Five Reasons for Deduplicating Traffic for Performance and Security Monitoring

Enterprises and Service Providers use TAPs and switch SPAN ports to capture network traffic and send it to performance and security monitoring tools using network packet brokers. To eliminate blind spots and to ensure 100 percent visibility, you need to capture traffic from multiple points along a network path. By nature of how traffic traverses between networks and servers, duplicate packets are often captured and aggregated together, sending nearly 40 percent duplicate traffic to the monitoring tools.

The reasons why enterprises implement packet deduplication in their packet broker deployments are:

1 Improve Monitoring Tool Accuracy

Many performance and security tools cannot perform packet deduplication. They assume all captured packets are valid in their analysis causing false positive errors, distorted measurements, and inaccurate KPIs.

2 Optimize Tool Performance

Monitoring tool performance and capacity are degraded due to the high volume of network traffic they process. Unnecessary, duplicate packets further burden these tools with unwanted overhead.

3 Free Up Storage, Network Bandwidth and Other Computing Resources

Monitoring tools archive packets for forensics and troubleshooting analysis. Duplicate packets consume large amounts of data storage, increase backhaul requirements and waste computing resources during analysis.

4 Shorten Troubleshooting and MTTR

When troubleshooting gigabit networks, it is nearly impossible to manually identify duplicate data. Even automated tools require time to process and identify duplicate data, causing inefficiencies and longer MTTR.

5 Reduce Total Cost of Ownership

Removing duplicate network traffic from reaching monitoring tools defers tool capacity upgrades and reduces total cost of ownership.

About NETSCOUT nGenius Packet Flow eXtender

The NETSCOUT® packet deduplication technology removes duplicate packets at line rate performance and provides a substantial reduction in traffic volume delivered and being processed by the tools. This provides an increase in tool efficiency, gaining value and performance by deferring future tool upgrades, a reduction in errors on the monitoring tool, and a closure of security holes that exist in other implementations. The deduplication capability includes selective packet deduplication, keyed secure hash for identifying duplicates, configurable duplicate packet detection window, discarding of all subsequent duplicates of any packet within the specified time window, and the generation of duplicated traffic statistics. The PFX software application runs on multiple x86 commodity server platforms with 4x10G, 2x40G and 2x100G interface configurations, providing high performance, scalability on demand in a cost-effective manner.

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

PFSFAQ_002_EN-2002 09/2020