Gaining Scalability and Flexibility for Monitoring and Security Tools

OVERVIEW

Industry

Financial Services – Worldwide

Business Challenges

- Adding a new inline security system to an existing packet flow switching environment supporting passive monitoring
- Simplifying traffic flow to multiple tools
- Ensuring continuous high performance and scalability of monitoring and security systems

NETSCOUT Solution

- NETSCOUT nGenius® Packet Flow Switches
- Optimizer 2400

Business Value

- Gained the ability to feed multiple passive and active tools simultaneously from the same traffic source: capture once, use multiple times.
- Easily integrated new nGenius Packet Flow Switches (PFS) into existing deployment
- Enhanced visibility for existing security systems
- Increased agility to meet changing security needs

Global Financial Services Company Creates Packet Visibility Foundation for the Future

"With nGenius Packet Flow Switches, we can easily add new inline tools, such as malware detection engines, without causing disruption to the network. NETSCOUT enables us to continually improve our security posture with the visibility we require as threats evolve."
– Network Engineer

Introduction

This company is one of the world's largest financial services institutions. It provides individual and institutional clients with a range of products and services, including life insurance, annuities, retirement-related services, mutual funds, and investment management. As the company evolved its security strategy, it turned to NETSCOUT to also help it increase visibility and achieve stability in its expanding security infrastructure.

Challenges

Financial services institutions are one of the top targets for cyber attackers. Protecting customer privacy and the security of financial data is mission critical. So, when the company reviewed its security strategy to stay ahead of evolving threats, it needed to simultaneously scale and achieve better visibility for its security monitoring solutions.

The company had previously deployed the Optimizer 2400 for packet visibility supporting Intrusion Detection System (IDS) and Network Performance Monitoring (NPM) tools, which were both passive. To enhance its security posture, the company was adding a Behavioral Analytics Security system, which was to be deployed inline, in active mode. Deploying an inline appliance means that traffic is returned back to the production network after inspection.

