

U.S. Agency Improves Network Agility and Further Secures R&D Environment with NETSCOUT PFS Technology

Innovative Solution Meets Cost-Containment Guidelines, Supports Network Transition to 100G Speeds

OVERVIEW

The Challenge

- Network upgrade to 100G surpassing support of installed packet flow switch footprint
- Refined packet conditioning requirements and additional cybersecurity tools requiring network packets

The Solution

- nGenius® 6000 series packet flow switch chassis
- PFS 6000 line cards, with 40 x 1Gb/10Gb and 6 x 100Gb QSFP28 Ports

The Results

- Increased network agility and R&D security
- Innovative solution design reduces data source footprint, meets government cost containment goals
- Extends value of investment made in monitoring tools



Customer Profile

This U.S. Government Agency is focused on research & development (R&D) activities designed to introduce scientific solutions that enhance the safety and environment of the country and its citizens.

Given the nature of the agency's work, their Network team is tasked with maintaining highly secure data center, computing, and campus environments with near-zero network performance latencies.

The Challenge

With their strategic focus and high-visibility organizational profile, the agency is a frequent target of cyberattacks. Maintaining high security is mission-critical for this agency, and for years their security assurance solution had benefited from NETSCOUT® packet flow switch (PFS) technology providing advanced packet slicing and active inline security functionality in their network environment.

The network team leverages traffic data (network or packet data) for several downstream tools and functions, including:

- Cybersecurity (e.g., Zeek intrusion detection system)
- Security incident and event management (SIEM)
- IT Service management (ITSM)
- Network performance monitoring throughout the network, including the SD-WAN

Of all the tools in place, deployment of cyber security tools consumes the most ports on the existing PFS platforms.

It was clear as the agency updated to higher network speeds of 100G for greater service performance, they were going to face challenges supporting these new speeds and higher traffic volumes with the existing packet flow switches and downstream monitoring devices, respectively. Simply put, they concluded that the most cost-effective solution was to update their PFS deployment, so it could support 100G interfaces. This would avoid the more costly alternative of replacing all their downstream monitoring and security solutions.

Additionally, the agency was now using 200G uplinks/ports, and the Network team had new, associated packet conditioning requirements involving de-duplication and packet slicing, then sending traffic to their security tools and other technology platforms that would further benefit from access to network packets.

All these changes were occurring in a network environment where the slightest network latency is an issue – even 1 millisecond delays are unacceptable to this agency.

For years, the NETSCOUT PFS footprint had well-served the agency's requirements, but the Network team knew a technology refresh would be required to handle increased network speeds and advanced packet conditioning requirements.

Given the value of intellectual property of the agency's collaborative R&D activities traversing the network and the open-ended cyberattack attempts the Network team was combatting every day, there was a high degree of organizational focus on this important PFS architecture refresh.

Solution in Action

The agency's deliberation in developing high-value technology for national security and U.S. residents also extended to their highly considered decision-making regarding new information technology acquisition, and this process also applied to refreshing their PFS environment.

After carefully mapping their requirements to possible technology solutions, the agency decided to address their 100G network upgrade and next-generation network packet conditioning specifications by deploying a NETSCOUT nGenius 6000 series packet flow switch (PFS) chassis in their computing data center, with hot-swappable PFS 6000 line cards supporting 40 x 1Gb/10Gb port and 6 x 100Gb QSFP28 port coverage, respectively.

This solution enables the Network team to bridge the gap in their transformative 1G, 10G, 40G, and 100G network and expanded cybersecurity tool environment, while assuring flawless network performance.

With this approach, the agency benefits from improved next-generation PFS technology supporting:

- Aggregation of 10/100G speed network taps, with the ability to then forward high-value network packet data to their in-place existing cybersecurity and IT tools
- Conditional packet slicing functionality for 64 kbps, which was a critically required feature
- Packet de-duplication

The Results

While there were competitive PFS solutions they could have pursued, the Network team's near-exclusive focus was deploying an innovative NETSCOUT solution that met the agency's government cost containment guidelines. With the agency relying on continued next-generation PFS technology and custom solution designs offered by NETSCOUT, they were able to avoid larger-scale solutions involving further deployment of additional data sources to process network traffic.

It is unlikely agency management would have been able to move forward with acquiring this important technology without the solution design and budget sensitivity shared by the NETSCOUT business partnership team.

Beyond maintaining access to the packet traffic in the data centers, the agency is extending the value of the investments made in their security and performance tools. With the nGenius PFS distributing the traffic from the 100GB links, with filtering and conditioning as appropriate, to the speeds available on the security and monitoring tools, they avoided a costly, early replacement and further capital outlay

Ultimately, the benefits offered by this new PFS deployment will enable the agency to develop new solutions that protect and benefit U.S. citizens in a secure, highly collaborative R&D environment.

LEARN MORE

For more information about NETSCOUT packet flow switch solutions, please visit:

<https://www.netscout.com/product/packet-flow-switches-and-taps>



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