ROI Experiences with Network Monitoring Switches – Managed Security Services Provider

Executive Summary

As network service traffic continues to grow, network-based security, performance and compliance monitoring become increasingly critical. But that doesn't mean the cost of network operations, and in particular the cost of monitoring, has to grow needlessly. Network monitoring switches offer compelling options for consolidating monitoring tools and architectures and can deliver significant CAPEX and OPEX savings over the status quo of deploying more and more security and network monitoring tools. This case study reviews an implementation of network monitoring switches – Anue Net Tool Optimizers (NTOs) – by a provider of enterprise-class Unified Threat Management (UTM) services, detailing experiences and expectations regarding both short- and long-term returns on those investments.

Challenges

As a full-service business communications provider, this organization brings many different communications services products to the market, both within North America and worldwide. One of those services is a managed security service, consisting primarily of firewall monitoring but also including monitoring of broader UTM deployments. UTM deployments can include intrusion prevention systems, Web application firewalls, and proxy servers – often a number of separate appliances in addition to traditional firewalls.

The provider enters into service-level agreements regarding the efficiency and quality of firewall throughput. When a customer has a problem and thinks that the problem resides within the security system, it is up to the provider's operations team to determine whether this is the case and to provide conclusive evidence back to the customer/subscriber. Penalties associated with service disruptions are significant enough that the provider assigns staff to be on-call to troubleshoot issues as they arise.

> The UTM services provider must assure that security measures are enforced without negatively impacting legitimate traffic flows

The lead manager and two of his engineering team members described the problem that they faced: "Before we deployed the Anue solution, we were collecting TCP dumps to UNIX boxes and using custom scripting to try and compare traffic on each side of the firewall. In many cases, inserting a TAP or SPAN during a network event would require a scheduled maintenance window. Ultimately, we took service penalty hits because it took a long time to identify and resolve the issue."

The provider deployed Network Instruments TAPs and GigaStor monitoring devices for capturing and analyzing the packet streams on both sides of each firewall. They also chose Anue Net Tool Optimizer (NTO) 5200-series network monitoring switches to provide connectivity for the monitoring tools. This allowed the team to gather and compare packet traces from multiple points around the UTM environment. Without the NTO in place, it would have been necessary to purchase and deploy far more GigaStor packet monitors, just to properly cover all of the potential links that might be needed when a service incident arose. The manager estimated current deployment costs per service site to be about $150,000, including the NTO and Network Instruments equipment.

Solution

In terms of cost savings, according to the manager, the NTO solution saved "several hundred thousand dollars" in additional 10Gbps ports that would have been needed for the monitoring devices. With the new instrumentation in place, enabled by the Anue NTO solution, the team has been able to substantially accelerate average troubleshooting and analysis time.

"In the past, it often took us two to three days working with the vendor to identify the source of an issue and implement a code patch," said the manager. "We have reduced that time from days to hours. Penalties from problems with the services have run as high as $100,000 for a single event, and we hope to save half of those charges with the new approach."

There were additional cost savings realized as part of the new deployment. For instance, the team believes that the improved efficiency will give existing Tier 3 engineers availability to support a greater number of overall customer incidents. Also, as the provider is moving towards E911 services that must also pass through its managed firewalls, stakes are rising significantly for both SLA penalties and the provider's reputation. The new monitoring approach will help to balance and minimize such risks.

The Anue NTO solution has also provided some other unexpected benefits. "We have used the NTO to directly help us understand HTTP traffic as we sized a new service. We were able to tune filters directly within the NTO's management interface to get some quick answers. We also see benefit as our sites continue to expand in total capacity and size, allowing us to transition our GigaStors over to 10G speeds on a more gradual, planned basis."

Based on EMA's assessment of expected savings, this provider has conservatively achieved a 1.6x payback on their investment ($250,000 in estimated reduced and saved costs versus roughly $150,000 invested in the total solution, including the Anue NTOs).

Hard and Soft ROI Summary

Hard ROI	After Anue	Approximate Savings
Reduced cost of instrumentation per site	4:1 reduction in number of performance monitoring appliances	$200,000
Reduced SLA penalties	50% drop in average penalties incurred	$50,000
Total Hard ROI		$250,000
Soft ROI	After Anue	Benefits
Improved incident responsiveness	Escalation staff can cover more incidents per engineer	Better customer satisfaction, incrementally lower overhead costs per customer.
Reduced time and risk for new services	Access in place for expanded monitoring and troubleshooting expected for E911 services	Reduces future costs for access and instrumentation, reduces penalty risk for service failures

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook. 2506.071712