NETSCOUT®

| WHITE PAPER |

Software-Driven Packet Flow Systems

Leveraging a Disaggregated Architecture with the nGenius 5000 Series Packet Flow Switch

Background

The development of Network Packet Brokers (NPB), or Packet Flow Switches (PFS), revolutionized network visibility and drastically improved the effectiveness of monitoring tools. NPBs enabled a new level of visibility optimization, forming the architectural backbone of the first monitoring networks. This optimization included solving the initial SPAN/monitor port contention problem, allowing customers to take a feed of network traffic from a tap and pass it to any number of egress ports, where the monitoring tools reside. NPBs also offered the ability to perform not just replication, but aggregation and load balancing as well. With filtered traffic coming from the network, NPBs were able to serve monitoring tools exactly what they needed to see.

This was the era of the Packet Broker 1.0 Architecture. There were challenges, however, as each vendor had its own equipment, and interoperability between different vendors was difficult. Once a customer had selected a vendor, they were often locked in to large expensive systems, and migrating to a new vendor was complicated and costly. In addition, the platforms and families of products, even within a single vendor, were rigid; line cards from one line might not fit in another; modules from one generation of switches might not fit in the next.

Scaling these solutions was difficult from an architecture perspective, where interlocking different sizes of equipment was technically and/or financially prohibitive. Customers often had to wait for new features to arrive. This rigidity led to some networks being built around the deficiencies of the monitoring equipment being deployed, rather than the requirements of the monitoring network itself.

Disaggregation and the Packet Broker 2.0 Architecture

As monitoring networks continued to grow and adapt to shifting trends, the architecture itself needed to change. A range of sizes for monitoring switches was called for; a variety of physical interfaces, as well as the number of physical interfaces per switch was needed. Smaller systems functioning as part of the entire solution but delivering cost-effective functionality were required. Monitoring networks aren't simply measured in their capital expenditures, but in operational costs involved as well, driving the need not only for a cost-effective solution, but a software-driven one. No longer can the monitoring network wait for new features and functionality; nor can these networks tolerate extensive maintenance windows in which to deploy new equipment.

Adding scale or functionality must be part of the architecture itself. This is something that disaggregation enables by virtue of delivering smaller, cost-effective platforms that, when system enhancements are needed, allows adding additional switches that become part of the larger monitoring solution seamlessly. This is the core of what a disaggregated architecture delivers. The monitoring network is free to scale on demand, when and where demand increases, without compromising performance or budgets.

Introducing the nGenius 5000 Series Packet Flow Switch

The nGenius® 5000 series packet flow switch is comprised of two solutions that leverage OCP switch hardware to deliver cost-effective, software-driven solutions that scale on demand with the monitoring network. With a range of physical interfaces up to 100 Gigabit, the nGenius 5000 series packet flow switch delivers flexibility in a compact OCP form factor.

Software-driven by the Packet Flow Operating System (PFOS)

Built from the ground up, the Packet Flow Operating System™, or PFOS, has packet broker in its DNA. PFOS is the lifeblood of the NETSCOUT® PFS portfolio, and even supports the portfolio's most powerful switch, the nGenius 6010 packet flow switch. Tried and tested with the largest service providers across the globe, PFOS is the apropos solution for powering OCP switches. Together, these two pieces form the cornerstone of the Packet Broker 2.0 architecture.

PFOS adapts and delivers functionality according to the platform. For example, with the nGenius 5000 series packet flow switch, PFOS supplies core packet broker functionality, but when combined with the nGenius 6010 packet flow switch blade-and-chassis model, PFOS adapts to the advanced hardware that the nGenius 6010 packet flow switch supports, delivering additional

LEVERAGING OPEN COMPUTE PLATFORMS

In 2011, the Open Compute Project (OCP) was formed to "redesign hardware technology to efficiently support the growing demands on compute infrastructure." For the monitoring network, this mantra meant that it could leverage the power of OCP platforms, alleviating the need for vendor-specific systems, and deliver monitoring solutions that are software-driven, atop open compute platforms/switches.

