nGenius 4200/2200 Series Packet Flow Switch

Service providers, private clouds, government organizations, and enterprises must contend with the collection, processing, and aggregation of traffic from a number of network segments. They also need to address space and power constraints in the data center, while managing the migration from 10 Gbps to 40 Gbps networks infrastructure.

Network professionals today face increasing network speeds and the pressure to optimize the cost of security and operational tools – challenges especially acute in fast changing environments.

High-density, flexible, modular, and powerful visibility systems are critical to enabling cost effective, large-scale network and security monitoring and can dramatically improve tool throughput and packet processing capacity.

The Solution

NETSCOUT® helps you maximize the insight and capabilities of your network intelligence infrastructure. Using nGenius® packet flow switches, you can make better use of your performance monitoring and security tools, simplify operational complexity and realize additional cost savings and service quality improvements.

The nGenius 4200 and 2200 series packet flow switches (also known as PFS 4204 and PFS 2204) improve network visibility for monitoring and security tools, accelerate the time to diagnose performance problems, and improve your ability to detect and respond to security incidents. This also eases the strain on capex and opex budgets as network size, complexity, and speeds grow.

The nGenius 4200 and 2200 series packet flow switches support a self-organizing mesh architecture (vMesh) giving you the flexibility and modularity to deploy just the appliances you need. vMesh enables the ability to scale link-layer visibility and data access to a system-level architecture; participating devices and hundreds of ports are now part of a single logical system.

Tool chaining delivers advanced active inline packet flow switching for 10 GigE and 40 GigE networks, while optimizing the effectiveness of security tools.

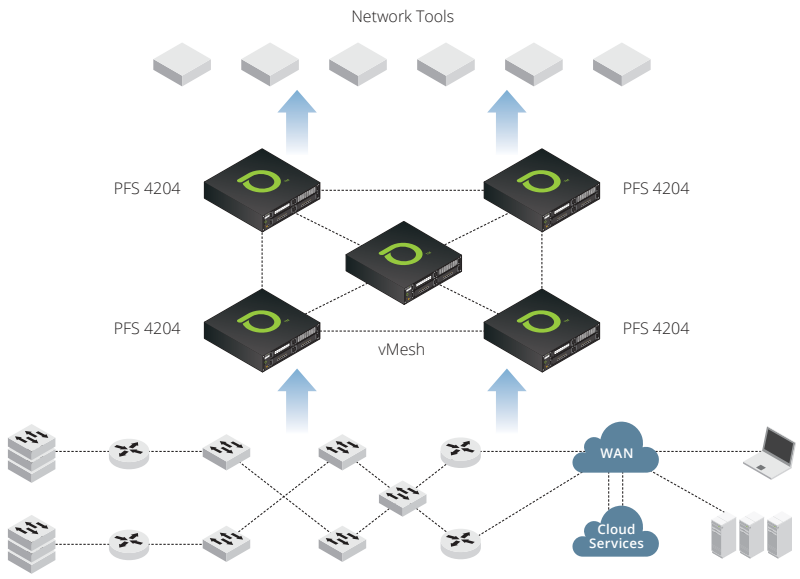

Figure 1: Packet flow switches create a unified visibility plane.

Modular Chassis

- 2 Rackmount Units
- Up to 4 chassis modules
- Up to 64 or 24 ports:
  - 64 or 24 1GigE
  - 64 or 24 10GigE
  - 16 40GigE
- Up to 640 or 240 Gbps throughput
- Line rate speed conversion; aggregation; replication; filtering; load balancing; port tagging; time stamping; deduplication; protocol stripping & de-encapsulation; conditional masking & slicing; encapsulated filtering & balancing
- Active inline and passive traffic forwarding with programmable fail-safety
- IP tunnel termination
- Self-healing, intelligent, self-organizing mesh technology
- Secure and reliable WAN tunneling
- Hot-swappable power supplies and fan trays
- Central management
- NEBS III compliant

