced businesses to accommodate remote access for almost 100 percent of their workers for virtually 100 percent of their workday, something that strained existing VPN capacity across the board.

VPN Capacity – In the early days of the pandemic, one of NETSCOUT's customers, a broker dealer in financial services, whose VPN was designed for 1,100 users, had to shift to accommodate 11,000 users overnight. To do this, the company upgraded their VPN software license as well as their internet bandwidth with relative ease. But this was not enough to ensure acceptable user experience. What remained was to match the VPN's physical resources (and other components now affected by the shift in traffic volume) with the new reality to ensure VPN hardware would not become a bottleneck.

To do this, you need data: data about the new traffic patterns, their impact on VPN concentrators, and the rest of shared infrastructure. Furthermore, this data must be evaluated in the context of user experience throughout the workday and across the work week to identify bottlenecks including transient ones. A good indicator for such anomalies is TCP zero window or reduced TCP window signaling that are encoded in network packets. TCP zero window indicates one or the other party is resource starved and unable to receive any more packets - a tell-tale sign of resource bottlenecks.

Enabling Design with Data - In order to accommodate increased VPN access demands, another accommodation had to be made. It was now necessary to remove any unnecessary internet-bound end-user network traffic from being routed through the VPN. This is known as a split tunnel VPN design, in which users' internet-bound traffic is routed directly through their broadband provider. This can be quite complicated, since some of the internet-bound traffic may still need to be routed via corporate network (e.g., certain SaaS applications). Again, to do this, in a world where the enterprise perimeter blends with so many internet-based services, you need network traffic data, including the mix of users, applications, and destinations - data that can serve as the foundation of split tunnel VPN configuration and later can verify its correct operation.

Once users are logged onto the VPN, one of the most tangible aspects of their experience is the system's responsiveness, because it is experienced repeatedly with every key-stroke, communication, transaction, or look up.

