



OPTIMIZE PROOF OF CONCEPT (POC) CYCLES FOR VALIDATING NETWORK INTELLIGENCE TOOLS WITH VSS MONITORING

VSS OPTIMIZED NETWORK INTELLIGENCE ARCHITECTURE ACCELERATES TECHNOLOGY ADOPTION, LOWERS COST OF OPERATIONS, AND REDUCES TIME-TO-PROTECTION AGAINST CYBER THREATS.

Network Security Landscape

"Our nation is at risk," says the White House spokesperson. "Cyber-security vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity."

"Cyber criminals don't take a day off. They are relentless, and everyone in America is at risk. They're trying to penetrate our critical infrastructure--including our power grid and financial networks--and harm our nation. With every passing day, we lose more and grow less secure. We must put an end to this," said Chairman Rockefeller

"Further delay compromises our ability to better protect Americans against cyber intrusions and attacks that target our financial, commercial, transportation, and communications sectors," says Senator Olympia Snowe.

These statements indicate a considerable growth in targeted cyber attacks that have been increasing in both frequency and malicious intent. The new breed of cyber threats leverage best of breed attack techniques across different layers, network, application and even user layers like social networking.

Although government agencies and private sectors are now trying to quickly move to cloud computing for the potential lower-cost and ease of maintenance, various reports give alarm that moving servers outside the enterprise firewalls leave gaping holes in the network security architecture that result in blinding security and monitoring tool. In addition, new regulations and standards have been set by the Federal Government, the ITU (a government organization responsible for information communication and technology issues), and the IEEE which may affect how Cloud Computing is implemented.

The need for rapid evaluation and deployment of network security solutions has become a vital part of our national and corporate welfare and security. There is a need for more optimized approach to accelerate the validation process and deployment of best-of-breed network security solutions in layers to reduce the time-to-protection against cyber-threats, increase network visibility, and lower the cost of operations.

Challenges around Network Security and Monitoring

Sophisticated Cyber-Threats

While cyber-threat counter measures continue to evolve, more effective network defense layers such inline Advanced Persistent Threat (APT) prevention solutions, Next Generation IPSs (NGIPS), and Next-Generation Firewalls (NGFW) that can be deployed either in proxy or transparent inline (layer 2) type of deployment are essential. As a result, the need for organizations to rapidly evaluate and deploy multiple network security tools in layers has become even more crucial in meeting the increasing complex challenges of cyber security today.

Shrinking Security Budgets

Security budgets have continued to shrink, increasing the importance of maximizing ROI from current investments by extending the life of monitoring and security tools. Networks at the same time however, are expanding to 10G data rates, creating the perceived-need to update existing 1G security and monitoring tools with 10G replacements.

Network Architecture

Network architectures have changed drastically due to the further adoption of tunneling protocols. Similar to Multiprotocol Label Switching (MPLS), GRE's rapid adoption of SaaS by business units are blinding security and monitoring tools.

Despite all these challenges and the increasing level of network saturation and congestions with VoIP, Video, and Social Networking, enterprises still need to meet their respective service level agreements.

Network Security and Monitoring Needs

Today, network security and monitoring tools need to achieve more complete visibility across the enterprise, which requires that every network security and monitoring tool has secure access to the traffic data, either in-line or through SPAN or Mirror Ports. To address this need, traditional monitoring systems provide a solution with a high cost as well as a high degree of risk for deploying multiple network security tools in-line one after another.

1. WHY POCs ARE CRITICAL STEPS FOR EVALUATING AND ADOPTING NETWORK-SECURITY SOLUTIONS

In the early stages of a product life cycle, the most likely question a customer will ask is, "Why should I change what I currently do, and buy a particular product or service?" The customer needs to be convinced that the perceived value from a particular product not only meets their business and technical requirement but it also outweighs any potential risk it can introduce to their environment upon making such change.

