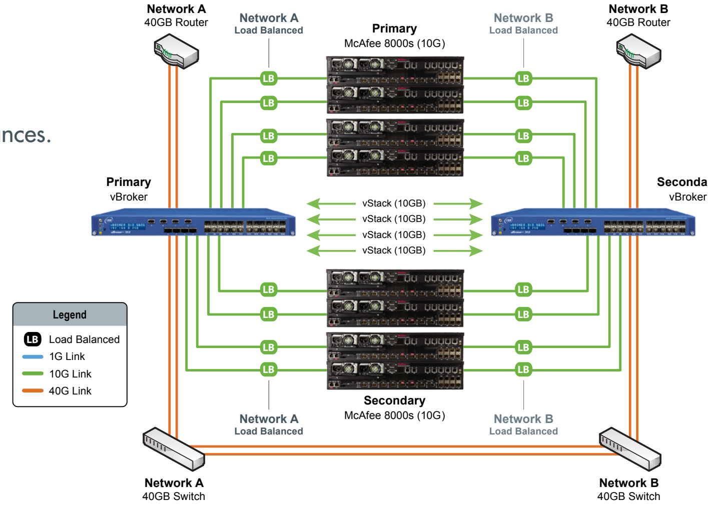
McAfee & VSS Monitoring – *Battle Card*

Customer Pain Points	*VSS/McAfee Solution*
How can the customer's existing McAfee 1 G products be used in the new 10 G environment? Difficulty in accessing the network (due to SPAN port contention, simple tapping or legacy in-line solutions) results in poor visibility for the existing McAfee solution. This contributes to longer incident-response/resolution times (increased MTTR).	**100% fail-safe visibility into all network links:** VSS's vBroker or vProtector products allow multiple McAfee tools to gain instant visibility into all network segments connected to any other VSS device within the vMesh™. Geographic limitations are removed and even remote sites are part of the same system via vMesh over TCP.
The customer needs to implement a comprehensive "security in Layers" approach using a McAfee based design. No matter which products the customer plans on integrating (McAfee Network Security Platform (NSP) Systems, McAfee DLP, and McAfee Email & Web Security Gateways) VSS allows them to work together seamlessly.	**Leverage existing tools more effectively:** Use selective aggregation, filtering and session-aware load balancing to unify multiple physical and logical network segments (1G/10G/40) and send only what's needed to the appropriate McAfee tools. vProtector allows customers to easily convert from passive IDS to active IPS in just minutes. The result is a far more efficient, cost effective, end-to-end solution, providing a complete security monitoring system and panoramic network visibility.
Inline security Proof of Concept (PoC) time and complexity is slowing the customer's approval process. Any evaluation of new inline security tools can be extremely challenging for the SEC Ops staff and often require numerous executive sigh-offs to be authorized and implemented. If any problem occurs it can disable the entire network and create unscheduled downtime. This adversely effects corporate productivity and causes decision makers to delay security projects. Is there an easier way to safely run PoCs in parallel?	**Inline security proof of concepts (PoC) each takes an average of 3 months to complete without VSS.** Using vProtector, customers can evaluate multiple new McAfee products in parallel showing performance results based on exactly the same traffic. This approach reduces the validation time and conclusively shows which PoC solution is best. Even if customers take a traditional one-after-the other (PoC) approach the traffic they are testing will change. You can easily achieve the goal of parallel PoC analysis using the unique features that vProtector provides.

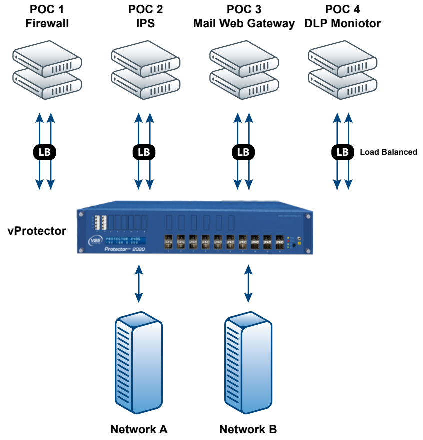
Use Case 1 – Ensure McAfee tool fault-tolerance in 10G/40G environments.

- Provide High Availability across all links with VSS and McAfee NSP Appliances.
- Using Session Aware Load Balancing customers can maintain full session integrity and maximize tool availability.
- Support either Active-Active or Active-Passive customer configurations.
- Pre-filter traffic leaving only what is required, thereby improving the performance of all McAfee appliances.
- Time and port stamp traffic to show exactly where and when a network event occurred.