Today, these OCP switches are level setting the monitoring network in terms of hardware, allowing NETSCOUT to focus on software-driven PFS features, offering a solution that is cost-effective and software-driven. But what about scalability as the network grows? A purpose-built operating system is needed to deliver the ability to run on one or dozens of switches simultaneously, operating as a single harmonious ecosystem. This is where NETSCOUT nGenius 5000 series packet flow switches deliver on the Packet Broker 2.0 Architecture.

advanced or expert functionality. The same operating system powers both platforms, and it's here that PFOS delivers on the software-driven needs of the Packet Broker 2.0 Architecture, by providing the right-sized features for the platform with a common interface, making migration from one platform to the other, or integration of the two platforms, an operational simplicity.

Scale on demand with pfsMesh

Leveraging PFOS as a common element between any nGenius 5000 series packet flow switch or nGenius 6000 series packet flow switch, customers can easily scale when and where it is needed, with the PFOS pStack feature. Through pStack, multiple switches can be interconnected in a dynamic and self-healing mesh. The result of this interconnection is called a pfsMesh. pfsMesh allows any tap connected to any packet broker or PFS switch in the system, to connect to any monitoring tool on any other packet broker or PFS switch also in the system. Should a link in the mesh go down, the system compensates for this automatically, and when the link is restored, the system responds again automatically, without requiring an operator or administrator to login and manually intercede.

Adding additional nGenius 5000 series packet flow switch switches to the monitoring network is easy to do. When the scale or performance of one nGenius 5000 series packet flow switch switch isn't enough, add another, and decide if pfsMesh is required. You can also interconnect an nGenius 5000 series packet flow switch device to the nGenius 6000 series packet flow switch switch when more advanced capabilities or conditioning is needed.

Some monitoring deployments see the nGenius 5100 packet flow switch as the spine of the monitoring network and the nGenius 5010 packet flow switch as its leaves. Whatever the requirement, the PFS portfolio contains the solutions needed to enable the monitoring network to be architected in a cost-effective manner, allowing for scale later and powerful features via PFOS today.

Unify security and service assurance visibility

Today, IT and security teams often use disparate products to achieve security and service assurance visibility, which results in high capital expenditures and silos of visibility. NETSCOUT addresses these challenges by providing network professionals with a common, unified packet acquisition plane that is both software-driven and cost-effective. Adding active security capabilities enables organizations to effectively manage their security risks in both passive and active modes with a unified architecture. With support for 100Gbps inline security, nGenius enables even the most data-intensive inline security applications.

nGenius 5000 series packet flow switches with inline tool chaining allow aggregation, filtering, and load-balancing of network traffic toward multiple inline security applications while maintaining only a single intrusion into each network link. They provide application-specific health checks (not just heartbeats) to ensure the active security tools are connected and functioning properly. External bypass TAPs can be used to ensure that the security policies are adhered to during power failure.

The NETSCOUT packet broker software, Packet Flow Operating System (PFOS), supports both service assurance and security capabilities, unifying data sources across a common infrastructure and delivering smart wire data to IT teams. The nGenius switches are an integral part of the NETSCOUT service and security assurance platform, which offers unique advantages, such as the ability to monitor the health of a visibility fabric from the nGeniusONE® console. This further streamlines IT operations by providing an integrated view of the entire monitoring infrastructure, so the data needed for full visibility can be available to network and security teams.

Figure 1: nGenius 5010 Packet Flow Switch.

Figure 2: nGenius 5100 Packet Flow Switch.

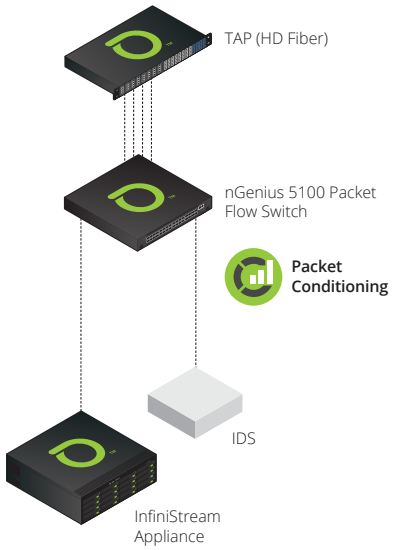

Figure 3: nGenius 5000 devices in the Enterprise creates a network that can move the traffic of interest to tools connected to the Packet Flow System.

The nGenius 5010 Series Packet Flow Switch

For deployments that require 10G port density, the nGenius 5010 packet flow switch is the solution to consider. Leveraging PFOS for on demand scalability, this switch provides up to 72 10G ports in a 1RU form factor. Leveraging OCP hardware, the nGenius 5010 packet flow switch comes in both AC and DC powered versions, and contains hardware redundancy with 4:1 redundant fans along with redundant power supplies.

