High Availability for Threat Prevention

OVERVIEW

Partner: FireEye

Industry: Bio-Tech

Location: California, USA

NETSCOUT Security Solutions

- nGenius® Packet Flow Switch Series
- Health checks to ensure tool uptime
- Redundancy

Business Value

- Assurance that 100% of traffic is monitored
- No single point of failure
- Seamless failover
- Efficient, inline tool deployment

"NETSCOUT allowed us to deploy a true HA scenario, with no single-point-of-failure anywhere on our network. Appliances seamlessly monitor both ingress and egress traffic to provide coverage in any outage scenario."
Company Vice President

A Leading Bio-tech Company Protects their Networks from Malicious Activity with the FireEye Threat Prevention Platform Optimized with NETSCOUT nGenius Packet Flow Switches

Despite the best efforts on the part of their employees, malware can infiltrate a company's internal environment and try to discover and transmit confidential information out of the company's internal network. The subject company, a leading bio-engineering company chose to address this by adding FireEye™ Threat Prevention Platform appliances to their security infrastructure to stop next-generation threats. The next challenge was to design the environment incorporating the FireEye appliances in a redundant, high availability manner, while keeping within a reasonable budget.

Challenge: Efficiently deploy inline malware protection in a high availability environment with no single point of failure.

The Company's goal was to efficiently deploy these devices to provide coverage on both the active and the passive failover network segment. In the initial design, devices were deployed off of SPAN ports on both the Active and the passive failover router. While this gives a certain level of coverage, it has failings in that the appliances are not inline, and there is no indication if a monitoring tool fails.

With the tools deployed off of SPAN ports, there was no real-time capability to block malicious or inappropriate traffic. All actions taken by the monitoring tools were taken passively, leaving the company vulnerable to an attack with limited response until the attack was reviewed and appropriate countermeasures could be taken. The second challenge was ensuring that the tools were not only accepting packets, but were working properly and providing the desired protection. In a passive environment, there is no indication that the tool has failed, leaving the company unprotected while the tool is offline.

Solution: True HA with NETSCOUT nGenius PFS 2204

Company was able to meet the challenges by deploying two nGenius Packet Flow Switches (PFS) PFS 2204 devices, one inline on each network segment. This allowed the devices to physically

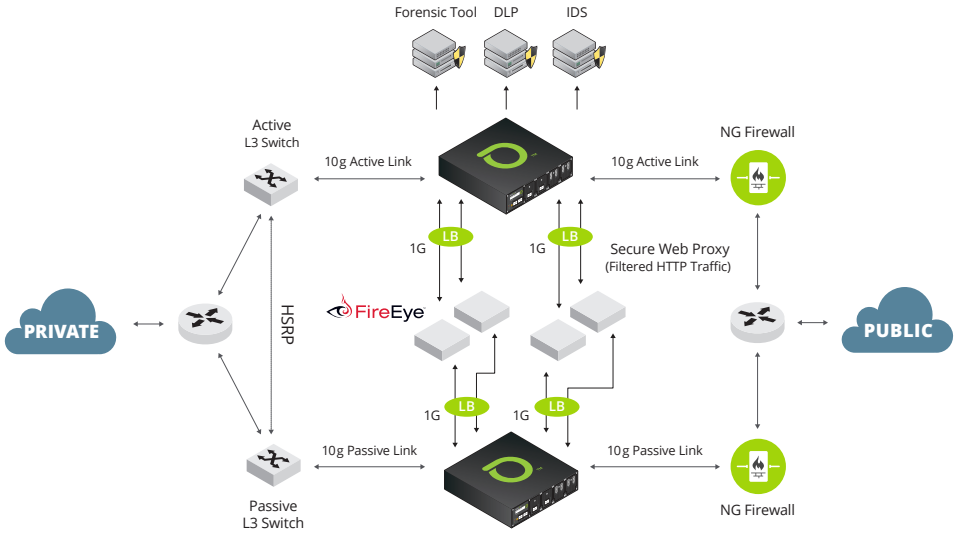

Figure 1: Total Visibility for Threat Prevention with nGenius Packet Flow Switches.

sit inline on the network and for the nGenius PFS 2204 to send live, inline network traffic first to the FireEye appliance and then to the Blue Coat appliance before it left their network. Each security appliance (FireEye and Blue Coat) was connected to both nGenius packet flow switches, allowing each security appliance to protect both the primary and secondary failover link.

The real-time monitoring capability allowed for traffic to be blocked or modified if it was determined to be malicious or inappropriate. This gave an enhanced layer of security by allowing live traffic to be blocked before it can infect an end user. In addition, with nGenius load balancing capabilities, asymmetrically routed traffic due to primary to secondary segment failover is always handled by the same appliance, ensuring that each appliance sees the entire conversation between two devices, ensuring full malware protection and that legitimate malware callback traffic is blocked.

In addition, the nGenius PFS 2204 is able to send user defined health check packets through each appliance to ensure that it is up and functioning properly. The health check packet is not only able to determine if the device is up and running, but is also able to block malicious content properly as well. In the event that a device is not functioning correctly, traffic can be routed to the backup appliance, ensuring that all traffic is monitored without any manual intervention.

In addition, the solution allows for maintenance to be performed on any tools that are connected through the vMesh, anywhere on the network with no downtime required. Each individual security appliance that is connected to a NETSCOUT packet flow switch, including the FireEye Threat Prevention Platform, and even the routers and firewalls, can be taken offline with no security protection downtime, allowing for a true HA solution.

About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time.

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.

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