High Availability for Malware Protection

FireEye & VSS Monitoring Case Study

In Brief

Partner: **FireEye**

Industry: Bio-Tech

Challenges:

- Efficient, Inline tool deployment
- No Single-point-of-failure.

Solution:

- VSS Monitoring Protector Series
- Health checks to ensure tool uptime
- Redundancy

Benefits

- Assurance that 100% of traffic is monitored
- No single point of failure
- Seamless failover

A leading bio-tech company protects their networks from malicious activity with the FireEye Malware Protection System™ optimized with VSS Monitoring Network Packet Brokers.

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 Malware Protection System (MPS) 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.

> *"VSS Monitoring 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

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.

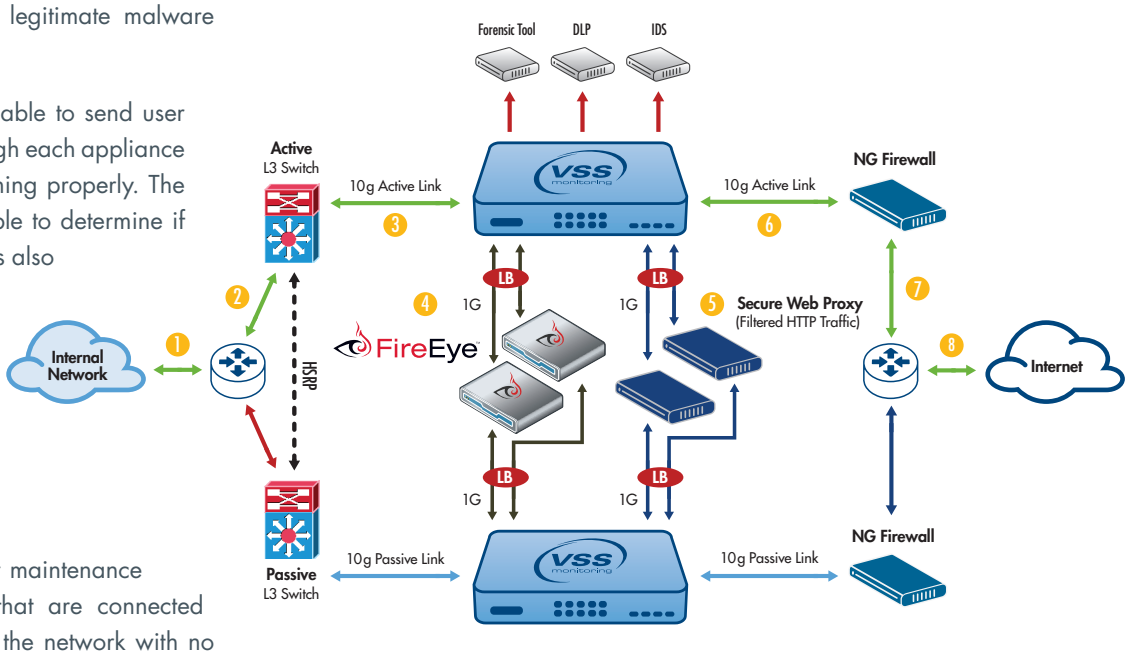
Solution: True HA with VSS Monitoring vProtector Series

Company was able to meet the challenges by deploying two VSS vProtector 2020 devices, one inline on each network segment. This allowed the devices to physically sit inline on the network and for the vProtector appliance 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 VSS vProtectors, 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 VSS Monitoring's 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 VSS vProtector 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 VSS NPB, including the FireEye Malware Protection System, 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 is the leader in stopping advanced targeted attacks that use advanced malware, zero-day exploits, and APT tactics. The FireEye solutions supplement traditional and next generation firewalls, IPS, anti-virus, and gateways, which cannot stop advanced threats, leaving security holes in networks. FireEye offers the industry's only solution that detects and blocks attacks across both Web and email threat vectors as well as latent malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Based in Milpitas, California, FireEye is backed by premier financial partners including Sequoia Capital, Norwest Venture Partners, and Juniper Networks.

About VSS Monitoring

VSS Monitoring is the industry leader in network packet brokers (NPB), providing a unique Unified Visibility Plane for network tools and security systems, enabling network-wide and link-layer visibility. Deployed globally by 80% of the world's tier 1 service providers, F500 corporations and major government agencies, VSS Monitoring packet brokers improve tool usage and efficiency, simplify IT operations, and greatly enhance tool ROI.

For more information please contact us at info@vssmonitoring.com