In the later stages of the product life cycle, when market demand is established, the primary question from the customer shifts to, "Why should I buy a particular solution from Vendor A rather than a competitive alternative from Vendor B?" At that point, it is about competitive differentiation and providing relevant product information to the customer which convinces them as to why they should buy the solution from one vendor vs. the other.

A Proof of Concept (POC) requires an agreed upon set of proofs or tests that define criteria for success. Proof requirements are generally agreed upon and documented after the vision-scope document is completed and before solution definition occurs. The proof requirements are used to drive the POC solution design and to manage project scope during subsequent phases of the POC. It is used as both a reference and a driver for the proof presentation and documentation, and can also be used to record results against each required proof.

POCs are a key validation tool to demonstrate solutions in a customer setting, but they do introduce some risk. For example, deploying an in-line device in a mission-critical network is fraught with danger from the perspective of both the customer and the sales agent, potentially resulting in outage or downtime.

Although a POC is essential for evaluating network security, it can be time consuming and offer potential associated risks to the network environment. For this reason, POCs are often performed in isolated network segments with limited access to real network traffic. In some cases, enterprises have set up real network traffic validation labs to perform continuous POCs.

VSS Monitoring Allows Rapid Performance of One or More Security POCs in Parallel

VSS Monitoring enables enterprises to continuously validate network security solutions. POCs can be carried out in a predictable manner to evaluate the desired functionality without the risk of a potential outage or downtime. It allows a more comprehensive and compelling proof of concept or even multiple POCs at the same time to take place with minimized change requirements and virtually no disruption to

the network. It further enables the customer to validate network security tools and business processes with either a subset of their live traffic or a copy of the traffic. This capability reduces the level of uncertainty when customers need to move intended security tools from POC environment to production.

Deploying VSS' Protector Series allows the customer to test several security solutions at the same time, individually or in groups; as well as providing a simple future expansion path if a VSS Monitoring customer has one product and wants to evaluate more. The inherent value that VSS brings is that it enables the shortening of the POC cycle; thus also shortening the tool validation and purchase cycle and ultimately speeding the technology adoption phase. By reducing customer fears that can occur when evaluating in-line security tools, the validation cycle is quickened and the number and length of technical resources required to manage and execute POCs on both sides of the table are reduced.

The Key Advantage of the VSS Protector

VSS Monitoring's Protector Series allows network operations engineers to confidently place security and monitoring tools in-line and out-of band with little effort and no re-wiring. This speeds the tool validation process during POCs, reduces the network change management overhead and the potential risk of network outages associated with testing new inline security tools. VSS Protector Series help increase network operations confidence when deploying new inline security technology (e.g. IPS, APT Systems).



2. BACKGROUND TECHNOLOGY: NEW PARADIGM IN EVALUATING AND DEPLOYING MULTIPLE SECURITY AND MONITORING TOOLS

With the advent of more capable and intelligent traffic capture tools, network security and monitoring is undergoing a paradigm shift from expensive and inefficient 1:1 stand-alone approach to a distributed traffic capture and optimized delivery model. VSS Network Intelligence Optimization solution is an intelligent system-based traffic capture solution powered by purpose-built hardware called vNodes using a distributed traffic capture and processing engine known as vEngine. These vNodes are intelligently interconnected using a full mesh topology (vMesh) that is both self-aware and self-healing. Together this architecture is known as VSS IntelliScale™ Architecture which offers a new Network Intelligence Optimization layer that meshes agnostically to the underlying communication and switching network, providing universal access for monitoring systems and security tools. VSS Monitoring Innovative Solution

The effectiveness of any network security or monitoring system is intertwined with the physical network architecture in which it is deployed. The network architecture drives performance of the security and monitoring tools. The traditional deployment has greatly limited tool efficiency and scalability. In order for a network security and monitoring solution to operate at peak effectiveness it must have complete and secure physical access; allowing total visibility of all critical links and, most importantly, to be fully leveraged in relation to the network.

