Case Profile

About the Company
Company: Application Service Provider
Application: Primarily security, but includes protocol analysis
Size: Medium to Large
Architecture: Inline and Span
Drivers: PCI compliance

Background
ASP-Co is an US based application service provider with an internationally distributed user population and a broad presence that spans 7 data centers in 4 countries. ASP-Co hosts a number of online application offerings that penetrate several key markets including home users, small businesses, large enterprise environments and government entities.

Due to the diverse nature of ASP-Co’s growing client base, a wide variety of sensitive data flows through its information systems. Organizationally, ASP-Co is in a growth stage and only recently begun the development of their formal information security program. The security team’s first formal task was to architect a scalable network security-monitoring infrastructure.

ASP-Co entered the first quarter of 2006 and found itself confronted by a new business driver known as Compulsory Regulatory Compliance. Specific mandates came by the names of PCI (Payment Card Industry) & Sarbanes-Oxley. While Sarbanes-Oxley non-compliance involved fiscal repercussions, legislative requirements were opaque with regard to technical measures. PCI, on the other hand, contains clear and quantifiable technical requirements (as well as serious non-conformance penalties) that demanded a direct and active response. Consequently, PCI compliance became the primary objective of information security deployment.

Application Service Provider (ASP-Co) uses VSS Distributed Taps to meet PCI Compliance Mandates

Customer Challenges

The Tech-Level Manager

ASP-Co’s Information Security initiatives were supported by the traditional “Fear, Uncertainty, Doubt” and “Best Practice” security drivers. With their regulatory based financial penalties being integrated into their threat model, ASP-Co found that their traditional business drivers were suddenly displaced by a hard business driver known as PCI compliance.

ASP-Co chose to deploy a Cisco SAFE style multi-tiered service provider hosting architecture for their data center environments.

While the ASP-Co model was designed to have a high meantime between failures (MTBF), the architecture displayed a distinct focus on Availability & Scalability information security monitoring and countermeasures. In terms of PCI compliance, architecture had achieved an appropriate security posture. However, the ability to perform incident response and security event monitoring was a requirement that needed to be addressed.

With fault tolerance remaining a critical component for ASP-Co’s new infrastructure, the information security team outlined a series of technologies that ASP-Co would be required to integrate into their hosting environments. These various technologies would allow ASP-Co to meet the needs of the various compliance bodies in addition to meeting their own internal best practice requirements.

The Security Engineer

ASP-Co’s compliance & security based business needs required the creation of an extensible and reliable network-monitoring system. Furthermore, the information security system had to be orthogonal to the online application-hosting environment. This meant traditional monitoring/troubleshooting technologies such as remote spanning (RSPAN) and VLAN access control lists could not be used to gather the security relevant data. While the chosen technology must support security needs, it must also support the network team’s service level agreement of 5-9s (%.99999) uptime.

Customer Requirements

The Network and Security teams generated a set of requirements vendors would need to meet before ASP-Co would sponsor a proof-of-concept for any products:

- All network gear placed within ASP-Co’s hosting environments must be Fault Tolerant (i.e. dual-powered, have the option to fail-open or fail-closed, and have the ability to intelligently failover when necessary).
- In order for a network monitoring infrastructure to be useful to ASP-Co, both the network and security teams require total network visibility which operationally means the ability to monitor all critical segments within of ASP-Co’s hosting environments.
- The network access solution must have the ability to support a multitude of monitoring technologies from a single, centralized point of access.
Lastly, the vendor of choice must bring to market a compelling value proposition in terms of economies of scale via cutting edge technologies.

Furthermore, whatever the solution chosen; it must support all of the following technologies.
- Network Behavior Anomaly Detection system
- Application (layer 7) Signature Based IDS
- Network Flight Recorder
- Traditional packet capture or “sniffer” technologies such as Wireshark or tcpdump.

In terms of network design, ASP-Co had 10 internal as well as two external network segments to monitor within a Cisco 6500 Active/Active fault tolerant network environment.

Given the series of business and technical requirements put forth by the ASP-Co, the search for a market leader in network monitoring access infrastructure led to several potential solutions.

