NETSCOUT nGenius 5000 Inline Security Solution

Market Impact Report

EXECUTIVE SUMMARY

Enterprise adoption of SaaS applications and migration of IT applications to the cloud have been accompanied by a dramatic increase in security threats, which are driving IT managers to deploy a new generation of inline security systems in the DMZ between untrusted public networks and trusted private networks. This has created another compelling packet broker use case that improves the performance, utilization, availability and manageability of these inline security systems. Savvy network managers are deploying packet brokers in the DMZ to direct packet flows through a central pool of inline security systems that are configured in application-specific service chains.

In 2017, NETSCOUT introduced the nGenius 5000 packet broker product line based on Open Compute Project (OCP) platforms, offering network operators a new generation of more cost-effective, software-driven, highly scalable packet brokers that use the same merchant silicon switching hardware deployed in massive hyperscale data centers. Recently, the company released a new version of its PFOS packet flow visibility software that supports inline security tool service chaining in the DMZ.

As a leading provider of comprehensive network visibility solutions unified in a common operational framework, NETSCOUT is also helping to break down the operational silos that exist in most large-scale IT organizations between network operations, security operations, IT operations and DevOps teams.

KEY FINDINGS

- OCP packet broker platforms are software-driven, cost-effective and easy to scale.
- Session-based, flow-aware load balancing of packet flows across multiple instances of active security systems.
- Active health checking of inline security systems, such as Intrusion Prevention System (IPS) and Web Application Firewall (WAF).
- Seamless integration with packet flow visibility for out-of-band passive monitoring tools.

Packet Brokers for Passive, Out-Of-Band Monitoring

In today's large-scale data centers, network and security operations teams are employing a diverse array of application performance monitoring (APM), network performance monitoring (NPM) and out-of-band security systems. This trend has driven the adoption of packet brokers, which are used to build overlay networks for tapping into the underlying production network and then distributing properly conditioned packets to various systems deployed in centralized tool farms. The benefits of using packet brokers for these passive, out-of-band monitoring use cases are well-established.

Active, Inline Security Systems in the DMZ

The growing adoption of SaaS applications and the migration of enterprise IT applications to hybrid clouds has been accompanied by a dramatic increase in the number of security threats and new types of attacks that are forcing IT managers to deploy a new generation of inline security systems. Figure 1 shows several typical tools between a network firewall facing the untrusted public network and the trusted private network deployed in the DMZ. (For simplicity, this diagram depicts only three types of systems in the DMZ, but other types could be deployed as well.)

Figure 1. Inline Security Tool Deployment in the DMZ

This scenario has created another compelling application for network packet brokers that improves the performance, utilization, availability and manageability of inline security systems.

First, let's consider the challenges of deploying inline security in this mode of operation:

- If any inline tool fails, then public-to-private network connectivity could be lost.
- If tools are deployed in pairs for high availability, then the switching of traffic to pair instances needs to be managed.
- If multiple tool instances are deployed because throughput outstrips tool capacity, then load balancers must be added to distribute flows across multiple instances.
- If tools need to be swapped in and out or turned up on demand, then this needs to be done without impacting connectivity or throughput.

Network managers can employ bypass switches for protection switching and redundant inline security systems; however, these are simple devices with no ability to filter, process and intelligently distribute or load balance individual packet flows to multiple tools in the DMZ.

Packet Brokers for Active, Inline Security Systems

As a result, savvy network managers are deploying packet brokers in the DMZ using a high-availability configuration that employs redundant data paths and a central pool of inline security systems that are

configured in service chains through which packet flows are directed based on application-specific criteria. This is shown in Figure 2.

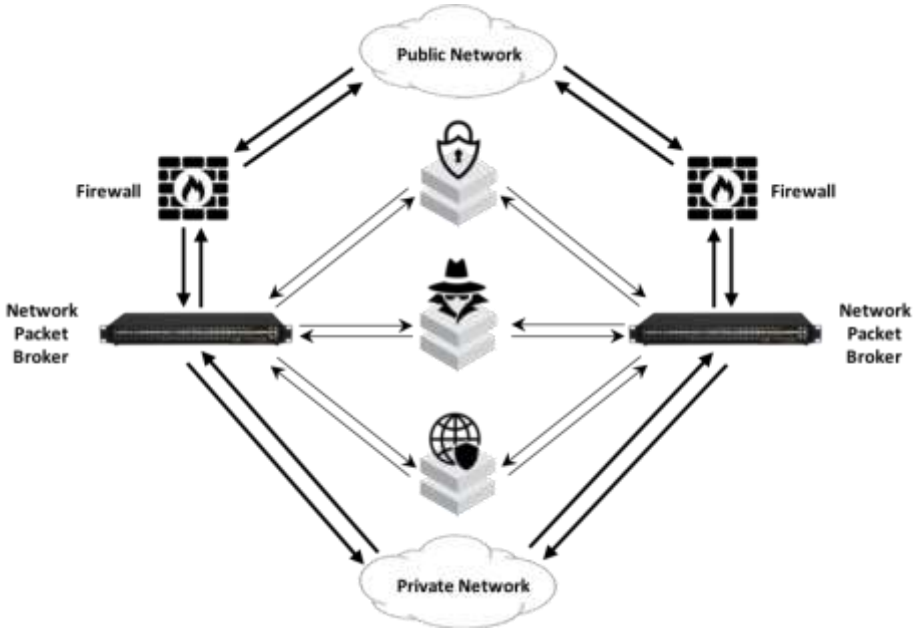

Figure 2. Packet Brokers for Service Chaining of Inline Security Systems with Built-in Redundancy

