

nGeniusONE for VPN Monitoring

The availability and performance of remote access infrastructure like Virtual Private Networks (VPNs) are critically important to enterprises today due to the dramatically increased use for remote workers in the wake of the COVID-19 pandemic. As VPNs afford companies the most secure way of digitally connecting employees to corporate resources, it has become an ever-more essential resource to enterprise businesses. Not surprisingly, VPN dominates the remote access market for enterprises, with that global market expected to exceed \$114.5 billion by 2027 according to recent analysis by Bizwit Research & Consulting LLP.

For employees connecting to corporate resources remotely over VPNs, anything less than a flawless experience is frustrating and demotivating. To corporate management, delays and unavailability are productivity killers and a negative for IT. Frankly, it is the last thing employees should need to wrestle with while scrambling to access enterprise resources in new and unfamiliar ways. As a result, visibility is a necessity for VPN planning, ongoing operations, triage and troubleshooting. It is not just a nice to have now, but a need to have!

The NETSCOUT® nGeniusONE® Service Assurance platform leverages smart data generated by patented Adaptive Service Intelligence™ (ASI) technology in InfiniStreamNG® (ISNG) software- and hardware-based appliances, as well as vSTREAM™ virtual appliances. The solution monitors and analyzes packet data, providing IT with a comprehensive view of service performance across complex N-tier application environments. nGeniusONE enables IT teams to triage issues impacting VPN performance and availability faster, which ultimately reduces Mean Time to Repair (MTTR). It does this by analyzing ASI data and by providing seamless, contextual workflows.

Performance Issues Addressed by nGeniusONE

nGeniusONE delivers end-to-end visibility into the performance of an integrated application environment including server activity, service enablers, database tiers, application tiers, Web tiers, and the network - including activity across the VPN. In particular, nGeniusONE answers several critical questions related to active sessions, usage, and transport issues;

factors that may impact VPN performance, including:

- How many remote users are connected?
- How much bandwidth is consumed? In volume (KB), in & out? In packets (K), in and out?
- Which VPN protocols are in use?
- Are there transport issues? Packet loss in or out? Responsiveness issues? Set up failures?

With nGeniusONE, IT organizations benefit from being able to monitor the physical links underpinning the VPN connection for such things as network load, number of concurrent users, and overall health of the ISP link for early indications of service disruptions like packet loss, to stay ahead of, or rapidly identify, problems and determine the root cause.