VSS IntelliScale™ Architecture provides a never before seen level of optimization for network intelligence tools. VSS's unique and innovative approach fundamentally improves tool capability and price-performance to help network managers and Information Security teams to work together and face the increasingly urgent and complex challenges in network security and monitoring and proactively protect large-scale networks.

Additionally, the VSS Protector Series offer the much needed inline bypass protection, speed and media conversion and layer-2 session-aware load-balancing to optimize and protect in-line security tools such as IPSs with ultra low-latency and high-availability for security tools with no single point of failure for these tools. VSS solutions offer complete network visibility and optimize network intelligence tools while enhancing operational efficiency and offering a much more immediate ROI.

3. PROBLEM: EVALUATING SYSTEMS FROM A SINGLE POINT IN THE NETWORK OFFERS LIMITED VISIBILITY

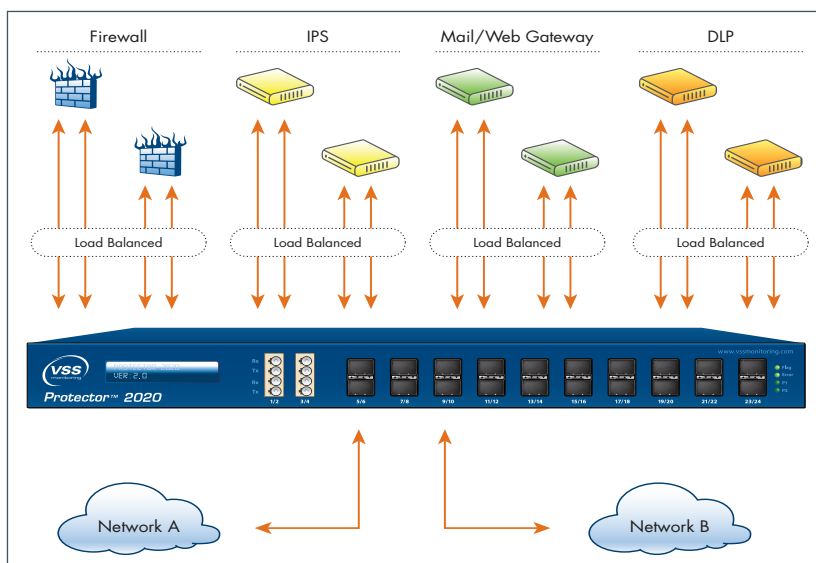
Evaluating in-line security tools one at a time is expensive, time consuming, and delays technology adoption while also delaying the ability to protect against cyber threats.

- Many devices and technologies compete for network access at a single network choke point.
- Network security and monitoring systems are overloaded with traffic that is of minimal interest or that the system is not tuned for.

- Installation of in-line devices typically requires outage windows and adds risk to an environment, while adding complexity to the physical layer infrastructure.

The problem of restricted visibility and inability to see the network traffic in any part or all of the largest distributed networks is a primary concern. Network visibility is the critical factor in heading off the increasing number of application performance issues, outages, and data breaches caused by persistent cyber

attacks. Network expansion is vital in accommodating growth in the number of users and the implementation of Ethernet speeds to 40Gbps and beyond. Meeting the requirements of market standards and regulatory bodies also requires increased flexibility and performance in network security systems afforded by



VSS monitoring. For these reasons, total visibility is the only way to achieve complete and proactive network control which maximizes network efficiency and optimization potential.

In comparison, one-to-one in-line traditional network taps are a direct way to capture traffic without the limitations of SPAN ports but they can present their own problems. That is, traditional taps and 1:1 inline bypass Fail Open kits have not had the desired range of port densities and intelligence—such as selective aggregation, traffic filtering, load balancing, and distributed management features needed to ensure both operational efficiency and service assurance. Instead customers have to rely on performing costly and time consuming data-center and network closet physical audits to ensure that these 1:1 taps and inline bypass fail open kits are functioning properly and not stuck in a zombie state.