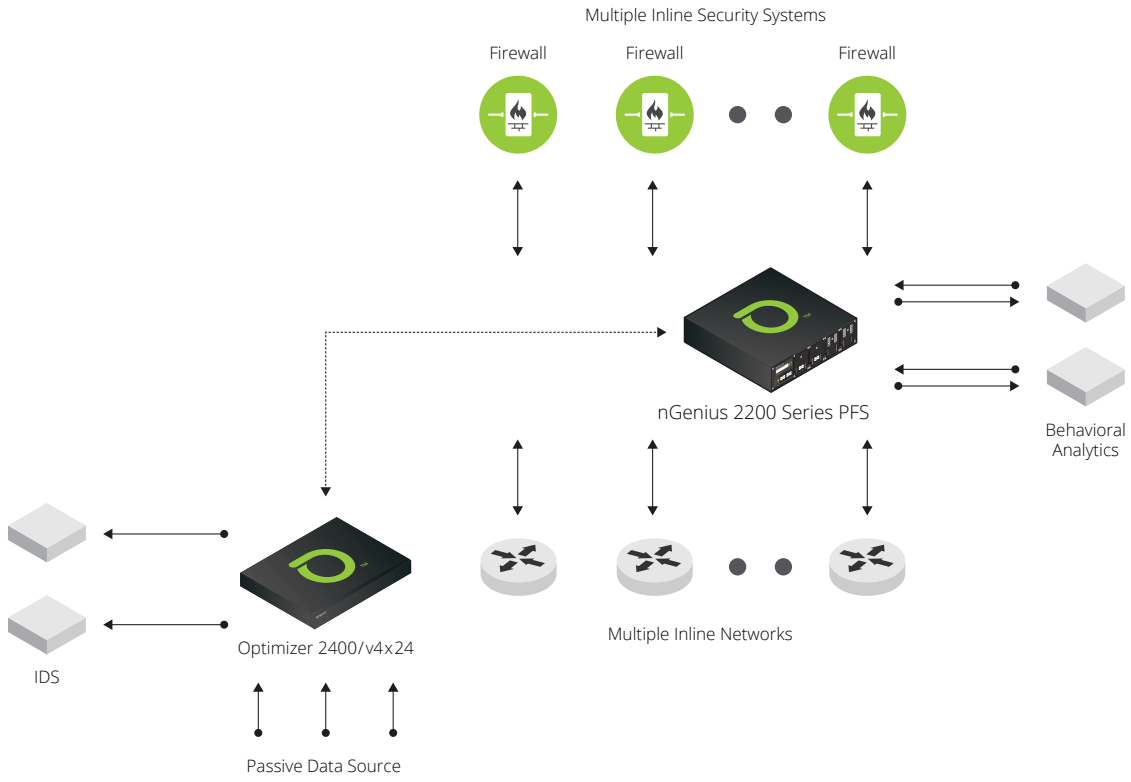

Figure 1: NETSCOUT packet flow switch deployment in financial services institution's monitoring infrastructure.

The security team also wanted to remove non-essential packets, such as backup traffic and routing protocol headers, from being sent to the security appliance, to improve system performance and reduce false positives. Easy troubleshooting was important, as was the ability to ensure that security appliances were functioning as expected through policy-based health checks. Finally, if a security system wasn't performing, the team wanted to prevent traffic from being sent to it in order to avoid possible network disruption.

The security team did not want to create a siloed, stand-alone deployment of the new Behavioral Analytics appliances. They wanted to create unified visibility for all of their network performance management and security systems. The visibility would span multiple network segments regardless of whether the tool was passive or inline.

Solution

Flexibility in Action

Based on its satisfaction with existing NETSCOUT products, the team approached NETSCOUT with its requirements. The goal was to deploy inline monitoring for the new Behavioral Analytics appliance traffic, and then send the same traffic to the existing IDS and NPM tools, which operate in passive mode.

The solution was NETSCOUT nGenius Packet Flow Switches. They access, optimize, and deliver traffic from multiple network segments to multiple network and security systems — both passive and inline. When deployed in the company's monitoring infrastructure, the packet flow switches optimize traffic from the network, provide it to the inline Behavioral Analytics appliances, and then send a copy of the data to the passive IDS and NPM tools that are connected to the Optimizer 2400. Traffic can also be sent to other inline security systems in the future if business requirements evolve.

The underlying NETSCOUT mesh architecture enables multiple PFS nodes to work together and be managed as one device. The self-organizing architecture provides a redundant mesh among packet visibility appliances for complete, fault-tolerant visibility. This architecture easily scales as needed for global packet visibility.

Investment Protection with Reduced Total Cost of Ownership

The new NETSCOUT deployment enables the company to retain its investment in existing monitoring infrastructure while gaining better visibility and more agility. Traffic can be captured once and sent to multiple passive monitoring and inline security

systems simultaneously. The company can now deploy new monitoring or security systems to meet changing requirements.

At the same time, the deployment of packet flow switches extends the life of existing tools retaining its investment. Nor does it have to add instances of the IDS and NPM solutions, reducing total cost of ownership.

Easy Scalability

Network traffic can be load balanced across multiple instances of a system to improve capacity and resilience of the monitoring infrastructure. This gives the team flexibility to redistribute traffic and improve system performance. If needed, the company could easily deploy additional systems and load balance across the multiples instances of the systems. Changes are now easier to make and can be implemented quickly.

Ensuring Tool Health

Unlike simple ping or heartbeat heath checks, the packet flow switches perform negative and positive health checks across the full system stack, from physical to application layer, to ensure the monitoring or security systems are functioning as expected. If a system is not behaving as expected, the packet flow switch can automatically change to an alternate configuration to maintain network, monitoring, and security functionality. Once the system has returned to a normal state, the original configuration can be automatically reapplied.

Foundation for the Future

With NETSCOUT packet flow switches and a flexible monitoring and security architecture, the financial services company has a solid foundation for ensuring visibility and scalability of its evolving monitoring and security infrastructure. Instead of having to change the network topology each time they want to implement a new system or add network segments to be monitored or secured, the team can make a simple configuration change as needed. Operations are simplified, with a flexible packet visibility infrastructure based on NETSCOUT packet flow switches.

"Security threats are only expected to increase and diversify, but with flexible, scalable packet flow switching, we are much better prepared to keep pace."
– Security Architect.

Operations are simplified, with a flexible packet visibility infrastructure based on NETSCOUT packet flow switches.

For more information, visit www.netscout.com/pfs.

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