NETSCOUT®

| WHITE PAPER |

Achieve Unified Packet Visibility at Scale

PACKET FLOW SWITCH

Packet Visibility as Prerequisite to Unified IT

In order to monitor and secure your entire infrastructure, today's service assurance and cybersecurity solutions require unified visibility into network traffic from key vantage points across your global enterprise. To direct the right traffic to the right tool at the right time and meet your corporate objectives you need a scalable, high-density packet acquisition system that provides capacity and flexibility via unified packet visibility. The resulting pervasive visibility can help you efficiently and intelligently optimize the flow of data from the network to the monitoring tools.

Old Siloed Approaches no Longer Work

Traditionally, different teams purchased its own packet visibility solutions to manage the flows of packets to performance monitoring and cybersecurity systems. With multiple monitoring systems in place, for service assurance and cybersecurity, they often contend for network switch ports because they can't all access every point in the network. If network or application performance problems occur, the lack of visibility slows troubleshooting and problem resolution.

Network Scale Brings New Challenges

Constrained budgets and lack of readily available IT talent mean that you have to do more with less. Updating monitoring tools or security systems in multiple locations consumes staff time in troubleshooting and firefighting. Many organizations are upgrading network capacity to cope with skyrocketing volumes of traffic. As they move from 1 Gbps switches and routers to 10 Gbps, 40 Gbps devices, or 100 Gbps the monitoring infrastructure can become overwhelmed with volumes of packet flows that it wasn't designed to handle, which is especially risky when it comes to network security.

Inline Security Deployments Exacerbate Risks

Security solutions are often deployed in response to a security attack. That means they are added over time, with teams choosing a different solution to cover each specific security gap. This creates multiple potential points of failure in the network, as well as differing bottlenecks in throughput.

From the monitoring perspective, the reach of a solution is limited by the number and bandwidth of ports available on the security solutions' hardware platforms and their throughput, which limits how many network segments they can protect. Software-based security solutions have varying performance "ceilings," depending on the task they perform, which can result in varying degrees of visibility.

THE NEED FOR UNIFIED VISIBILITY

The network is now assuring business success. Reliance on the enterprise IP networks drives the need for extensive monitoring infrastructures to ensure uninterrupted business services. But without deep packet visibility, you can't easily deploy new applications or secure them. This is why organizations must begin to take a strategic approach to gaining network visibility through a unified packet flow switching infrastructure, in order to stay agile and respond to evolving business needs.

Taking a New Approach

If anything, network complexity and competing demands for resources will continue to increase. Your teams need a more strategic approach to monitoring packets, via unified packet visibility that automatically delivers packets for performance management and security monitoring, according to policy.

Abstracting the monitoring tools from the network creates flexibility and efficiency for the IT team, letting them access the packet flows on demand. The visibility layer becomes a shared resource, managed by the IT or networking team. With unified visibility, you can standardize the monitoring architecture to reduce costs, simplify operations, and deliver true copies of traffic in real time. Security, application, and other teams can access the packets as needed. And new monitoring and security tools can be tested and deployed without network downtime or ongoing change approvals required. You can move to unified packet visibility in manageable phases, starting from wherever you are today and adding capabilities as required.

Phase 1: Laying the groundwork

When you're ready to gain visibility across the IT environment, use packet flow switches (also known as network packet brokers) to aggregate, optimize, and deliver traffic from networks to performance monitoring and security systems. Packet flow switches provide aggregation, load-balancing, replication, inline tool chaining, health checks, and more – in a cost-effective, software-driven architecture, both for passive monitoring and active (inline) security systems.

The latter is a requirement if you are deploying inline security systems, such as Intrusion Prevention Systems (IPS) or Next-Generation Firewalls (NGFW). The hybrid capability will allow simultaneous use of passive and active monitoring, migration from one to the other, and both passive and active traffic monitoring by the same tool port. Active security service chaining lets you deploy inline security infrastructure in a virtual chain, which significantly reduces port and cabling requirements. At the same time, it ensures that each device gets exactly the traffic it requires, at the right speed, and in the correct form.

Phase 2: Adding advanced capabilities

If you want to increase the effectiveness and usefulness of your monitoring and security infrastructure, add advanced packet-conditioning functionality to your existing packet flow switch devices for capabilities such as packet deduplication, header stripping, and NetFlow generation. This can be done by adding software capabilities on an external server or by deploying purpose-built, hardware-accelerated packet flow switches where this advanced functionality is required.

Phase 3: Achieving visibility at scale

In large networks, comprehensive analysis capabilities can give you rich network, service, and user metrics. A packet flow switch platform with massive scalability will support large, distributed service delivery environments – both passive and active. Combine your packet flow switches in an intelligent, self-aware mesh architecture. Should a link go down, the system of connections will automatically reconfigure itself – without manual intervention or the need to respond to an alert.

Figure 1: Developing unified visibility.

Gain Efficiency and Simplify Network Operations

Moving to unified visibility delivers a number of operational benefits. Increased efficiency, process simplicity, and reduced risk are some of the important advantages. Combined, they add up to a new level of IT agility – and a better way to confidently move beyond siloed cybersecurity and service assurance to business assurance.

Increased efficiency

Maximize your existing resources as you move toward unified packet visibility. Packet flow switches extend the life of existing 1 Gbps or 10 Gbps tools, avoiding the need to completely replace your monitoring infrastructure. Today's packet flow switches support 40 Gbps and 100 Gbps links so that you don't have to worry about running out of capacity and ports. Bringing active inline tools together in a redundant architecture lets you eliminate multiple single points of failure, achieving high availability of your security systems.

Simplified operations

With unified visibility, policies enable you to deliver the right packets to the right place, at the right speed, and in the right form. All constituents can get the packets they need – when and where needed. Reduce or eliminate complex design, approvals and change management processes.

With greater visibility, problems are identified and resolved quickly, compressing your meantime-to-resolution and thread-identification windows. Automation and event policies simplify additions and changes, saving time and reducing workloads.

High scalability and accuracy

With unified visibility, you can scale packet delivery for every need across an organization – whether it resides in a single campus or spans continents. Based on a self-organizing mesh architecture, it provides centralized management and delivers any to any packet flows from the network to the monitoring and security systems.

UNIFIED VISIBILITY AT SCALE

Unified visibility enables you to easily deliver service assurance and cybersecurity capabilities from one place, instead of having multiple, standalone monitoring projects across the infrastructure. Whenever and wherever an incident arises in your infrastructure, you have the deep visibility you need to respond fast and effectively. Key benefits are:

- **Deployment Readiness:** Ensure business services (applications) are rolled out smoothly and meet the expectations of the user community.
- **Proactive Monitoring:** Continuously measure the performance of services and infrastructure to identify potential problems and plan for new services.
- **Service Triage:** Quickly pinpoint and resolve problems before they have significant impact on the business.

For more information about NETSCOUT® packet flow switches, visit www.netscout.com/pfs.

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

PFSWP_007-1801 02/2018