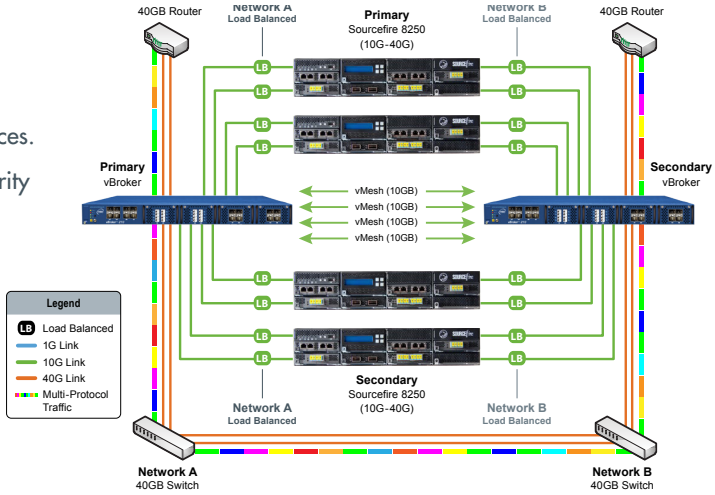
Sourcefire & VSS Monitoring – *Battle Card*

Customer Pain Points	VSS/Sourcefire Solution
How can the customer's existing Sourcefire 1/10 G products be best used in new 10/40 G environments? The customer has an existing Sourcefire deployment that was appropriate for their network's speeds at the time of purchase. However, since that time, their network speed has increased to 10G or 40G.	**VSS allows for continued use of existing 1/10G products with increased network speeds:** The VSS Monitoring network packet broker system bridges the gap between 10/40G links and 1/10G tools, using selective hardware-based filtering, high data burst buffers and session-aware load balancing to reduce the amount and speed of traffic that each tool receives without loosing any packets.
The customer needs to implement a comprehensive "Security in Layers" approach using a Sourcefire based design including the following products: Next-Generation IPS, Application Control, Next-Generation Firewall, Centralized Management and SSL I3Dection. These resources need to be seamlessly integrated with Sourcefire Malware products such as FireAMP, FireAMP Virtual, FireAMP Mobile, AMP for FirePOWER.	**Leverage existing tools more effectively:** Use selective aggregation, filtering and session-aware load balancing to unify multiple physical and logical network segments (1G/10G/40G) and send only what's needed to the appropriate Sourcefire 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 Security Ops staff and often require numerous executive sign-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.	**Customers can evaluate multiple security tools in parallel shortening PoC times.** Using vProtector, customers can evaluate multiple new Sourcefire products at the same time showing performance results based on exactly the same traffic. This approach reduces the validation time and conclusively shows which PoC solution is best.

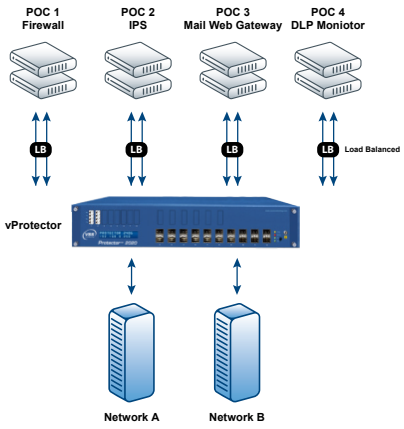
Use Case 1 – Ensure Sourcefire tool fault-tolerance in 10G/40G environments.

- Provide High Availability across all links with VSS and Sourcefire 3D 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 Sourcefire 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 Sourcefire 3D 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 five 9s level service assurance.
- Run multiple POCs in parallel with minimal risk and significantly reduce the time required to complete the evaluation.



Qualifying Questions

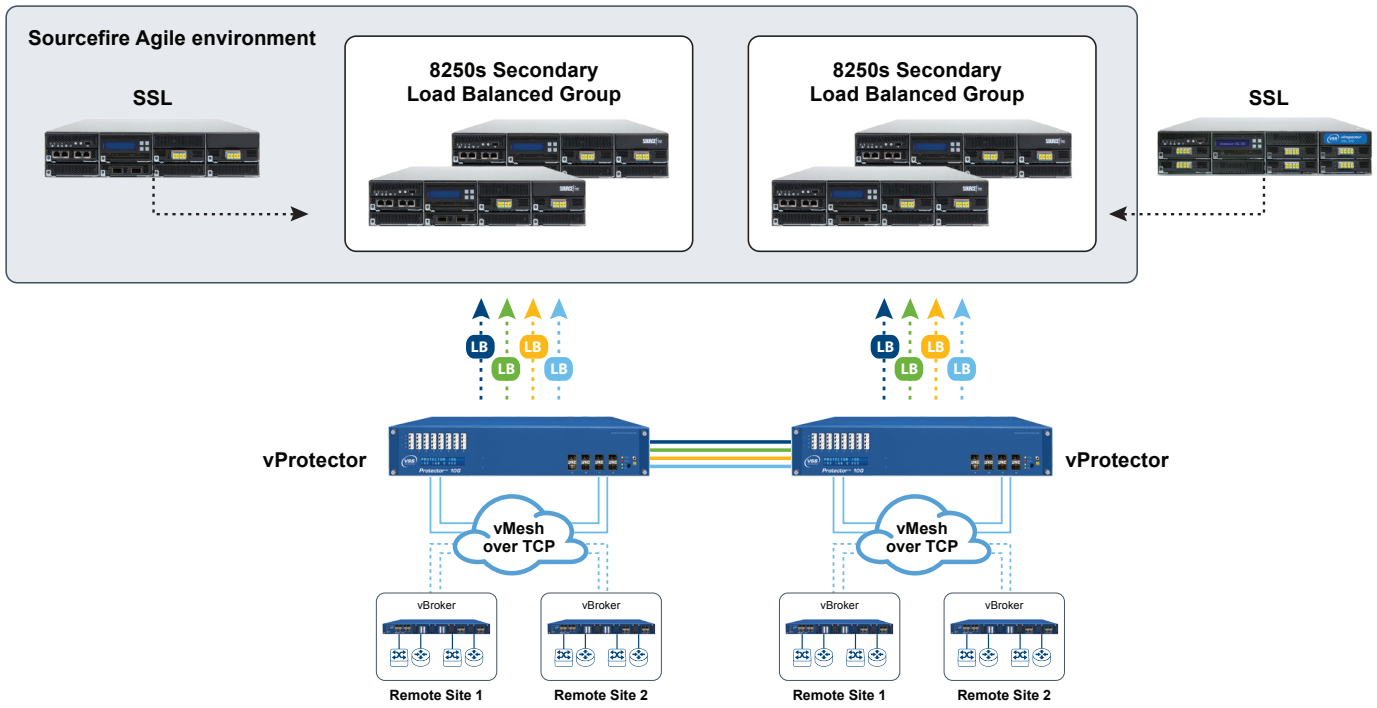
New Sourcefire Deployments

- Does the customer need to tap into one or more 10/40G links and have the traffic aggregated and filtered to multiple, active or passive Sourcefire 3D 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 Sourcefire Deployments

- Has the existing Sourcefire 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 Sourcefire 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 Sourcefire device be running short of memory?

Solution Example



Sourcefire & VSS Monitoring Products

The VSS vBroker series aggregates, filters and delivers traffic from one or more full-duplex networks, to one or more Sourcefire 3D 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 Sourcefire solution. These unique capabilities enable customers to realize a reduction in MTTR, increased efficiency and ROI with new or existing Sourcefire deployments.

Contact Us

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

For more resources: Sourcefire@vssmonitoring.com