Global Biotech IT Group Ensures Telecommuter Productivity

While most enterprises had procedures for telecommuting, only a few were ready to accommodate virtually all of their employees working from home (WFH) at once due to the pandemic. The IT team of a major multinational biopharmaceutical organizations also scrambled to prepare their business continuity plan, which included provisioning adequate resources for the virtual private network (VPN) connectivity in all domestic and overseas locations.

Due to the unexpected nature of the pandemic, this IT team had to add extra capacity using a combination of virtual and physical VPN appliances. They relied on the VPN gateway vendor data sheets to size the new capacity provisioning, however confidence in their plan was shaken as some of the remote users began to experience inconsistent VPN quality of experience.

The Challenge: Confidence in Business Continuity Plan

This organization increased VPN capacity across two of their major international sites. They thought they had dimensioned the VPN gateway to accept 4,000 and 6,000 concurrent SSL VPN connections. However, the new rollout wasn’t as smooth as they had hoped, as multiple issues were reported by their employees, impacting their user productivity. The IT organization was facing a crisis.

Company:
• A top, multinational biotech company

Key Issues:
• Surge in number of telecommuters strained the VPN infrastructure
• Maintain employee’s productivity without security compromise

Solution:
• Keysight’s SSL VPN Assessment Service

Results:
• Proper sizing of the infrastructure
• Optimization of the VPN gateway parameters to maximize user experience
The VPN gateway vendor was not able to isolate the issue but did reconfirm the provisioning should be able support the desired concurrent SSL VPN sessions. They recommended the IT group contact Keysight for a test solution that could validate the limits of the VPN infrastructure under their realistic production network conditions.

**The Solution: Just-in-Time Validation**

Keysight’s SSL VPN Assessment Service was the right fit to validate the realistic capacity and performance of their newly upgraded VPN gateways that were servicing two key offshore sites. In partnership with the Keysight’s Professional Services engineers, the IT team was able to systematically isolate the issue through a series of tests that were executed simulating various real-world deployment conditions and VPN gateway parameters. The turn-key SSL VPN Assessment Service emulated the desired number of VPN clients from a public cloud—initiating connections to the VPN gateways and generating a controlled volume of traffic over the established VPN connections. The entire testing was conducted in a controlled and secured manner during a maintenance window to avoid any undue disruption to the production network.

![Cloud-Scale, Kubernetes-Based Platform for VPN Client Emulation](image)

Keysight’s service measurements employ a highly distributed, dynamically variable number of VPN clients talking to each other and/or LAN server(s).
The Test Results: Under-sized VPN Infrastructure

One of the suspicions for the reported connectivity issues was the connection rate, several test sessions were executed at varying connection setup rates between 2 and 16 new connections per second. Results clearly showcased the number of successful connections and connection establishment time, and no major differences were noticed for the different connections rates. The IT/Keysight team concluded that the VPN gateway was able to sustain the VPN connection rates.

Keysight then moved on to validate the VPN capacity limits and were able to prove that both of the VPN gateways were capable of sustaining the maximum capacity of 4,000 and 6,000 concurrent VPN tunnels.

SSL VPN assessment results showcasing that close to 4,000 VPN tunnels were successfully established.

However, the surprising result was on total throughput capacity of one of the sites. The test was configured to establish 4,000 VPN client sessions, with each session transmitting 100kbps throughput over each VPN tunnel, the expected total throughput was 400Mbps. However, the VPN gateway’s throughput capacity was capped out at 110Mbps, drastically affecting the per-tunnel throughput performance across all tunnels. This has direct correlation to the quality of experience for all users.
Throughput stats for total VPN gateway and each emulated VPN client.

The graph above clearly shows how initially the throughput linearly increased as the VPN tunnels were getting established and then capped out at 110Mbps. In the bottom graph, you can see some of the tunnels were able to sustain 100kbps initially and as the throughput caps out, throughput profile per tunnel drops and becomes inconsistent (graph on bottom left).

Another surprising result was observed when validating the “Hardware Acceleration” option on the VPN Gateway. It was noted the acceleration option has no effect if IP encapsulating security payload (ESP) encrypted traffic is sent on the VPN tunnels. Enabling “Hardware Acceleration” only helps improve the overall throughput (by about 66%) when the traffic is SSL encrypted.

What were some of the findings?
- VPN tunnel capped out at 110Mbps
- Throughput per tunnel drops as VPN tunnel caps out
- Hardware acceleration only improves throughput when traffic is SSL encrypted
**Actionable Steps to Improve Capacity and Save Costs**

By validating their VPN gateways with Keysight’s SSL VPN Assessment Service, the IT organization was able to identify and address the bottlenecks. As the network operations manager concluded, “disappointing, yet informative.” Armed with specific insights into the realistic capacity limits, the team took action to increase capacity and also use split tunneling policies to alleviate the throughput bottleneck and for better user experience. They will use Keysight to retest once their remediation steps are implemented.

Many companies are over provisioning their VPN deployments at added cost in an effort to ensure good quality of experience to telecommuters. Using Keysight’s SSL VPN Assessment Service, IT organizations will have the confidence that their infrastructure is properly dimensioned at optimum cost to support the increased workload.

**Related Information**

- SSL VPN Assessment Service: [https://www.ixiacom.com/VPN-Check](https://www.ixiacom.com/VPN-Check)
- SSL VPN Assessment Solution Brief: [SSL VPN Gateway Test Service](https://www.ixiacom.com/VPN-Check)
- Free self-service SSL VPN Availability check: [https://vpncheck.io/](https://vpncheck.io/)
- Demo Video: [VPN Gateway Validation Service](https://vpncheck.io/)

Learn more at: [www.keysight.com](http://www.keysight.com)

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: [www.keysight.com/find/contactus](http://www.keysight.com/find/contactus)