DELL Technologies

NETSCOUT Packet Flow Operating System for Dell EMC PowerSwitch Hardware

Expand Your Visibility Fabric with Advanced Packet Broker Functionality

SOLUTION OVERVIEW

The combination of NETSCOUT's nGenius® 7000-series Packet Flow Operating System (PFOS) with Dell EMC PowerSwitch hardware configurations is designed to bridge the gaps between 1GbE, 10GbE, 25GbE, 40GbE, and 100GbE networks and tools.

Available out-of-the-box configurations offer SFP+, SFP28, QSFP+, and QSFP28 ports in various 1RU and 2RU fixed configuration form factors. All ports are enabled by default, with each port configurable as an input port, intermediate (service) port, or output port. With a self-organizing architecture, the NETSCOUT-enabled PFOS software on Dell EMC PowerSwitch hardware can be deployed in a redundant, low-latency meshed configuration for dynamic and fault-tolerant visibility that can scale to over 4000[1] ports across LAN and WAN environments.

COST-EFFECTIVE FEATURE SET

Providing multiple interfaces within a compact form factor, the NETSCOUT PFOS Solution on Dell EMC PowerSwitch hardware supports core network packet broker features including filtering, load balancing, replication, and aggregation. With an expansive feature set, PFOS-enabled Dell EMC PowerSwitch switches can manage a monitoring network independently. Connect the HD Fiber TAPs and any number of tools, including NETSCOUT's Service Assurance and Security Assurance products, to a Dell EMC PowerSwitch embedded with PFOS software 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, packets from a 40GbE TAP can be captured and automatically load-balanced across multiple 1GbE or 10GbE monitoring tool ports based on user-defined session criteria. The PFOS software can load balance among tools of different processing capacity (e.g., 10GbE tools and 40GbE tools) by assigning weights to each tool port to achieve weighted load balancing. Load balancing across multiple L2GRE or VxLAN tunnels allows traffic to be spread among several remote or virtual destinations. Flow-aware load balancing can operate in tandem with hardware-based filtering or independently.

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 is to be inspected.

NETSCOUT

THE NETSCOUT / DELL TECHNOLOGIES PARTNERSHIP

NETSCOUT provides organizations with Commercial Off the Shelf (COTS) deployment options for both the InfiniStreamNG and Packet Flow Switch solutions. As part of the current portfolio, NETSCOUT PFOS software is available for purchase and use on Dell EMC PowerSwitch hardware configurations.

Dell Technologies' OEM Engineered Solutions program enables streamlined purchase and deployment of turnkey solution configurations in collaboration with leading technology partners.

Program benefits include the following:

- Accelerated and cost-effective deployment
- Certified hardware from Dell Technologies
- Fully integrated solutions
- Turnkey purchase-to-deployment process
- NETSCOUT MasterCare support coverage

NETSCOUT PFOS solutions on Dell EMC PowerSwitch hardware with inline tool chaining allow aggregation, filtering, and load-balancing of production network traffic toward multiple inline security applications whilst adding only a single device to each network link. Application-specific health checks (not just ICMP heartbeats) 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 NETSCOUT solution on Dell EMC PowerSwitch hardware can be managed via a Web UI, CLI, and NETCONF XML API using HTTP, HTTPS, or SSH and the system can be monitored via Syslog and SNMP. Each device ships with an intuitive and easy-to-use graphical element management system (EMS). Simply point a web browser at the PFOS enabled PowerSwitch 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. NETSCOUT PFOS can terminate these tunnels so the traffic can then be forwarded on to monitoring applications. Conversely, the PFOS-enabled solutions can also be used to forward packets from physical TAPs to virtual monitoring applications such as NETSCOUT's vSTREAM.

FEATURES AND BENEFITS

Features	Benefits
32 to 64 ports in 1RU or 2RU, Fixed Configurations • Compatible with SFP, SFP+, SFP28, QSFP+, and QSFP28 MSA compliant transceivers	• Drives cost-effectiveness by reducing per-port cost and increasing flexibility • Condenses the solution footprint (rack space) into compact 1RU or 2RU of space in a fixed configuration • Reduces power consumption • Software-driven, simplifies management
Configurable I/O • Full flexibility in selecting ports for network access, intermediate service, interconnect, or monitor output • Dual network access & monitor output port class • IP tunnel (e.g. NVGRE, ERSPAN) termination	• Enables agile response to monitoring infrastructure changes • Facilitates effectively doubled capacity for input and output • Allows virtualized traffic to be forwarded over an IP network to solution ingress ports, and then forwarded onto monitoring devices as is or de-encapsulated[2]
Selective Aggregation • Fully flexible any-to-any port mapping	• Enables large scale aggregation to maximize tool visibility • Addresses asymmetrical routing issues
Flexible and Powerful Filtering • OSI Layers 2 - 7 • Ingress • Overlapping	• Allows only traffic of interest to be forwarded to each tool, increasing tool efficiency and reduces the number of required tool interfaces
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
Weighted Load Balancing • Distributes traffic among tools of different capacities	• Prevents oversubscription of monitoring tools and security systems • Preserves investment in existing tools while allowing growth with newer, higher-capacity tools

Features	Benefits
Tunnel Load Balancing • Distributes traffic among multiple instances of remote destinations or virtual tools	• Prevents oversubscription of virtual tools • Prevents oversubscription of routed back-haul networks
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
Packet Time Stamping (select PFOS-enabled models)	• Provides time-of-capture information for latency analysis
Intelligent Stacking (pStack) • Enables pfsMesh architecture for local and remote of up to 256[3] Total PFOS-embedded 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
L2GRE and VxLAN 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
Intelligent Stacking over IP (pStack over L2GRE or VxLAN) • Extend Monitoring fabric over routed networks	• Create a single monitoring fabric across sites • Simplify and unify monitoring across multiple sites
Line-rate header stripping • VLAN • VxLAN • VN-tag • MPLS • L2GRE	• 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
LLDP neighbor learning & LLDP transmission	• LLDP neighbor learning simplifies operations by allowing the operator to quickly determine what is connected to each PFOS-enabled device port – no more tracing cables • LLDP transmission, if enabled, tells neighboring devices about the PFOS-enabled device.
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 • Syslog (transport over UDP, TCP, or TLS)	• 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

Features	Benefits
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

AVAILABLE CONFIGURATIONS

EMBEDDED NETSCOUT Software	Dell Model Number	Configurations
PFOS 7031	S5248F-ON	48xSFP28 2xQSFP28-DD 4xQSFP28
PFOS 7031	S5232F-ON	32xQSFP28 2xSFP+
PFOS 7121	Z9264F-ON	64xQSPF28

1 Total number of ports in a single pfsMesh is dependent on quantity and complexity of filtering
2 De-encapsulation may require purchase of NETSCOUT's packet broker eXtender PFX
3 Total number of ports in a single pfsMesh is dependent on quantity and complexity of filtering

Learn more about Dell EMC PowerSwitch

Learn more about Dell OEM Solutions

Contact a Dell Technologies Expert

Follow Dell EMC Networking on Twitter

DELL Technologies