Cisco and NETSCOUT: Actionable Visibility and Advanced Security Controls

With ever-expanding connectivity in our modern networks, the widespread adoption of cloud computing and BYOD, the requirements for actionable security have never been more demanding. Networks now go beyond traditional walls and include data centers, endpoints, virtual environments, branch offices and the cloud. Gaining visibility is challenging as these networks become more complex, distributed, and dynamic. As threats to the network become more sophisticated and targeted, the need for comprehensive network visibility has never been greater.

Deploying analytical devices at every point where network traffic needs to be captured is cost prohibitive for large-scale, complex networks. In addition, performance and throughput limitations of these devices hamper the responsiveness and intelligence needed to protect against escalating threats, damaging attacks, and very diverse threat vectors. Attackers are taking advantage of gaps in visibility and protection to compromise network security. Cisco and NETSCOUT have partnered to provide you with a cost-effective, highly scalable, and pervasive approach to achieving comprehensive network visibility, enhanced network security and forensic capabilities.

Proven Integration Between Cisco FirePOWER Security and NETSCOUT nGenius Packet Flow Switches

The NETSCOUT nGenius® packet flow switches offer advanced packet conditioning solutions for both passive and active inline security tools. These systems enable you to easily and rapidly deploy, scale and optimize your Cisco® FirePOWER security solution into complex environments where there is significant contention for data access and visibility (via SPAN or TAPs). The packet flow switches support demanding NGFW and NGIPS throughput requirements with hardware-accelerated line rate performance. In environments where asymmetric routing occurs, the NPBs provide L2 session-aware load-balancing capabilities as well.

With nGenius, you can connect multiple Cisco FirePOWER sensors to each packet flow switch incrementally multiple Cisco FirePOWER sensors to each packet flow switches incrementally, in passive or inline configurations, to support multiple networks, network segments, and diverse policies. The combined technologies deliver a high level of network security, availability, redundancy and flexibility—future proofing your overall IT investments in security and network infrastructure. The joint solution provides a sophisticated infrastructure that offers unmatched visibility spanning the entirety of the network, endpoints, private clouds and the data centers to deliver a unified packet plane. Together, the combined Cisco and NETSCOUT solutions have been field tested and proven in live production environments across many verticals: Financial Services, Energy, Government and Critical Infrastructure, Pharmaceutical and Healthcare, and Telco Operators.

Enhanced Security

Functionality and features gained:

- Security service assurance
- Speed/Media conversion
- L2-7 traffic grooming
- Load balancing/asymmetric routing support
- Decrypt once; feed many security systems
- Security-in-series (security service chaining)
- High availability for security systems
- Thresholds, alerts & auto triggers
- Custom security system health checks (negative and positive)
- Fault tolerance for security systems & networks
- Test/deploy security systems without network disruption
- Actionable XML/API integration

Simplified Design and Deployment for Scalable Fail-Safe Security

Use Case: Scalable Network Security Architecture

Deploy multiple Cisco FirePOWER security layers (inline and passive) through a single nGenius packet flow switch.

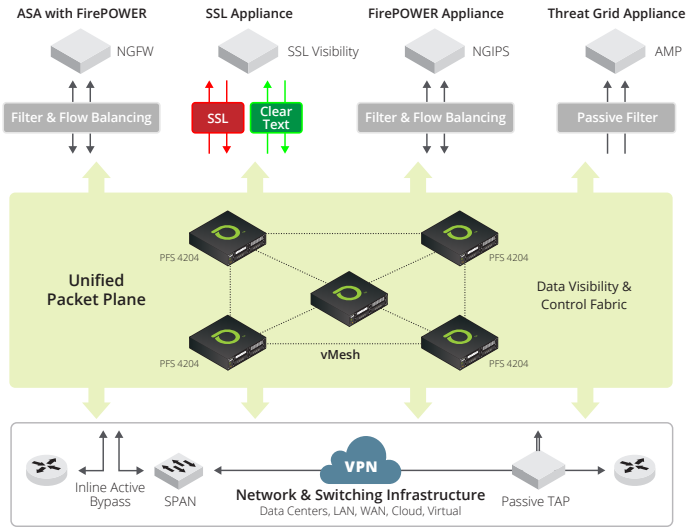

Figure 1: Cisco FirePOWER threat-centric layered security through packet flow switching from NETSCOUT.

Unlike the traditional approach of using dedicated devices for each security layer, you can leverage the nGenius packet flow switch with PowerSafe™ to provide active inline packet redirection based on user-defined policies for specific network flows. By leveraging the nGenius unique tool chaining features, you can also identify specific traffic flows and actively redirect these flows for analysis to the appropriate Cisco FirePOWER security appliance or series of appliances, each offering a focused and layered approach to network security. Users can configure multiple Cisco FirePOWER Sensors so that they process only certain types of traffic or so that the traffic is spread across the Cisco FirePOWER sensors via session-aware load balancing with optimized fault tolerance and High Availability (HA) functionality.

Summary

As outlined in the use case, nGenius packet flow switches can optimize visibility, scalability, and security across the Cisco FirePOWER solution portfolio and deliver:

- Session-aware load balancing with support for asymmetrical traffic for NGIPS & L2 NGFW deployments
- Scalable deployment for transparent SSL proxies
- End-to-end visibility for Advanced Malware Prevention (AMP Threat Grid) solutions
- Security service chaining to achieve a highly scalable network security architecture

Together, Cisco and NETSCOUT provide a joint security solution that delivers a highly scalable network security architecture to address increasingly sophisticated and targeted network threats.

About NETSCOUT nGenius Packet Flow Switches

NETSCOUT nGenius packet flow switches optimize the flow of traffic from the network to the security systems and monitoring tools. These appliances collect and organize packet flows—creating a unified packet plane that logically separates the network layer from the tool layer. Our customers use packet flow switches to optimize and scale both their service assurance platform and cybersecurity deployments so that they can spend less time adding, testing and managing their tools.

About Cisco Threat-Centric Security

Cisco provides one of the industry's most comprehensive advanced threat protection portfolios of products and solutions. Our threat-centric and operational approach to security reduces complexity, while providing superior visibility, continuous control, and advanced threat protection across the extended network and the entire attack continuum. The Cisco threat-centric security model is built to address your biggest security challenges, cover the entire attack continuum, and reduce security gaps and complexity caused by disparate products and disjointed solutions. For more information, visit: http://www.cisco.com/c/en/us/products/security/technology.html

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000