Visualizing Vendor-Encrypted SD-WAN Network Traffic with NETSCOUT

Security Operations (SecOps) teams today are using industry-standard or proprietary protocols to encrypt traffic traversing their network to increase privacy and integrity protection across their businesses.

This Use Case describes how one enterprise information technology (IT) team used NETSCOUT to provide much-needed visualization and monitoring of networked application traffic that was being encrypted and compressed by wide area network (WAN) accelerators used in their vendor-provided Software-Defined WAN (SD-WAN).

Issue

The company employed an SD-WAN overlay, with all company sites operating in a network meshed with encryption. This configuration provided advanced routing, segmentation, and security capabilities for interconnecting the company's complex enterprise network, easing Network Operations (NetOps) efforts to deploy and manage the SD-WAN.

This solution addressed the company's security needs but made for difficult troubleshooting when issues surfaced regarding network capacity, application issues, and site-specific performance. Since the network packet traffic traversing the SD-WAN was encrypted with a proprietary protocol, NetOps could not view standard metrics and key performance indicators essential to standard troubleshooting and root cause analysis. Additionally, using a Decryption Appliance tool would not enable IT to visualize network traffic, since it had been encrypted using a proprietary, vendor-specific protocol rather than industry-standard TLS or SSL.

Impact

The employee-generated Help Desk tickets associated with network responsiveness, application access, site-specific business service performance, and high-level troubleshooting persuaded IT operators that SD-WAN performance was likely linked to the root cause of these issues. All told, IT leadership estimated that 30% of their work cycles were spent on trying to troubleshoot these issues.

Several of the sites experiencing performance issues were involved in the company's specialized manufacturing operations, so these poorly performing applications and SD-WAN network segments were hindering production and distribution activities, having a measurable financial impact on production costs and productivity loss.

Troubleshooting

The company had long relied on NETSCOUT® for smart visibility and real-time monitoring solutions to maximize business service performance and end-user experience. In looking for solutions to these performance issues, IT leadership conferred with the NETSCOUT Premium Support Engineer (PSE) contracted to operate NETSCOUT solutions at the company. The company's NETSCOUT investment included both InfiniStreamNG® smart visibility appliances and nGenius® NetFlow Collectors, both of which were used as data sources for real-time nGeniusONE® single-pane-of-glass analysis into network, application, cloud, site, and business service performance.

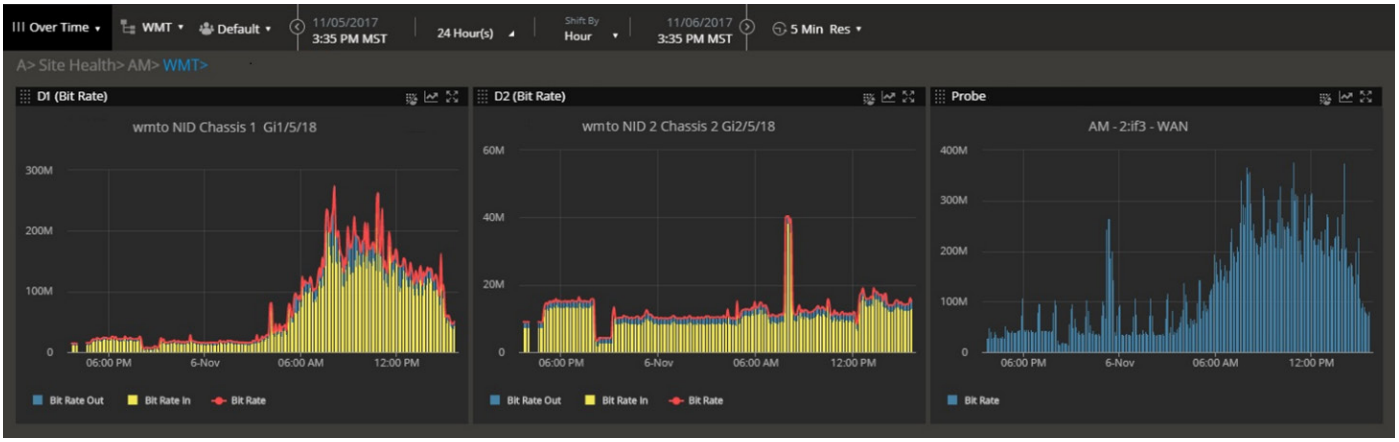

Figure 1: This nGeniusONE "Over Time" view provided Site Utilization statistics into network traffic spikes at the company's remote locations.

Based on the PSE's knowledge of SD-WAN operations, as well as the applications and sites reportedly experiencing performance issues, the troubleshooting process first focused on identifying a data source and instrumentation configuration that would provide the needed visibility into the encrypted traffic. In this case, the PSE's guidance was to use the deployed NETSCOUT nGenius NetFlow Collectors, which would hopefully yield unencrypted SNMP, MIB II, Cisco NetFlow data, and SFlow data from routers and switches operating in remote environments that could in turn provide smart data for nGeniusONE analysis.

When combined with nGenius for Flows, the NETSCOUT nGeniusONE Service Assurance platform provided single-pane visibility across data centers and remote networks using NETSCOUT smart data generated from a combination of wire data and flow data in one solution. The PSE took advantage of nGeniusONE's SNMP and NetFlow Monitors for analysis of network management protocols, as well as the contents of collected NetFlow in the Traffic Monitor. The results of IPPING/IPSLA tests were also reported in the Universal Monitor via nGeniusONE's Discover My Network functionality.

The PSE customized nGeniusONE service dashboard and monitor views to analyze the Flow-based data, including building real-time snapshots of site-specific performance.

As exhibited in Figure 1, a contextual drill-down from an nGeniusONE Site Health dashboard to associated bit rate analysis showed problematic spikes in network traffic in an "Over Time" monitor view.

Remediation

The IT team shared nGeniusONE Site Monitoring analytics with their SD-WAN provider as evidence of network traffic and associated capacity management issues in their remote environment, which persuaded that vendor to make necessary configuration changes to return business service operations to acceptable levels at impacted facilities.

Summary

In today's multi-vendor, multi-tier network operations, IT visibility problems inadvertently generated by a single element in the infrastructure have become commonplace – in this case, involving an SD-WAN supplier's use of encryption and compression.

In enterprise environments comprised of large-scale remote site operations, NetFlow remains a valuable data source for IT troubleshooting when traditional visibility options are limited.

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

© 2022 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.