Use Case 2 – vProtector supporting multiple inline Proof of Concepts (PoC)

- Support multiple In-line McAfee Network Security Platform POC deployments that require in-line bypass functionality.
- Policy Based Triggers allow customers to customize vProtector's behavior when security or network events occur.
- Fail-open or fail-closed functionality provides ultimate flexibility when working with confidential or classified networks.
- Easily comply with PCI, HIPAA or Sarbanes Oxley regulations by maintaining 5 9s level service assurance.
- Share Data Access and Intelligence between Inline active McAfee WAF, DSG & File FW(s), and OOB DMG or File Activity Monitoring appliances.
- Run multiple POCs, in parallel with minimal risk and significantly reduce the time required to complete the evaluation.



Qualifying Questions

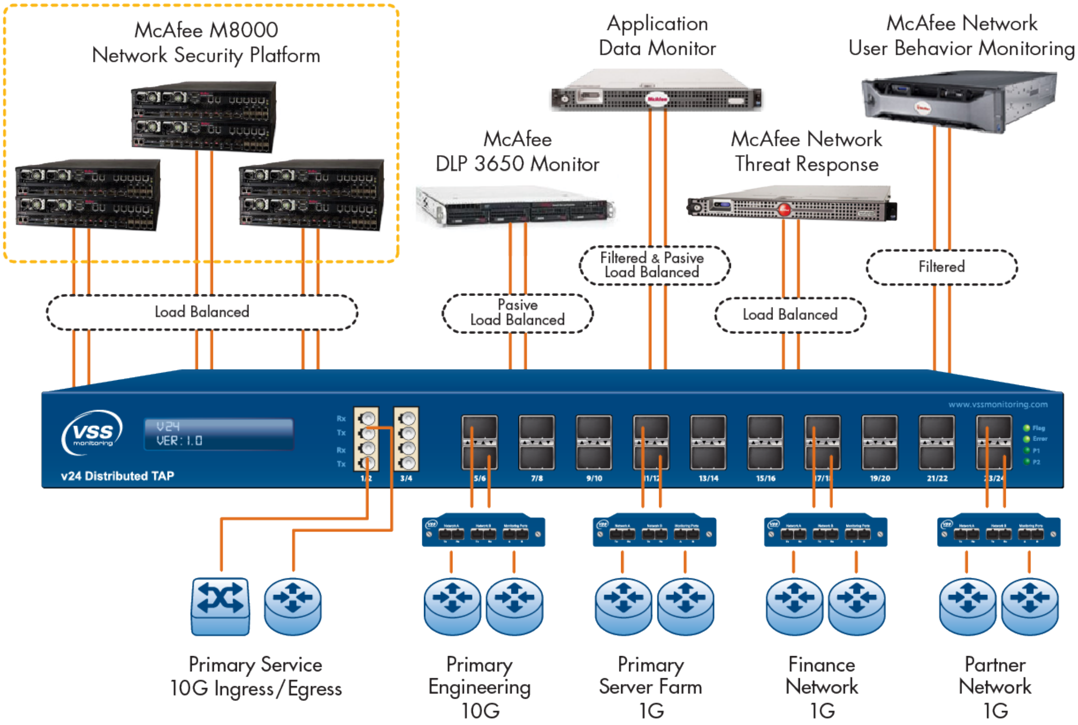
New McAfee Deployments

- Does the customer need to tap into one or more 10G links and have the traffic aggregated and filtered to multiple, active or passive Network Security Platform Appliances?
- Does the customer need precise port and time stamping to identify exactly where and when an event occurred?
- Does the customer require five 9s uptime?
- Are there other monitoring or security tools used by the customer that need to see the same network traffic?
- Does the customer need in-line bypass functionality for their active security tools (IDS vs IPS)?

Existing McAfee Deployments

- Has the existing McAfee solution dropped packets due to being overloaded?
- Has the customer increased network link speeds (1G to 10G or even 10G to 40G) since the initial McAfee deployment?
- Does the network configuration include multiple monitoring or security tools that need the same network traffic information?
- Does the customer need advanced policy based, filtering or triggering functionality?
- Could the McAfee device be running short of memory?

Solution Example



McAfee & VSS Monitoring Products

The VSS vBroker series aggregates, filters and delivers traffic from one or more full-duplex networks, to one or more McAfee NSP appliances. VSS's vProtector provides policy-based triggers, health checks, fail-open / fail-close configurability and can be augmented with filtering and advanced session aware load balancing. Using these features together provide redundancy and high availability to the McAfee solution. These unique capabilities enable customers to realize a reduction in MTTR, increased efficiency and ROI with new or existing McAfee deployments.

Contact Us

For more information on the VSS/McAfee partnership, including relevant Solution Briefs, Use Cases, Product Brochures and Whitepapers, please go to http://www.vssmonitoring.com/partners/alliances/McAfee.asp or scan:

For more resources: McAfee@vssmonitoring.com