nGenius 5110 Packet Flow Switch

Software-Driven and Cost-Effective Performance

**Product Description**

The nGenius® 5110 Packet Flow Switch (PFS) is a dense 10G/25G model and is a part of the nGenius 5000 series of Packet Flow Switches. The nGenius 5110 model is designed with dense 10GbE and 25GbE deployments in mind and bridges the gap between 1GbE, 10GbE, 25GbE, 40GbE, and 100GbE Ethernet networks and tools.

The nGenius 5110 Packet Flow Switch has built-in 48 x 1GbE /10GbE/25GbE SFP28 ports and 6 x 40GbE/100GbE QSFP28 ports which provide a maximum of up to 72 10GbE or 25GbE ports via breakout cables all in a 1RU, fixed-configuration form factor. All ports are enabled by default, with each port configurable as an input port, intermediate (service) port, or output port. With the NETSCOUT pfsMesh, a self-organizing architecture, the nGenius 5110 Packet Flow Switch can be deployed in a redundant, low-latency meshed architecture for dynamic and fault-tolerant visibility that can scale to over 4000* ports across LAN and WAN environments.

**Cost-effective Feature Set**

Providing a lot of interfaces into a compact form factor, the nGenius 5110 Packet Flow Switch supports core network packet broker features which includes filtering, load balancing, replication, and aggregation. With an expansive feature set, the nGenius 5110 Packet Flow Switch is, like other devices in the PFS portfolio, capable of working and managing a monitoring network independently. Connect the HD Fiber TAPs and any number of tools, including the NETSCOUT's Service Assurance and Security Assurance products, to the nGenius 5110 Packet Flow Switch and easily manage a diverse and complex monitoring network. With NVGRE tunnel origination monitored packets can be forwarded across routed networks or to virtual monitoring applications.

Flow-aware load balancing enables intelligent control of traffic distribution to the monitoring tools, increasing output capacity while maintaining session integrity. For example, a 100GbE TAP from the network can be captured and automatically balanced across multiple 10GbE, 25GbE or 40GbE monitoring tool ports based on user-defined session criteria. Flow-aware load balancing can operate in tandem with hardware-based filtering or independently.

---

1 1GbE fiber (IEEE Clause 37) auto-negotiation is not supported so use of 1GbE fiber should be limited to use with TAPs. 1GbE copper does not have this restriction.

2 Total number of ports in a single pfsMesh is dependent on quantity and complexity of filtering.

### nGenius 5110 Packet Flow Switch Port Maximums

<table>
<thead>
<tr>
<th>Option</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GbE Options</td>
<td>48 x 1/10/25GbE SFP28 Ports</td>
</tr>
<tr>
<td>10GbE Options</td>
<td>48 x 1/10/25GbE SFP28 Ports (expandable to 72 x 10GbE Ports total)</td>
</tr>
<tr>
<td>25GbE Options</td>
<td>48 x 1/10/25GbE SFP28 Ports (expandable to 72 x 25GbE Ports total)</td>
</tr>
<tr>
<td>40GbE Options</td>
<td>6 x 40/100GbE QSFP28 Ports</td>
</tr>
<tr>
<td>100GbE Options</td>
<td>6 x 40/100GbE QSFP28 Ports</td>
</tr>
</tbody>
</table>
Security Optimization

To take action as offenders and bad actors are detected active inline security tools need to see and handle all the traffic that needs to be inspected. nGenius Packet Flow Switches with inline tool chaining allow aggregation, filtering, and load-balancing of actual network traffic toward multiple inline security applications whilst adding only a single device to each network link while providing application-specific health checks (not just ICMP 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. Triggers allow automated event-driven behavior (such as redirecting traffic, deactivating ports, or sending notifications via syslog or SNMP) to enable highly available (HA) inline security configurations.

Management

The nGenius 5110 Packet Flow Switch can be managed via a Web UI, CLI, and NETCONF XML API using HTTP, HTTPS, or SSH. The system can be monitored via Syslog and SNMP. Each device ships with an intuitive and easy to use graphical element management system (EMS) out of the box. Simply point a web browser at the nGenius 5110 Packet Flow Switch to manage and let the web-based user interface (WebUI) power the packet flow system. Management IP addresses can be manually assigned or obtained via DHCP.

Virtual Access

For accessing traffic that is completely virtualized and never makes it onto a physical network, traffic can be mirrored and forwarded from the virtual network to the physical network using tunneling protocols such as NVGRE (L2GRE) or ERSPAN which encapsulate the traffic of interest. The nGenius 5110 Packet Flow Switch can terminate these tunnels so the traffic can be forwarded on to monitoring applications. Conversely, the nGenius 5010 packet flow switch can also be used to forward packets from physical TAPs to virtual monitoring applications such as NETSCOUT’s vSTREAM.