Another problem is that if multiple taps are connected i.e. Daisy chained, and each tap may require that it be managed separately. If one tap fails, the entire traffic capture system may fail. In addition high-speed 10Gbps taps may not have the port density (low or high) required for a given deployment. In gigabit copper networks, where a tap cannot be completely passive due to both sides of a link transmitting simultaneously, a tap can cause network link failure in the event of tap power loss and restore.

Traditional security monitoring systems offer solutions for evaluating security systems that result in limited network visibility by not offering a centralized view over a LAN or WAN down to Layer 2. Since service level agreements for real-time applications such as video, VoIP, financial transactions, and other critical applications cannot be assured, enterprises cannot comply with regulations that require a true and complete copy of transactions and lawful intercepts. This situation is exacerbated by the need to use existing Gigabit monitoring infrastructure for cost reasons even as 10Gbps switches continue to be rolled out at the core and access layers.

4. SOLUTION: EVALUATING MULTIPLE SECURITY TOOLS IN PARALLEL WITH VSS NETWORK INTELLIGENCE OPTIMIZATION SYSTEMS

The VSS Monitoring’s innovative IntelliScale™ Architecture offers a highly scalable Network Intelligence Optimization Layer that allows for evaluation of one or more passive network security systems at once across physical boundaries over LAN, WAN and the Cloud.

Furthermore, VSS Protector Series™ offer hardware-based traffic grooming, selective aggregation, and session-aware load balancing for both passive and active in-line monitoring and security tools. These capabilities facilitate optimized evaluation of both in-line and passive network security tools by enabling optimized Proof of Concept (POC) cycles that require minimized operational overhead and reduced risk to network environments and security systems. The Protector Series™ appliances are session-aware load balancers and speed converters for in-line active and Passive network security and monitoring tools including intrusion prevention systems (IPS) and IDS, DLP, and Email/Web Gateways along with Network Forensic systems.

Overview of VSS Network Intelligence Optimization Systems.

VSS Monitoring’s IntelliScale™ Architecture and Network Intelligence Optimization Systems form a highly scalable layer between network infrastructure and analytical and security tools. Today, the IntelliScale™ Architecture allows for up to 63 vNode appliances to be interconnected and operate as one scalable network intelligence optimization system.

VSS Monitoring offers a complete portfolio of Network Intelligence Optimization Systems, traditional simple taps, and an innovative system of intelligent in-line bypass systems (Protector Series™) and advanced DPI sensors. VSS delivers optimized network visibility, enhanced network performance

and increased tool efficiency and high-availability that are essential for critical network security and monitoring tools while reducing their associated CAPEX and OPEX.

For passive monitoring, the purpose-built vNode appliance collects a copy of the network traffic either via in-line taps or from switch SPAN/Mirror ports at capture points anywhere across your LAN, WAN or the Cloud. It then grooms traffic and distributes it to any network monitoring and security device connected to the system. The grooming operations include selective aggregation, highly-granular hardware-based filtering on layers 2 to 7, packet slicing, session-aware load-balancing, and port and time stamping. These grooming and optimization operations ensure that each monitor tool receives only the traffic of interest to its function. These operations occur in real time and solely in hardware.

For active in-line security and monitoring tools as well as passive tool, the Protector Series™ appliance directs the traffic from in-line port pairs to in-line monitor ports while offering secure bypass functionality, enabling traffic grooming, selective aggregation, and session-aware load balancing. Protector Series™ appliances also provide high-availability and fault tolerance for the in-line active and passive network security and monitoring tools.

Benefits of Evaluating Security Systems and Optimized Proof of Concepts with the VSS Solution

This section discusses some of the benefits that the VSS solution provides, which address present and future network security challenges.

Reduced Time to Protection Against Cyber Threats

VSS Network Intelligence optimization System enable the rapid validation and confident deployment of Network Security and Monitoring solutions at the speed of business, enabling faster validation and adoption of disruptive cybersecurity technology in government, financial, healthcare and enterprise environments alike.

