Security Visibility

Optimize Packet Flows from the Network to Security Systems with NETSCOUT

NETSCOUT® nGenius® packet flow systems (PFS) collect and organize the flow of traffic from the network to the security systems and monitoring tools – creating a unified packet plane that logically separates the network layer from the tool layer. Packet flow switches are an integral part of this approach. Use them to optimize and scale both your service assurance platform and cybersecurity deployments so that you can spend less time adding, testing, and managing your tools. IT organizations are under pressure to rationalize network resources and extend the life of their current investments, rather than add new network capacity. NETSCOUT enables the networking and the security teams to implement joint packet visibility projects, rather than tackling each initiative individually, or on an ad hoc basis.

TOP 3 BENEFITS OF DEPLOYING UNIFIED VISIBILITY

1. Strengthen Your Network Security Architecture

Need to secure your network without risking its disruption? Afraid to place security systems inline? Want to maximize the efficiency of existing tools?

The nGenius architecture enables you to overcome objections to placing security systems inline. Defend your network in real time–without impacting performance. By providing a single, fail-safe access point into the network, nGenius packet flow switches let you deploy security systems inline virtually, to see and respond to threats as they occur. Avoid impacting the network, and gain flexibility to quickly respond to incidents and change configurations as needed, at any time.

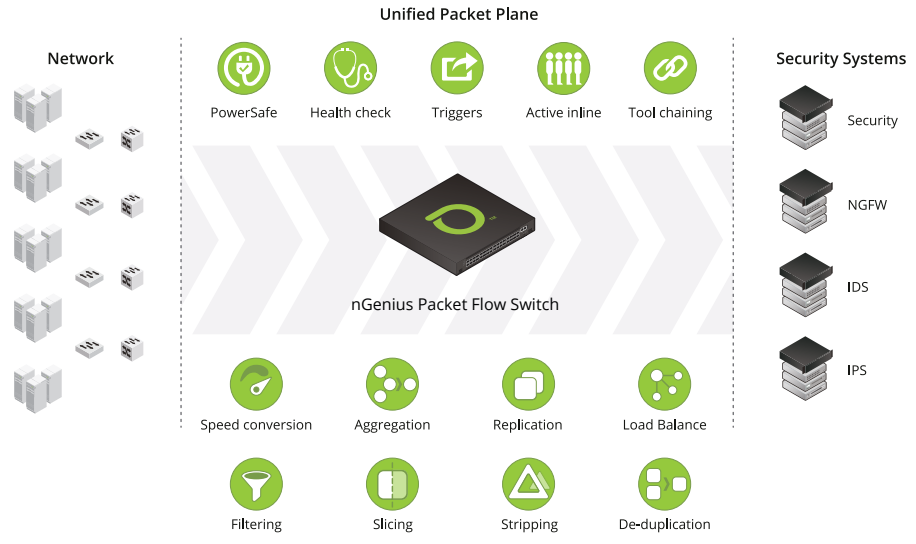

Figure 1: Packet flow systems provide the foundation for a scalable monitoring architecture needed for security and service assurance.

2. Increase IT Agility by Quickly Adapting to New Security Threats

Upgrading your network? Piloting or adding new security systems? Expanding to new data centers?

With nGenius, security tools are not anchored to static links. Dynamically control when new systems are deployed, what each system receives, the speed at which systems receive traffic, contingencies for "what ifs," and event notification timing. Make changes in software, at anytime, from a single interface. No need to make site visits or re-cable, saving time and money.

3. Optimize the Operation of Security Systems

Dealing with duplicate packets? Aggregating links? Need to analyze tunneled traffic that your security systems can't process?

Move beyond basic TAPs and matrix switches, which don't provide the features needed to get the most out of your security systems. When you're not able to fully optimize traffic for each of your tools, you drive up your monitoring infrastructure costs. Get answers fast and resolve issues as they occur, while effectively managing costs.

INLINE SECURITY CHALLENGES

According to the 2017 SANS Institute survey, *Network Security Infrastructure and Best Practices*, IT managers deploying inline security are most concerned about its adverse impact on the network. The majority (77%) cite the possible performance impact such devices can have, followed by concern over potential network outages and the introduction of additional network latency, at 54% and 52%, respectively.

Source: *2017 Network Security Infrastructure and Best Practices: A SANS Survey*

Key Capabilities for Security Visibility

- **Passive and active security:** create a pervasive defense architecture against a broad range of attacks. The nGenius packet flow switches provide critical visibility to combinations of security solutions like active inline network analysis and passive, out-of-band network forensics appliances as well as active payload analysis offerings.
- **Active tool chaining:** deploy an inline security infrastructure in a virtual chain, rather than cabling each system into a physical configuration. The key advantage of the nGenius implementation is the 50% reduction of ports needed and elimination of complex physical cabling configurations. Each device gets exactly the traffic it requires, at the speed and in the form that it is designed to accommodate, improving monitoring efficiency.
- **Application-level health checks:** performs a full diagnostic of the security system's functionality with both "negative" and "positive" health checks, beyond a simple on/off response, ensuring applications function as expected.
- **Policy-based triggers:** customize monitoring performance via user-defined mechanisms that trigger actions related to monitoring, forwarding rules and health status. Users can specify event policies that trigger certain actions, such as providing alerts via SNMP and Syslog, forcing ports into down link status and/or changing traffic forwarding mapping to tools.
- **Network bypass:** enforce your organization's specific security policies in the event of power loss. Behavior can be either Fail-Open, which allows the network traffic to flow back to the network unmonitored, or Fail-Closed, which blocks the network traffic from continuing to flow unmonitored.
- **Passive and active hybrid mode:** older security systems were dedicated to either active or passive inspection, but today's security systems fuse these functions into a single device which needs to receive both active and passive traffic. The nGenius PFS delivers both types of traffic on the same port to the security system that needs it.

NETSCOUT Packet Flow Systems

Switches

nGenius 5000 series packet flow switch

Software-driven and open compute-based platform for cost-effective packet brokering on 1G, 10G, 40G, and 100G networks. Provides up to 48 1G, 128 10G, 32 40G, or 32 100G ports; an external bypass tap is required for fail-safe operation.

nGenius 2200/4200 series packet flow switch

Hardware-accelerated packet optimization for service assurance and security systems on 1G, 10G, and 40G networks. Modular chassis provide a built-in bypass and up to 64 1G, 64 10G, or 16 40G ports.

nGenius 6000 series packet flow switch

Hardware-accelerated, highly dense blade and chassis packet flow switch that supports 1G, 10G, 40G, and 100G deployments. Includes built-in extended buffering to protect against the effects of microbursts.

TAPS

100% fail-safe access points for providing a copy of network traffic to a security system or packet flow switch.

ISNG Software

Built on the InfiniStreamNG™ platform, Packet Flow eXtender (PFX) integrates with NETSCOUT's packet broker products to enable expert-level capabilities, such as NetFlow generation.

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

© 2018 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.

PFSQL_004-1801 02/2018