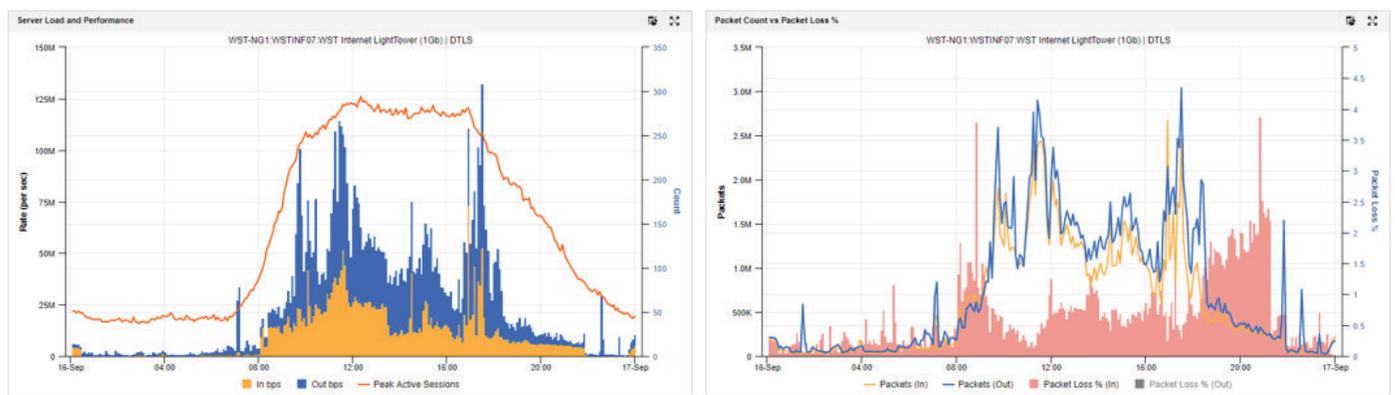


Figure 1: VPN Monitor view provides metrics and analysis on VPN load and performance, response time and throughput, successful vs. age-out transactions, and on packet loss over time. This particular graph shows inbound packet loss increasing from lows in the early part of the day around 4 AM to highs experienced late in the day after 8 PM.

Support for VPN Services

In order to help IT resolve poor user experience issues, nGeniusONE relies on the power of ASI. Through continuous monitoring of all protocol and application traffic, ASI data enables nGeniusONE solution to deliver a holistic view into the activity and performance of VPN services to identify and mitigate performance and availability problems. This highly structured data provides operational insights and visibility into the potential bottlenecks, disruptions, or slowdowns. In addition to application performance, nGeniusONE provides advanced analysis to help identify any network level issues.

nGeniusONE provides IT teams with a vendor-neutral view of common VPN Services with the ability to recognize and track activity for key protocols: IPSec-ESP, IPSec-NAT, and DTLS. nGeniusONE brings useful, efficient top-down workflows to IT teams for problem identification, service triage, and resolution. These consistent, service-oriented workflows enable seamless, contextual drill-downs and analysis, facilitating efficient and informed handoff of VPN performance issues across different groups, fostering IT team collaboration.

The nGeniusONE platform simplifies the challenges for IT in delivering high-quality, performance and user experience across the VPN by providing logical contextual workflows that typically start with dashboard views, dependency maps, specialized service monitors, e.g. VPN Monitor, session and packet analysis. Specifically, for nGeniusONE in-depth analysis of VPN activity the focus is:

- **VPN Monitor** – The VPN Monitor is a specialized service monitor for IT to monitor VPN user-experience metrics for IPSec-ESP, IPSec-NAT, and DTLS protocols as used in either Client-to-VPN Concentrator deployments or Site-to-Site VPN deployments. Key metrics in at-a-glance views are available to investigate both VPN activity and health, as exhibited in Figure 2. Critical metrics include:
 - **Active Sessions** for number of connected remote users; number of active peering connections; and capacity of the VPN concentrator
 - **Bandwidth usage** for bandwidth consumption in volume (KB) for both in & out traffic and in packets (K) for in & out traffic
 - **Transport issues** to stay ahead of emerging problems, with VPN Monitor tracking the number of packets lost for both inbound and outbound traffic, as well as the number of setup failures that occur
- **Packet Analysis** – Enables deep-dive protocol level analysis and forensic evidence collection. Using packet analysis, IT teams get visibility into VPN protocols, including DTLS, IPSec-NAT, and IPSec-ESP.

For many enterprise organizations, VPN Monitor analysis and views will provide the deep-dive troubleshooting necessary to identify issues they are facing. Should IT teams require additional detail, they can drill down further to the Packet Analysis layers.

Benefits of nGeniusONE for VPN Monitoring

- **Quickly and Efficiently Triage Issues** – Comprehensive visibility and sophisticated VPN Monitor analysis in nGeniusONE enable IT teams to efficiently research performance issues, rapidly identify the root cause, and reduce MTTR.
- **Ensure Business Continuity** – Assuring high-quality performance for a remote workforce across critical VPN access ensures employee productivity, which in turn helps meet revenue and business goals.
- **Improve Collaboration** – Using visibility on both sides of the VPN gateway provides the analysis and evidence necessary to improve time to knowledge and effective collaboration among and between network, security, and third-party ISP / WAN teams.
- **Optimize Budgets** – As volatility in number of remote users and the capacity consumed for what they are accessing over VPN continue, trended data in nGeniusONE will help IT better analyze and plan bandwidth and capacity changes, based on evidence, to balance availability and budgets in the best way possible.



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