The nGenius 5100 Series Packet Flow Switch

For deployments that require 40 or 100G port density, the nGenius 5100 packet flow switch is the solution to consider. Like the nGenius 5010 packet flow switch, the nGenius 5100 packet flow switch leverages PFOS for on demand scalability, and provides up to 32 100G QSFP28 ports in a 1RU form factor. Utilizing OCP hardware, the nGenius 5100 packet flow switch comes in both AC and DC powered versions, and contains hardware redundancy with 5:1 redundant fans along with redundant power supplies.

Both the nGenius 5010 and 5100 packet flow switches include, as part of PFOS, an intuitive, graphical user interface (GUI) out of the box, and CLI for local configuration and management.

Use Cases

Wondering which situations and scenarios are best suited for the nGenius 5000 series packet flow switch? The following use cases are examples of where the power and flexibility of the nGenius 5000 series packet flow switch is suited for monitoring deployment.

Base packet broker functionality in dense 10/100G deployments: The Standalone or Remote Site Use Case

In this scenario, the deployment requires dense 10G, 40G, or 100G interfaces, with the need for a basic set of packet broker features and functionality. These features include filtering, load balancing, aggregation, and replication. No advanced features, like deduplication or masking of information, is required. Here, the nGenius 5000 series packet flow switch is perfectly suited; each switch can be deployed and stand alone, as a single unit or be combined together into a larger ecosystem, powered by pfsMesh, to deliver any packet to any tool, anywhere in the mesh.

An example of this type of deployment can be one, or several, nGenius 5010 packet flow switches connect to an nGenius 5100 packet flow switch, as a spine. In this case, multiple 10G tap interfaces feeding into the nGenius 5010 switch for filtering and aggregation, connect to the nGenius 5100 packet flow switch with a 40G interface, and from there, traffic is fed to one or more monitoring tools.

This deployment could be within the data center, or with nGenius 5010 packet flow switches deployed at small or remote sites, feeding back into an nGenius 5100 packet flow switch at a core data center, with or without pfsMesh interconnects.

For virtualized network segments, traffic can be mirrored and forwarded from the virtual network to the physical network using tunneling protocols such as ERSPAN. The nGenius 5000 series packet flow switch devices can be the destination of these tunnels and terminate them.

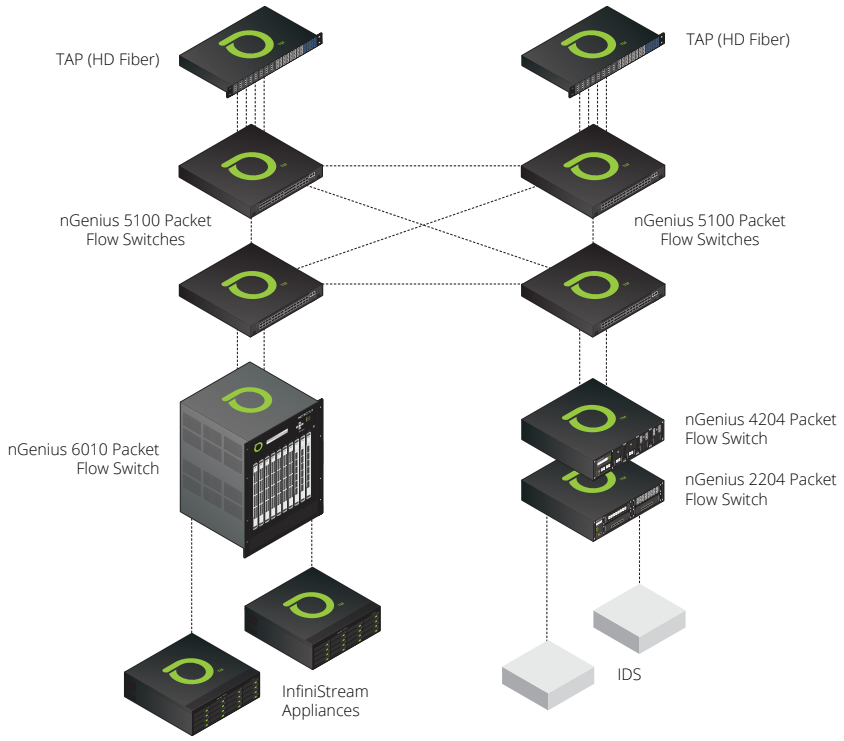

Figure 4: Aggregation Use Case, with nGenius 5000 Series Packet Flow Switch and nGenius 6010 Packet Flow Switch or nGenius 3900 Series Packet Flow Switch.