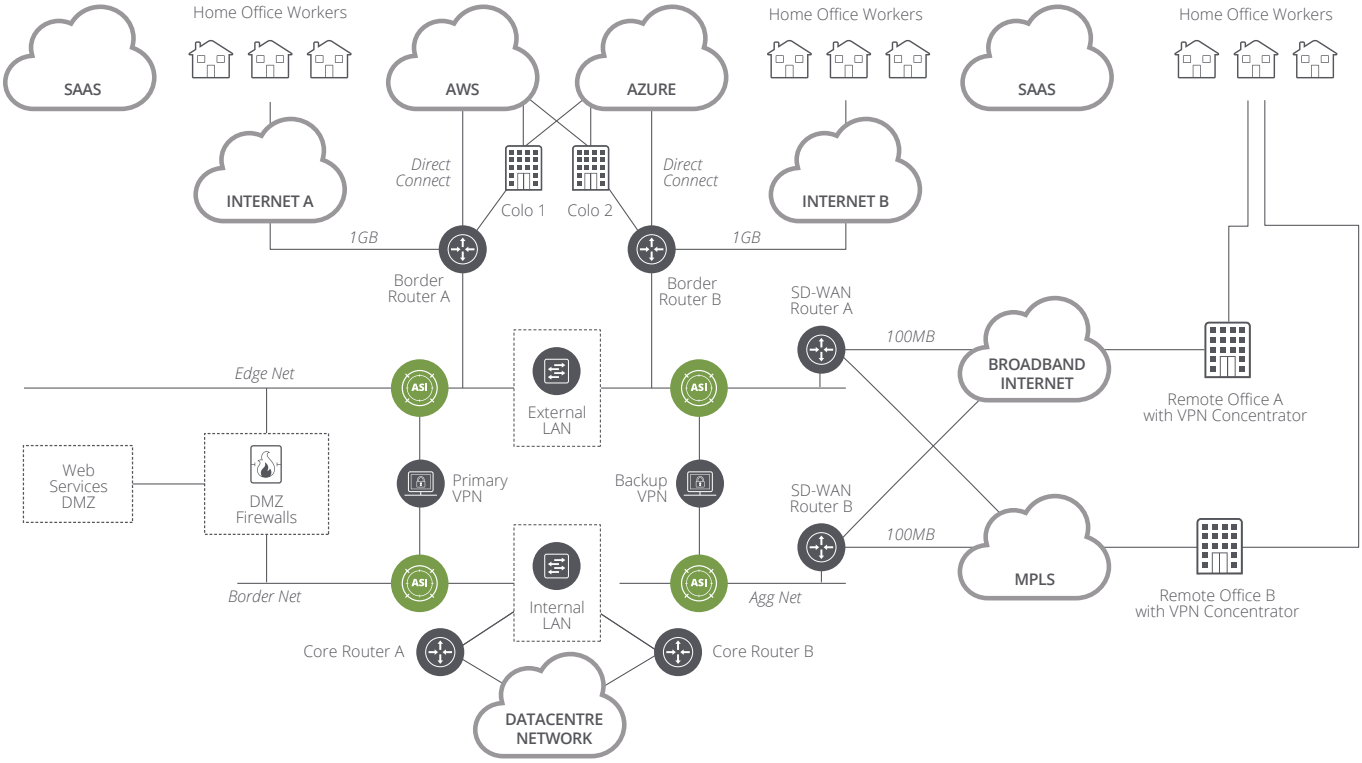

Figure 3: Recommended points for NETSCOUT instrumentation placement in a VPN infrastructure.

Assuring User Experience – As governments all over the world begin the process of lifting work-from-home-directives and replacing them with phased approaches to re-opening businesses, some employees will begin returning to their offices. This is unlikely to look anything like it did before COVID-19 arrived. With major corporations such as Twitter, Google, Facebook, and others announcing employees can work from home through the end of 2020 or longer, VPN access will continue to be necessary and, in fact, will become a strategic business enabler.

In IT operations, change is the enemy of stability. Delivering high-quality user experience through the VPN could be challenging during normal times, given the dynamic nature of user behavior. A period of increased changes amplifies the risk profile by introducing configuration errors with unintended consequences. Employees working from home often expect nearly the same quality of user experience they receive when they are in their offices. For VPN, this means a secure and available service, seamless logon, and responsive user experience. At the same time, IT is faced with the challenge of delivering good user experience across hundreds or thousands of employee homes, each with its own broadband carrier and Wi-Fi networks, in as many varieties as you can imagine, over which IT has no control.

Once users are logged onto the VPN, one of the most tangible aspects of their experience is the system's responsiveness, because it is experienced repeatedly with every key-stroke, communication, transaction, or look up. To deliver quality user experience, response-times must be managed within acceptable thresholds. For a web or client/server transaction, 1 second is a good place to start, although research shows, that over the past two decades users have come to expect a response-time of 500 ms or less. However, for both UC&C and VDI applications, which are critical to remote work, response-time thresholds are more stringent.

Both UC&C and VDI services run their own transport over the network. An ideal network round-trip response-time for both services is a threshold of 100 ms or less; at 150 ms both services start to deteriorate, and at 200 ms network round-trip delay, they both become essentially unusable. They are also highly sensitive to network jitter and packet loss, which can make a call jumbled or choppy and can cause smearing or pixilation in video, or even gaps in recordings or in devices being marked offline in a video-management system. Here, underlying causes of poor performance are often found in the introduction of additional hops in the network, under-resourced hardware such as VPN appliance and Wi-Fi access points, sudden shifts in traffic resulting in network congestion, asymmetric routing, misconfigured network quality of service (QoS) settings, and older or faulty hardware. To mitigate these risks, you need real-time visibility into not only user experience but also its components of network time, server time, and client time.

NETSCOUT's nGeniusONE® Service Assurance platform leverages smart data generated by patented Adaptive Service Intelligence™ (ASI) technology found in InfiniStreamNG® (ISNG) software- and hardware-based appliances, as well as vSTREAM™ virtual appliances. The solution monitors and analyzes packet data, using machine learning (ML) algorithms, throughout private and public cloud environments for any application, anywhere, to quickly pinpoint and resolve issues that may impact your business and end users' experience. The solution even stores actual network traffic to provide deep forensic analysis for security or application performance issues.

