Packet Deduplication with nGenius Packet Flow eXtender

The NETSCOUT® packet deduplication technology removes duplicate packets and provides a substantial reduction in the volume of traffic being delivered to, 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.

Background

Packet deduplication technology removes duplicated packets from network traffic that are being forwarded to the analytic tools for the purpose of monitoring, analyzing, and recording (see Figure 1). When accessing data from multiple points along a network path to gain visibility, by nature duplicate packets are often captured and aggregated together. Without the duplicate packets being identified and removed first, the tools will degrade in performance, alarm on the duplicates or produce compromised data and results.

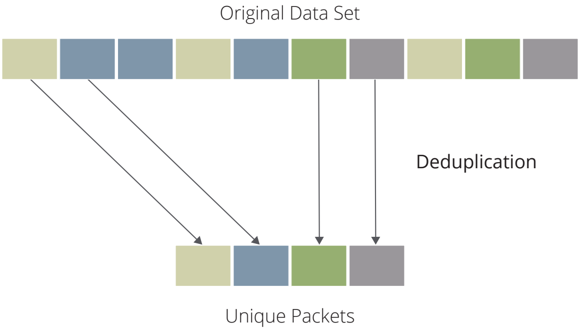

Figure 1: Unique packets are retained as shown, while duplicates are discarded before reaching the tools.

Primary Cause for Packet Duplication

Enterprises and Service Providers use TAPs and switch SPAN ports to capture network traffic and send to performance and security monitoring tools using network packet brokers. To eliminate blind spots and to ensure 100 percent network visibility, enterprises tap multiple segments of their networks. 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 tools.

Failure to deduplicate network traffic may cause the following issues:

- Monitoring and analysis tools may report false positive errors
- Additional bandwidth is needed for backhauling traffic to monitoring applications
- Duplicate packets can overload monitoring tool, resulting in packet drops

To avoid these unwanted effects, the monitoring tools need to deduplicate packets themselves before performing analysis of the traffic, which results in the following:

- Consumption of bandwidth on the monitoring tool port
- Consumption of valuable processing resources on monitoring tools resulting in a decrease of actual processing performance

Solution: NETSCOUT Deduplication Capability

The NETSCOUT deduplication technology removes packet duplicates and provides a substantial reduction in the volume of traffic to the tools. This provides an increase in tool efficiency, a reduction in errors on the monitoring tool, and a closure of security holes that exist in other implementations.

The nGenius® Packet Flow eXtender (PFX) software is key for performing packet deduplication. In visibility network deployments with nGenius 5000 Series and 7000 Series Packet Flow Switch, where packet deduplication capability is required, PFX can be added to perform the packet deduplication. PFX directly connects to the nGenius PFS port and the aggregated traffic is fed to PFX where the deduplication is performed, and then the de-duplicated traffic is returned to the PFS and available for all your tool needs (see Figure 2).

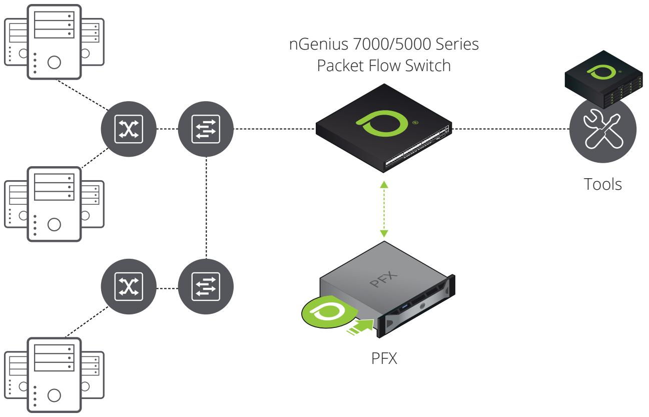

Figure 2: Deployment with nGenius PFS and PFX.

Key Capabilities

- Up to 200 Gbps line rate packet deduplication
- Configurable duplicate packet detection with IP header, IP header & CRC, Inner VLAN & IP header, Outer VLAN & IP header, IP header & 32-bit maskable offset
- Simultaneously work with all other PFX feature capabilities such as NetFlow generation, packet slicing, masking and tunnel header stripping

Solution Benefits

- Substantially reduces traffic volume sent to tools
- Improves monitoring tool performance, efficiency, and defers or eliminates costly upgrades
- Eliminates duplication-related errors and increases monitoring tool accuracy
- Reduces data recording wastage, storage devices and related costs
- Enhances forensics analysis efficiency and speed

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

© 2020 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.