Leveraging cost-effective nGenius 5000 series ports everywhere and aggregating into an nGenius 6010 or 3900 switch: The Aggregation Use Case

In this scenario, a network typically has a higher number of NPB port requirements, usually calling for two or more nGenius 5000 packet flow switches. However, in this use case, some number of NPB ports require advanced NPB functionality. Here, it might be suitable to leverage the nGenius 5000 series packet flow switch ports in the parts of the monitoring network that require base NPB functionality, and aggregate back into another PFS switch; for example, the nGenius 6010 packet flow switch or nGenius 3900 series packet flow switch. Deploying this way allows the monitoring network to scale on demand, adding base NPB ports where needed, and advanced NPB ports in other places, utilizing the nGenius 5000 series packet flow switch to aggregate into a pre-existing or additional PFS switch.

With this aggregation model, pfsMesh is available through PFOS, and can be easily enabled and deployed where required. Leveraging pfsMesh allows for total visibility across the monitoring network, eliminating silos of visibility in various spots, and delivering a totally unified packet plane.

nGenius 5000 series for active (inline) security deployments: The Inline Security Use Case

In this example, IPS and WAF systems need production traffic for inspection and protection. Use nGenius 5010 series switch to aggregate network traffic from multiple network segments. The switch selectively forwards and load balances traffic across multiple instances of IPS and WAF. It also conducts health checks on all instances of the IPS and WAF applications. The end result is pervasive security visibility across the network and efficient use of IPS and WAF applications.

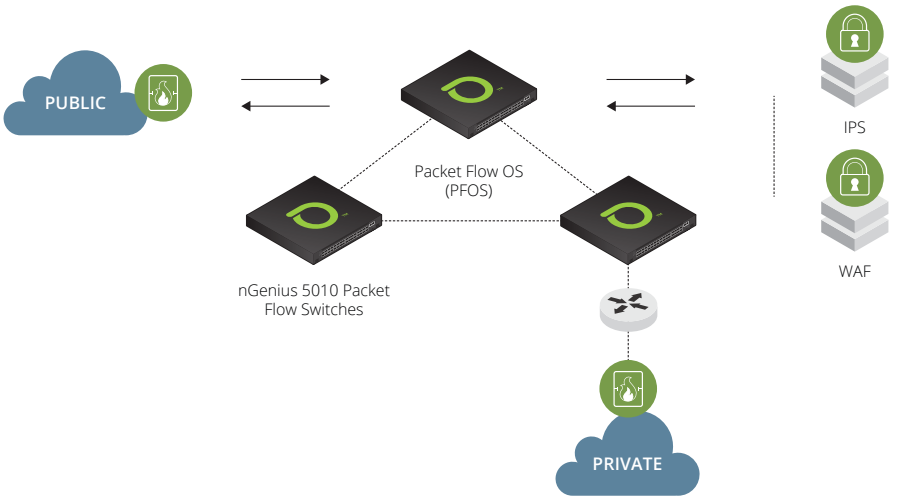

Figure 5: Inline Security Use Case, with nGenius 5000 Series Packet Flow Switches in a Mesh Configuration.

Summary

The monitoring solution landscape is experiencing a transformation, led by NETSCOUT, from the Packet Broker 1.0 Architecture, with rigid, vendor-specific, expensive systems, to the Packet Broker 2.0 architecture, which delivers on three powerful tenants:

- Be software-driven
- Be scalable on demand
- Be cost-effective

With this disaggregated approach, the Packet Broker 2.0 architecture revolves around software-driven features and functionality. Powered by PFOS, customers can easily scale on demand when and where needed, and deploy pfsMesh to dynamically interconnect and scale. Finally, utilizing industry standard OCP switches delivers cost-effective NPB functionality across the monitoring network.

The nGenius 5000 series packet flow switch is core to the Packet Broker 2.0 Architecture, with an OCP switch at the center of its hardware technology, using software-driven purpose-built PFOS, and capable of scaling on demand with pfsMesh, it enables any tap to feed any tool anywhere on the mesh.

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_006-1801 02/2018