Power and Cooling

The nGenius 5110 Packet Flow Switch supports two redundant, hot-swappable power supplies and five redundant, hot-swappable fan modules (in a 4+1 configuration) supplying ample cooling in a front to back air flow configuration.

Features and Benefits

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Up to 72 ports in a 1 RU, Fixed Configuration</strong>&lt;br&gt;• 48 x 1GbE&lt;br&gt;• 48 x 10 or 25GbE, up to 72 x 10 or 25GbE via breakout&lt;br&gt;• 6 x 40 or 100GbE&lt;br&gt;• Mix of 1, 10, 25, 40, and 100GbE ports per PFS&lt;br&gt;Compatible with SFP, SFP+, SFP28, QSFP+, and QSFP28 MSA-compliant transceivers – for complete details, please refer to the list of transceivers offered by NETSCOUT</td>
<td><strong>High Density System:</strong>&lt;br&gt;• Drives cost-effectiveness by reducing per-port cost and increases flexibility&lt;br&gt;• Condenses the nGenius PFS footprint (rack space) into the most compact 1RU in a fixed configuration&lt;br&gt;• Reduces power consumption&lt;br&gt;• Software-driven, simplifies management</td>
</tr>
<tr>
<td><strong>I/O Configurable</strong>&lt;br&gt;• Full flexibility in selecting ports for network access, intermediate service, interconnect, or monitor output&lt;br&gt;• Dual network access &amp; monitor output port class&lt;br&gt;• IP tunnel (e.g. NVGRE, ERSPAN) termination</td>
<td>Enables agile response to monitoring infrastructure changes&lt;br&gt;Facilitates effectively doubled capacity for input and output&lt;br&gt;Allows virtualized traffic to be forwarded over an IP network to PFS ingress ports, and then forwarded onto monitoring devices as is, and then forwarded onto monitoring devices as is, or de-encapsulated^3</td>
</tr>
<tr>
<td><strong>Selective Aggregation</strong>&lt;br&gt;• Fully flexible any-to-any port mapping</td>
<td>Enables large scale aggregation to maximize tool visibility&lt;br&gt;Addresses asymmetrical routing issues</td>
</tr>
<tr>
<td><strong>Flexible and Powerful Filtering</strong>&lt;br&gt;• OSI Layers 2 - 7&lt;br&gt;• Ingress&lt;br&gt;• Overlapping</td>
<td>Allows only traffic of interest to be forwarded to each tool, increasing tool efficiency and reduces the number of required tool interfaces</td>
</tr>
</tbody>
</table>

^3 Requires connection to a PFX or advanced PFS.
<table>
<thead>
<tr>
<th><strong>Features</strong></th>
<th><strong>Benefits</strong></th>
</tr>
</thead>
</table>
| **Session-based/flow-aware Load Balancing**  
• Distributes traffic load across multiple instances of a tool or tool port  
• Maintains session stickiness for full conversations | • Prevents oversubscription of monitoring tools and security systems – eliminating blind spots without sacrificing session integrity  
• Copied traffic can be easily distributed across multiple lower speed tool ports, allowing users to preserve existing tool investments |
| **Monitor Traffic Port Tagging**  
• Provides identification of traffic based on source network/link using VLAN tagging | • Users can quickly and precisely pinpoint where an issue, such as latency or security event, is occurring in the network  
• Allows different tools to access port identification |
| **Intelligent Stacking (pStack)**  
• Enables pfsMesh architecture for local and remote of up to 256 Total PFS devices as a single redundant system | • Ensures highly available monitoring  
• Scales visibility with network infrastructure and new tools  
• Ensures delivery of traffic across LAN or WAN to tools |
| **GRE tunnel initiation and termination**  
• Send monitored packets over routed networks | • Forward packets from remote offices to centralized tools  
• Forward packets from physical TAPs to virtual tools |
| **Line-rate header stripping**  
• VLAN  
• VXLAN  
• VN-tag  
• MPLS | • Preserve tool resources (bandwidth and processing) by eliminating unnecessary headers  
• Re-use legacy tools that may not understand newer protocol headers  
• Enable native filtering and load balancing on inner packet fields |
| **Policy-based event triggering and actions**  
• Dynamic traffic redirection based on occurrence of events  
• Send alerts when specific events occur | • Reduces management overhead and enables faster response times to incidents |
| **Active Inline Access and Forwarding**  
• Aggregation of multiple network segments  
• Filtering and load balancing towards applications/tools  
• Easy to configure simple and complex inline tool chaining  
• Customizable health check packets for “positive” (return) and “negative” (no return) checks | • Removes multiple points of failure  
• Gains visibility for a single inline security tool (e.g. security proxy, IPS) and/or WAN optimization  
• Easy deployment of layered security  
• Removes multiple points of failure by fully exercising tools |
| **Local and Remote Management**  
• NETCONF XML API  
• CLI (SSH)  
• GUI (HTTP/HTTPS)  
• SNMP (v1, v2, v3)  
• Syslog | • Easy to use via graphical interfaces or via CLI  
• Easy integration with applications using CLI or NETCONF XML API  
• Alerts can be received by any Syslog server or SNMP manager, with option for sending securely |
| **Role-based Access**  
• Multiple user and user role support  
• Flexible user/role defined privileges, unique screen views, and access control | • Conforms to security policy needs of IT organizations |
| **AAA Security with Remote (RADIUS and/or TACACS+)** | • Meets authentication policy needs of IT organizations and Local authentication |
| **Redundant Power Supplies**  
• AC and DC hot-swappable options | • Maintains high availability for the device |
| **Traffic Statistics**  
• Port-level packet and throughput metrics, including overflow drops, bad packets, etc.  
• Flow level packet and throughput metrics | • Visibility into network and tool port activity  
• Visibility into traffic type activity |