Alternatives Considered
Alt-Vendor offered a series of inline wire access technologies that required one physical tap device per collection point, accruing a total of 26 tap devices (two per unit of space) to monitor a single ASP-Co Data Center environment. Furthermore, Alt-Vendor did not support data aggregation technology or span port replication. Each tap interface would need to use one NIC per tap on each monitoring device.

While the Alt-Vendor architecture permitted the monitoring of a single instance of a network monitoring system, it did not support span port replication or offer multiple traffic feeds to the series of network monitoring and security technologies required by ASP-Co. The tap solution created 26 potential fault points within the ASP-Co’s network environment. With respect to the regulatory and compliance requirements mandated by the PCI Standard, the Alt-Vendor’s solution offered the ability to view most critical network segments, however, without enough monitor feeds, pertinent security systems would still be excluded.

Due to Alt-Vendor’s many-device architecture and lack of central tap management, troubleshooting network issues would become a costly human resource game of chance rather than a proven, repeatable, technical process.

In terms of power utilization and rack-space cost, Alt-Vendor’s solution required a dedicated 120amp feed as well as a dedicated cabinet to house the many tap devices.

Network and security implications, coupled with a high total cost of ownership, proved the Alt-Vendor’s solution in-feasible for ASP-Co. Consequently, the solution was disqualified.

VSS Solution
Leveraging VSS’ advanced inline tap and port replication technologies, only seven traffic collection devices would be required per datacenter.

All SPAN replication traffic was managed on a single 10/100/1000 12x4 Distributed Tap; external traffic was gathered on two gigabit fiber taps that replicated each network to two aggregated outputs; and the internal inline networks were collected with three 12x4 Distributed Taps. The top-tier device – a fifth 12x4 Distributed Tap – functioned as the primary aggregation and replication feed for the network and security monitoring systems. This architecture allowed for all internal data aggregation to be managed on a total of seven 12x4 Distributed Taps across all ASP-Co datacenters.

The VSS tap and replication solution enabled immediate response time for network outages and incidents. The fault-tolerant architecture paired with technical capacity to monitor all network segments from a central point provided ASP-Co complete 24/7 visibility into the ASP-Co’s host environment. Thanks to VSS’ user-friendly GUI-based method of remote tap access and management, ASP-Co was also able to minimize human resource utilization as well as limit human errors when addressing network and security issues. Troubleshooting that once took 3 network engineers and a multitude of changes to the environment was now handled by a single engineer with no environment changes and a scripted process. The time to troubleshoot network faults was cut by 75% due to the network data being aggregated in a single point of entry.

Through the port density found in the 12x4 aggregation taps and the efficient power utilization in all of the VSS devices, the monitoring infrastructure used minimal rack space and consumed minimal power all the while remaining fault-tolerant with open port space for future network expansion.

The VSS solution enabled ASP-Co to develop a compliance strategy that addressed the network monitoring requirements of the PCI standard. ASP-Co’s requisite internal network and security needs were met in a scalable, secure and cost effective manner.

Solution Benefits
Flexibility
VSS Distributed Taps can collect and aggregate both inline and span traffic. They can also be cascaded to create a flexible and easy to adopt traffic collection solution.

Visibility
Network managers have total visibility into multiple networks via a combination of span and inline monitoring ports with any monitoring tools of choice.
**Improved Response time**
Solution allows for easy access to all data streams from a central location—at any time—without the need to locally troubleshoot. Clickable reconfiguration options vastly improve response time.

**Remote manageability**
Each deployed network is manageable from a remote, central location.

**Scalability**
Additional Distributed Taps can be added to the solution in a similar configuration to allow for future growth.

**Cost Savings**
Remote management eliminates the cost of dispatching technicians to monitor equipment or change cabling at a remote location. The ability to aggregate traffic also eliminates the need for multiple analyzers and/or NICs.

---

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

VSS Monitoring is a world leader in network packet brokers (NPB), providing a visionary, unique systems approach to integrating network switching and the broad ecosystem of network analytics, security, and monitoring tools.

VSS Monitoring, the VSS Monitoring logo, vBroker Series, Distributed Series, vProtector Series, Finder Series, TAP Series, vMC, vAssure, LinkSafe, vStack+, vMesh, vSlice, vCapacity, vSpool, vNetConnect and PowerSafe are trademarks of VSS Monitoring, Inc. in the United States and other countries. Any other trademarks contained herein are the property of their respective owners.