Reduced Cost of POCs

The VSS solution reduces the total cost of POC associated with evaluating security and monitoring tools by running

Estimated Average Hourly Cost (Total Compensation) Per POC Cycle for a single Security Tool	Full Time Employee	Contractor
Project Manager	\$70	\$150
Information Security Analyst / Architect	\$90	\$185
Network Engineer/Net Ops	\$80	\$165
Average duration of a POC for Security tools : 3 weeks to 3 months		
Estimated POC Cost for each Security Tool: \$28,800 to \$360,000		

multiple POCs for both in-line active, and passive monitoring security solutions in parallel. This reduces the cost of POC for evaluating security tools, including operational overhead, change management cost, IT and network Ops resources, vendor management, purchasing, and technical resources. The following table shows an estimated average cost for running POC for each security tool.

Reduced Change Management Overhead

In a traditional enterprise distributed network, different sets of tools are scattered across the network in numerous physical locations. Each vendor's tools have their own suite of management software, which is often not compatible with that of other vendors. If a network configuration change is needed, the management, reconfiguration and updating of this large number of devices would be substantial. VSS solutions enable users to share network tools locally or over the cloud; ultimately reducing the number of tools needed for optimal monitoring and security. Fewer devices mean fewer configurations needed, and fewer service contracts to maintain.

Reduced Risk

VSS Protector Series allows transparent network testing and validation of security tools using live traffic to efficiently transition from POC to production, while reducing potential risks to network and service availability. The installation of an in-line device typically requires an outage window and adds risk to an environment's physical layer via additional infrastructure complexity. The VSS Protector allows in-line devices to be integrated into an environment via software configuration rather than through physical cabling, greatly reducing time and risk

Optimized In-Line Security Tools and Reduced Latency

VSS Monitoring's Protector allows for the testing, validation, and optimization of the latency associated with in-line security tools. Leveraging the Protector's intelligent hardware-based filtering one can send only the traffic of interest to each tool or security layer. This results in optimal performance of the tool while reducing its latency.

VSS Contributing Technologies to Security Challenges: Proof Points

The following are specific VSS innovative technologies that enable optimized POCs for evaluating and optimizing active and passive Network Intelligence tools:

Selective Aggregation

Traditional network taps offer static aggregation that does not allow for configuration of the aggregated network traffic to each monitor port. In contrast, VSS Monitoring systems provide selective aggregation, enabling the user to map the

flow of traffic from each network input port, or group of input ports, to each monitor output port, or group of output ports. This presents each monitor port with an independent and completely selectable view of the network access points.

Session-Aware Load Balancing

The distribution of traffic across groups of inline security tools i.e. IPS systems can be defined by the user so that session consistency is maintained for each tool. Once session criteria have been defined, the traffic is automatically (dynamically) load balanced across the inline monitor ports. In the event of link failure to a tool in a load balanced group, the traffic will redistribute across remaining ports in the group. A failover policy can also be implemented where traffic would be sent to a designated redundant tool.

Hardware-Based Filtering

Hardware-based Filtering allows users to specify what type of traffic is to be copied or redirected (in case of active in-line traffic) from the network ports to the monitoring ports based on Layer 2-7 specifications.

Inline Tool Redundancy

N+N options for tool redundancy can be implemented through either session-aware load balancing or user-defined failover actions, where, in the event of primary tool failure, traffic is directed to a backup tool.

Network Bypass

In event of total inline tool failure, i.e. IPS Sensor, the Protector can bypass the inline tool and allow traffic to flow uninspected or it can close the network traffic stream to prevent uninspected traffic from continuing through the network.

Centralized Integrated Management

The VSS Monitoring solution identifies network taps not as a single device on a per box basis, but rather as a network-wide platform of distributed intelligent devices which are acting as a single system for traffic capture. The VSS solution framework separates the monitoring tools from the network communication and switching infrastructure by creating a single traffic-capture and optimized delivery layer that is universal to all tools.