* Total number of Packet Flow Switches in a single pfsMesh is dependent on device sizes, number of ports, and complexity of filtering.
### Standards and Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Specification(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>IEEE 802.3, IEEE 802.3by, IEEE 802.3ae, IEEE 802.ba</td>
</tr>
<tr>
<td>VLAN ARP</td>
<td>IEEE 802.1Q, IEEE 802.1ad, IETF RFC 826</td>
</tr>
<tr>
<td>IP</td>
<td>IETF RFC 791, 2460</td>
</tr>
<tr>
<td>UDP</td>
<td>IETF RFC 768, IETF RFC 793</td>
</tr>
<tr>
<td>TCP</td>
<td>IETF RFC 768, IETF RFC 793</td>
</tr>
<tr>
<td>FTP</td>
<td>IETF RFC 959, 2228</td>
</tr>
<tr>
<td>SSH</td>
<td>IETF RFC 4251, 4252, 4253</td>
</tr>
<tr>
<td>HTTP</td>
<td>IETF RFC 2616, 2817, IETF RFC 4492, 5246</td>
</tr>
<tr>
<td>TLS (SSL)</td>
<td>IETF RFC 1157, 3411-3418</td>
</tr>
<tr>
<td>SNMP</td>
<td>IETF RFC 5424, 5425</td>
</tr>
<tr>
<td>Syslog</td>
<td>IETF RFC 2865, 2866</td>
</tr>
<tr>
<td>RADIUS</td>
<td>IETF RFC 1492, 1493</td>
</tr>
<tr>
<td>TACACS+</td>
<td>IETF RFC 1492</td>
</tr>
<tr>
<td>NTP</td>
<td>IETF RFC 1492</td>
</tr>
<tr>
<td>EMC</td>
<td>FCC Part 15 Subpart B/ICES-003 Class A, EN 55032 Class A, VCCI Class A, AS/NZS CISPR 32 Class A, EN 61000, EN 300 386 Class A, CNS 13138 Class A, KCC Class A</td>
</tr>
</tbody>
</table>

### Ordering Information

<table>
<thead>
<tr>
<th>Part Numbers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>51FCNAQK000</td>
<td>5110 Switch with 48 x 1/10/25Gb SFP28 and 6 x 40/100Gb QSFP28 or 72 x 10/25Gb Ports, AC Power</td>
</tr>
<tr>
<td>51FCNDQK000</td>
<td>5110 Switch with 48 x 1/10/25Gb SFP28 and 6 x 40/100Gb QSFP28 or 72 x 10/25Gb Ports, DC Power</td>
</tr>
</tbody>
</table>

For transceivers, please refer to the list of transceivers offered by NETSCOUT.
SPECIFICATIONS

Packet Capture Ports
48 x 1GbE
48 x 10 or 25GbE, up to 72 x 10 or 25GbE via breakout
6 x 40 or 100GbE
Mix of 1, 10, 25, 40, and 100GbE ports per PFS

Data Rates
1Gbps, 10Gbps, 25Gbps, 40Gbps, 100Gbps

Interface Types
Ethernet: 1000 Base-T, 1000 Base-SX, 1000 Base-LX, 10GBase-T,
10GBase-LR, 10GBase-SR, 25GBase-LR, 25GBase-SR, 40GBase-SR4,
40GBase-LR4, Cisco 40GBase-SR2 BiDi, 100GBase-LR4,
100GBase-SR4

Rack Unit
1 Rack Unit (1 RU)

Dimensions
1.73 in (44 mm) Height
17.3 in (438 mm) Width
18.6 in (473 mm) Depth

Weight
20.78 lbs. (9.43 kg) with 2 Power Supply Units (PSUs) installed

Power (AC)
583W (1989 BTU/hr) max
front to back airflow
AC: 90 to 240VAC/50-60Hz
DC: -36 to -72VDC

Operating Temperature
32° to 113°F (0° to 45°C)

Storage Temperature
-40° to 158°F (-40° to 70°C)

Operating Humidity
5% - 95% (non-condensing)