Let's assume that the firewall and packet broker pairs are operating in a simple active/standby mode. In this model, traffic flowing to and from the public network traverses the active firewall and then application traffic is switched by the corresponding active packet broker, which filters, processes and distributes flows to the various inline security systems, with each packet following its proper sequence through the service chain. Note this implies that not all packets are necessarily sequenced through all inline security systems. In addition, the packet brokers may also filter, replicate and distribute certain traffic for passive monitoring by out-of-band security, APM and NPM tools (not shown in the diagram).

This method of inline security system service chaining offers the following benefits:

- Security systems can be deployed in pairs for high availability and run in active-active mode with load balancing across each pair.
- Tool capacity can be increased by adding more tool instances and then load balancing across multiple instances.
- The rate at which packets flow to tools can be matched to capacity of each tool.
- Different inline security systems can be swapped in and out without impacting connectivity.
- Specialized inline security systems can have traffic directed to them on demand in the presence of specific security threats.

Open Compute Project (OCP) Platforms for Packet Brokering

Inline security packet broker deployments have typically utilized purpose-built platforms based on FPGAs and specialized network processors. However, the widespread commercial availability of high-performance white-box switches such as those specified by the Open Compute Project (OCP) has

enabled a new generation of more cost-effective, software-driven, packet broker platforms based on merchant silicon hardware.

Some of the world's largest hyperscale data centers are built using OCP platforms supporting 10G, 40G and 100G interfaces in high-performance leaf/spline switching architectures. Under software control, these same switches can be readily adapted for packet brokering applications, including out-of-band passive monitoring and active inline security in the DMZ.

NETSCOUT OCP Based Inline Security Solution

In 2017, NETSCOUT introduced a new line of nGenius 5000 packet flow switches based on OCP platforms, which includes the 5010 and 5100 models. In early 2018, the company is releasing a new version of its PFOS packet flow visibility software that supports inline security tool service chaining, as shown in Figure 2.

The NETSCOUT OCP platform inline security solution supports the following features:

- Operators can deploy multiple tool instances to increase effective tool capacity and ensure high availability.
- NETSCOUT's PFOS performs session-based, flow-aware load balancing of traffic across multiple instances of active security systems.
- PFOS also performs active health checks of IPS and WAF instances to detect tool malfunctions that could result in undetected security breaches.

Data center operators can also choose to deploy NETSCOUT's PFOS software on OCP compliant platforms purchased from preferred suppliers, which simplifies procurement and allows the operator to easily upgrade the packet broker hardware when performance demands exceed the capacity of the current platform.

NETSCOUT Helps Break Down Operational Silos

In most large-scale IT organizations, network operations, security operations, IT operations and DevOps teams inhabit their own silos. This is not by choice, but out of necessity, as each team employs the tool set needed to achieve its specific objectives. These silos will exist if these tools are sourced from many different vendors and cannot be easily integrated using open APIs.

As a leading provider of comprehensive network visibility solutions unified in a common operational framework, NETSCOUT is helping to break down these silos. NETSCOUT's PFOS software integrates packet flow visibility for both out-of-band passive monitoring and inline security applications encompassing both purpose-built and OCP packet broker platforms, all managed by NETSCOUT's nGenius PFS Fabric Manager.

NETSCOUT also provides a suite of industry-leading passive monitoring tools for application performance management, network performance management and network security that span data centers, private wide area networks, the public Internet and the cloud.

Moving to a software-driven packet flow visibility should enable NETSCOUT to facilitate greater synergies between network and security operations teams, enabling them to immediately detect security threats and move rapidly to mitigate against them.

Analyst Biography: Stephen Collins is Principal Analyst at ACG Research, leading the firm's practice in network visibility and analytics. He has more than three decades of networking and telecommunications industry experience across many segments of both the enterprise and service provider markets. Stephen has worked in business and technical organizations for many leading hardware and software infrastructure vendors, serving in executive and managerial roles, including: general manager, VP of marketing, VP of product marketing, VP of business development, product line manager and software engineering manager. He has extensive experience bringing new products to market with technology-driven startups and emerging growth companies as a company founder, member of the senior management team, independent consultant and advisor to early-stage investors.

Stephen is a frequent speaker at industry conferences and has authored numerous articles for trade publications. He holds an M.S. in Computer, Information and Control engineering from the University of Michigan and a B.S. in Computer Systems Engineering, Summa Cum Laude, from the University of Massachusetts, Amherst. He currently serves as an advisor to the ECE department at UMass Dartmouth and mentors students in technology innovation and entrepreneurship at Brown University.

Authorship: This paper was authored by ACG Research, which is solely responsible for its contents.

Sponsorship: NETSCOUT Systems, March 2018.