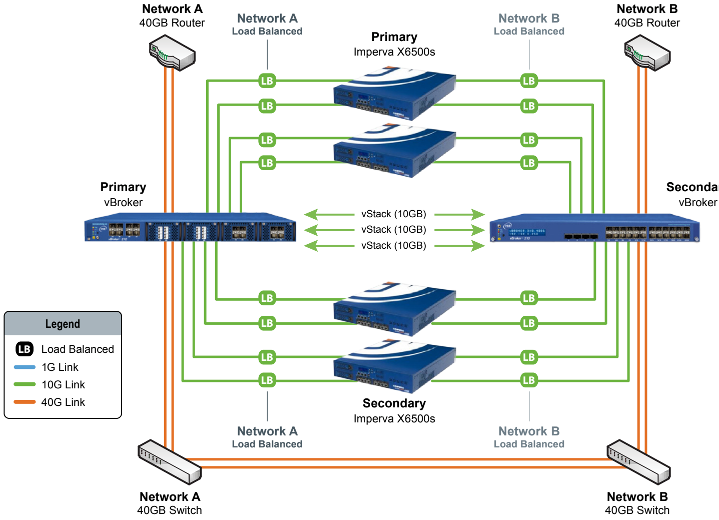
Imperva & VSS Monitoring – *Battle Card*

Customer Pain Points	VSS/Imperva Solution
Limited network visibility due to outdated network instrumentation method: Difficulty in accessing the network (due to SPAN port contention, simple tapping or legacy in-line solutions) leads to poor visibility for multiple Imperva tools. This contributes to potentially lengthy incident-response/resolution times (increased MTTR).	**100% fail-safe visibility into all network links:** vBroker or vProtector products, once wired into the network, allow multiple Imperva tools to gain instant visibility into all network segments connected to any other VSS device within the vMesh. Customers can expand to include remote sites via vMesh over TCP.
Network speeds have increased from 1G to 10G/40G but current tools lack the performance or 10G ports. Buying new 10G tools can be extremely expensive, while network infrastructure speeds have increased rapidly the corresponding tool budgets frequently are underfunded. Figuring out a way to leverage existing tools not only increases their ROI but helps older tools play an even more functional role within the overall network plan.	**Leverage existing tools more effectively:** Use selective aggregation, filtering and session-aware load balancing to unify multiple physical and logical network segments (1G/10G) and send only what's needed to the appropriate Imperva tools. The result is a far more efficient, cost effective, end-to-end solution, providing comprehensive and strategic network visibility. VSS also offers a central management solution.
Network or Imperva tool downtime: A customer typically has to experience network outages when adding new Imperva tools into the production network or taking them offline for maintenance. And if 1G Imperva tools are overloaded by 10G traffic, limited performance could prevent maintaining mandated security compliance and monitoring mission-critical core links.	**100% network and Imperva tool fault-tolerance:** VSS's vProtector is wired into the network once, allowing new Imperva tools to be added or taken offline for maintenance without causing network outages. VSS can load balance 10G traffic to 1G Imperva tools, perform custom health checks on them and bypass failed tools to either backup tools and/or send reset packet to firewalls.

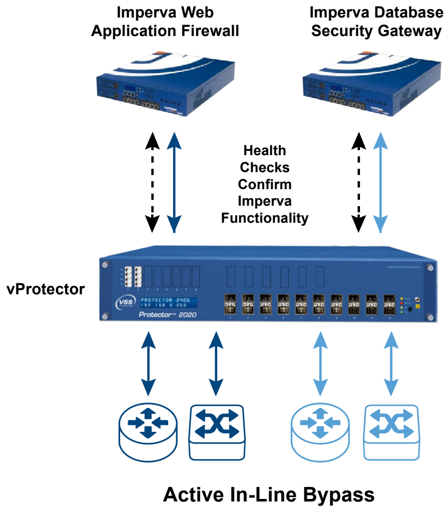
Use Case 1 – Establish 100% network visibility for all Imperva tools.

- Aggregate all required traffic together in a single traffic stream while maintaining link level visibility.
- Pre-filter traffic leaving only what is required, thereby improving the performance of Imperva appliances.
- Time and port stamp traffic to show exactly where and when a network event occurred.
- These features allow customers to quickly respond to dynamically changing network or security requirements.