Intelligent Stacking

VSS Monitoring's vMesh architecture offers a fault-tolerant approach for optimizing network intelligence by allowing traffic-capture appliances (vNodes) to be deployed in a fully-distributed mesh configuration. This eliminates a single point of failure in traffic capture and ensures optimum delivery of the traffic captured to a central location for analysis.

Policy-Based Triggering

In addition to monitoring the state of the inline (e.g. IPS) tools, users can select from and define additional policies for triggering actions to be taken by the Protector Series™. Triggering can be set for events such as link/port activity, power supply status, health (using custom crafted health-check packets) of the inline tool (not just outright failure), or status of another interconnected Protector, and a variety of trigger actions can be defined based on one or more trigger conditions being true or false. This unique capability from VSS offers customers a much higher level of service assurance for their inline security tools. The ability to define both positive and negative state health checks for inline tools eliminates the need for performing costly and time consuming data-center and network closet physical audits to ensure that unintelligent 1:1 taps and unmanaged inline bypass fail open kits are functioning properly and not stuck in a zombie state.

Trigger conditions include:	Trigger actions include any combination of:
<ul style="list-style-type: none"> ▪ Any port/link status ▪ Any port utilization ▪ Unit power ▪ Unit temperature ▪ Heartbeat packet (testing both positive & negative state of the inline tool) ▪ Combination of triggers 	<ul style="list-style-type: none"> ▪ Block Traffic (closed) ▪ Move to other tool(s) ▪ Write to Syslog ▪ Illuminate front panel LED ▪ Force specific ports down

5. CONCLUSION

VSS Monitoring enables you to architect and speed deployments for highly-scalable and fault tolerant Defense-in-Layer solutions by validating best-of-breed network security solutions at the speed of business and proactively combat emergent and ever evolving cyber threats.

The VSS Protector Series™ offers a solution to protect your network from in-line tool failures via its innovative in-line bypass capabilities and helps maximize your ROI and overcome the cost and risks associated with the evaluation and deployment of network inline network security and monitoring tools. Furthermore, the network and monitoring ports on VSS Network Intelligence Optimization Systems (*vNodes*) have no IP-stack and thus helping you also protect your tools from the network, i.e. from DDoS attacks.

Customers now have a viable and highly scalable alternative for optimizing Network Intelligence with VSS Monitoring *IntelliScale™ Architecture*. VSS' innovative *IntelliScale™ Architecture* has been uniquely designed in The United States from the ground up by network intelligence and optimization experts.



Network Visibility. Optimized.

USA
 (Corporate HQ)
 + 1 650 697 8770 phone
 + 1 650 697 8779 fax
 1850 Gateway Drive - Suite 500
 San Mateo, CA 94404
 USA
www.vssmonitoring.com

Japan
 + 81 422 26-8831 phone
 + 81 422 26-8832 fax
 T's Loft 3F, 1-1-9,
 Nishikubo, Musashino,
 Tokyo, 180-0013
 Japan
www.vssmonitoring.co.jp

China
 + 86 10 6563-7771 phone
 + 86 10 6563-7775 fax
 C519, 5 Floor,
 CBD International Tower
 16 Yong'An Dong Li,
 Beijing, China 100022
www.vssmonitoring.com.cn

VSS Monitoring, Inc. is the world's leading innovator of Distributed Traffic Capture Systems and network taps, focused on meeting the rapidly evolving requirements of security and performance conscious network professionals. Distributed Traffic Capture Systems herald a new architecture of network monitoring, one which fundamentally improves its capability and price-performance.

VSS, Distributed Traffic Capture System, vAssure, vStack+, and LinkSafe are trademarks or registered trademarks of VSS Monitoring, Inc. in the United States and other countries. Any other trademarks contained herein are the property of their respective owners.