Product Description

nGenius 4204 and 2204 packet flow switches are 2RU models that bridge the gap between 1 GigE, 10 GigE, and 40 GigE networks, providing network intelligence on a large scale. nGenius 4204 and 2204 packet flow switches offer a range of chassis modules that support different features, port densities, and port speeds up to a maximum line-rate throughput of 640 Gbps. All ports are enabled by default and are fully I/O configurable. Any port can be designated as an input port or an output port, or as an intermediate or a stacking port. Chassis modules are available with either SFP+ or QSFP+ ports, or with fixed media ports for active inline tapping or bypass. Active inline chassis modules provide the active bypass or tapping capability using the PowerSafe technology with configurable fail-safe operation to ensure continuous traffic availability or blocking.

nGenius PFS can be locally managed via a serial console and remotely managed via HTTP, HTTPS, SSH, Telnet, and SNMP v1-v3.

Hardware-based, user-independent filtering allows traffic to be distinguished according to source and destination MAC/IP address as well as by specific protocols, such as HTTP, VoIP, and others. A customizable (user-defined) filter offers more granular selections, specifically within the payload of a packet. Filters can be ingress, egress, and overlapping depending on use of port classes.

Session-based, flow-aware load balancing provides user control of traffic distribution to monitoring tools, increasing output capacity while maintaining session integrity. For example, a 40 GigE network can be captured and automatically balanced across multiple gigabit or 10 GigE monitoring tools based on user-defined session criteria. The load balancing can operate in tandem with hardware-based filtering or independently.

The inline security capabilities and unified packet visibility from NETSCOUT allow organizations to accelerate advances in cyber security posture, capabilities and responses. The nGenius packet flow switches provide network visibility for multiple active inline and out-of-band security systems tool-chained together, creating a pervasive defense architecture against a broad range of attacks. This includes active inline bidirectional traffic forwarding and health checks. Integrated fiber bypass provides the fail-safe capability to ensure no interruption to the inline traffic availability. Should any inline security applications fail, they can be bypassed or traffic can be sent to another system, in the event of power loss.

Advanced chassis modules have additional hardware resources for a suite of features including time and port stamping, protocol stripping/de-encapsulation (FabricPath, GRE, GTP, MAC-in-MAC, MPLS, NVGRE, TRILL, VLAN, VN-tag, VXLAN), deduplication, conditional packet masking and slicing, and real-time microburst measurement. Traffic forwarding is also extended to filtering and load-balancing on inner layer 3 and 4 packet headers inside encapsulation headers (e.g. GTP, MPLS).

nGenius PFS supports the vMesh intelligent stacking through the use of the vStack+® protocol, which enables traffic capture devices to be deployed in a redundant, low-latency mesh for total, dynamic, fault-tolerant visibility. A vMesh system can include a mix of nGenius 4204 and 2204 packet flow switch appliances, and can be tunneled securely and reliably over WAN connections.

nGenius 4204 packet flow switch provides automated event-driven monitor output traffic direction and responses (Syslog messages, SNMP traps, light front LED, deactivate ports) with seven user-definable trigger event types.

Redundant power supplies allow seamless transitions between power systems and ensure uptime. nGenius 4204 and 2204 packet flow switch appliances are NEBS compliant with hot-swappable power supplies, fans, and air filters.

The nGenius packet flow switches support field software updates for additional features and performance enhancements, and also support updating of FPGA firmware in the field.

The nGenius packet flow switches deliver maximum performance, scale and flexibility in both distributed environments and hyper-scale data centers. Carriers, private clouds, and large enterprises now have solutions that can match and grow with their network densities and performance needs.

Benefits

- Gain link-layer visibility and data access across entire network
- Centralize tools while increasing their reach
- Flexibly forward traffic to passive and active inline tools
- Boost monitoring and security tool efficiency
- Reduce both capex and opex through longer tool lifecycles
- Support network upgrades by load balancing existing tools
- Quickly provision new tools by eliminating SPAN port contention
- Centrally, remotely, and/or locally manage network visibility and access
- Higher port density with flexibility in speed and media

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

PFSQL_009-1801 02/2018