Use Case 2 – 100% network visibility and Imperva tool fault-tolerance in 10G/40G environments.

- Provide High Availability across all links with VSS and Imperva Secure Sphere 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.
- Easily replace, upgrade or insert new Imperva tools into the network without experiencing any downtime.
- Pre-filter traffic leaving only what is required, thereby improving the performance of Imperva appliances.



Qualifying Questions

New Imperva Deployments

- Does the customer need to tap into one or more 10G links and have the traffic aggregated and filtered to multiple Secure Sphere 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 or filtered network traffic?
- Does the customer need in-line bypass functionality for their security tools?

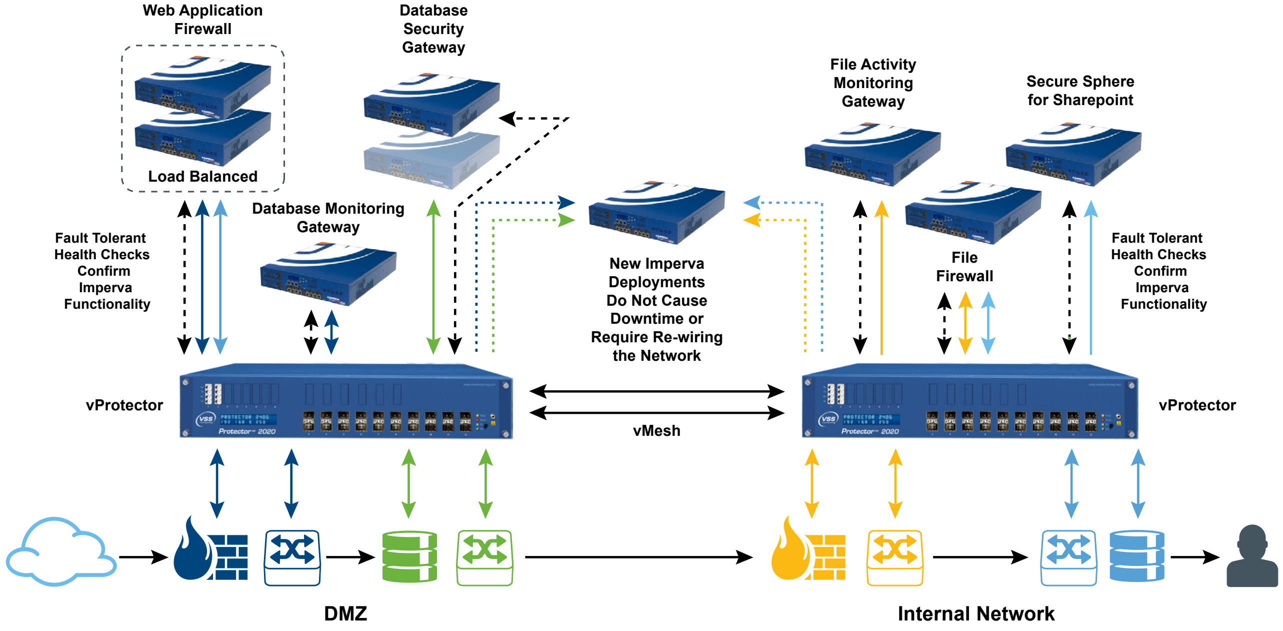
Existing Imperva Deployments

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

Solution Example

VSS vProtectors Providing In-Line Bypass Functionality with Imperva X6500s

Health-Checks, Filtering, Policy Based Triggers and Session Aware Load Balancing


Web Application Firewall
Load Balanced
Database Security Gateway
Database Monitoring Gateway
Fault Tolerant Health Checks Confirm Imperva Functionality
New Imperva Deployments Do Not Cause Downtime or Require Re-wiring the Network
File Activity Monitoring Gateway
Secure Sphere for Sharepoint
File Firewall
Fault Tolerant Health Checks Confirm Imperva Functionality
vProtector
vMesh
vProtector
DMZ
Internal Network

VSS Monitoring and Imperva Secure Sphere Products

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

Contact Us

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

For more resources: Imperva@vssmonitoring.com