As shown in Figure 3, recommended NETSCOUT instrumentation, denoted by the green ASI circles, is accomplished by tapping network traffic on either side of VPN concentrators at each location and feeding that traffic to NETSCOUT ISNG physical or vSTREAM virtual appliances.

Figure 4 demonstrates a subset of capabilities within the nGeniusONE and ISNG solution that could address all the challenges associated with delivering good user experience across the VPN infrastructure. Service dependency mapping provides real-time, as-is, application infrastructure dependency mapping, while the configurable dashboard provides a high-level mechanism for managing a service by its key performance indicators (KPIs). Service and link monitors provide detailed KPIs about the operation of applications, user experience, servers, network, and the client and greater client communities.

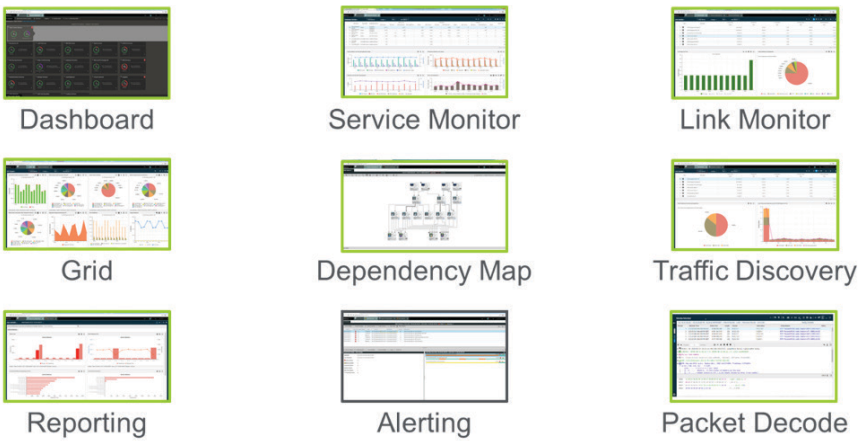

Figure 4: Subset of nGeniusONE capabilities used in monitoring user experience and VPN performance.

Traffic discovery, grid, and reporting provide real-time and historical mechanisms for exploring data such as inbound and outbound traffic rates, user, destination, and application mix needed for network engineering and verification of split tunnel VPN operation. TCP window signaling and packet loss reported over time in service and link monitors provide the data necessary for ensuring that a VPN appliance is correctly sized for the task. By comparing these metrics on both sides of the VPN, you can quickly determine whether there is a bottleneck upstream, downstream, or within the VPN itself. The solution even provides a specialized monitor for analyzing inbound packet loss on the encrypted side of the VPN concentrator. Similarly, packet loss and network jitter are among a powerful set of features for UC&C applications troubleshooting. The platform also reports a breakdown of user experience into network, server, and client time. Finally, reporting and alerting allow you to manage each service within the desired thresholds.

The solution does not stop there, however. To address the challenge of managing user experience when it also depends on employee home networks, NETSCOUT also provides the ability to run synthetic business transaction tests by using nGeniusPULSE technology for analyzing the tests conducted by nPoints. These tests can run virtually anywhere - on a user's computer, as a small device that plugs into the network, or as a Wi-Fi endpoint. These synthetic tests run 24x7 and can detect potential issues before a user may see them. They can be distributed to home or remote users.

Finally, the entire NETSCOUT solution portfolio can be delivered by NETSCOUT's VaaS (visibility-as-a-service) organization. The VaaS team will deploy, configure, operate, and address the day-to-day upkeep of the solution so customer can focus on delivering superior service.

Summary

The sudden and unexpected impact of the COVID-19 pandemic has amplified the importance of visibility for ensuring that the employees' experience using corporate application resources from home is as seamless and high-quality as it was when they were working in their offices. As a new normal emerges for corporations and their employees, NETSCOUT nGeniusONE and nGeniusPULSE, will help ensure performance and end-user experience meet these critical goals and expectations today and into this new future.

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

EWP_026_EN-2001 07/2020