Health Information Provider Upgrades Network Security

New solution increases network visibility for security devices, monitoring tools and virtual networks

Summary

Customer: Healthcare Enterprise

Location: USA

Challenge:
- Monitoring the influx of data
- Lack of virtual network monitoring

Solution:
- IntellaFlex XR monitoring system
- IntellaStore II
- Bypass Switch

Benefits:
- Complete network visibility
- Integrated physical and virtual traffic monitoring
- Remote site monitoring

A leading healthcare information services company processes millions of patient and provider records that it must keep secure.

After a detailed internal review, APCON's customer decided to significantly upgrade security in the areas of inline tool visibility and protection, expanding security monitoring with additional tools and gaining virtual network visibility of east-west blind spots.

To gain the visibility needed for their security network upgrade, the healthcare company leveraged APCON's network monitoring solutions.

A comprehensive approach to 100 percent visibility

The healthcare information processing company knew that upgrading the security tools at several locations would require a monitoring solution that would increase network visibility, scale for future growth, and increase efficiency of new and existing tools.

The company purchased APCON's IntellaFlex XR aggregation and filtering switches to increase visibility in both physical and virtual networks. They selected the Bypass Switch to protect its inline devices, the IntellaStore II to monitor traffic at its remote locations, and the HyperEngine packet processor to help monitor traffic in its main data centers.

Protecting Inline Security Systems

The company was looking for better firewalls, intrusion prevention devices and other inline security systems. Adding a bypass switch to its network gave the network engineers the ability to protect the production network when or if one of the inline security tools physically failed, and provided the option of redirecting traffic or load balancing across additional systems.

The network was already able to handle inline security tool hardware failure, but sometimes the software failed even though the hardware was still functional. In that case, the production network was blocked. For a company that processes healthcare data with customer and provider access 24×7, downtime is unacceptable.

With APCON's Bypass Switch in place, inline monitoring tools are no longer a single point of failure on a network. The switch sends a bi-directional heartbeat that confirms a security device is passing traffic normally. If the heartbeat detects a security tool failure, it will automatically bypass that tool or load balance the traffic to remaining systems, and traffic will continue to flow unimpeded through the network. Once in bypass mode, network engineers are alerted and can easily take security systems offline for maintenance.

Virtual Network Visibility

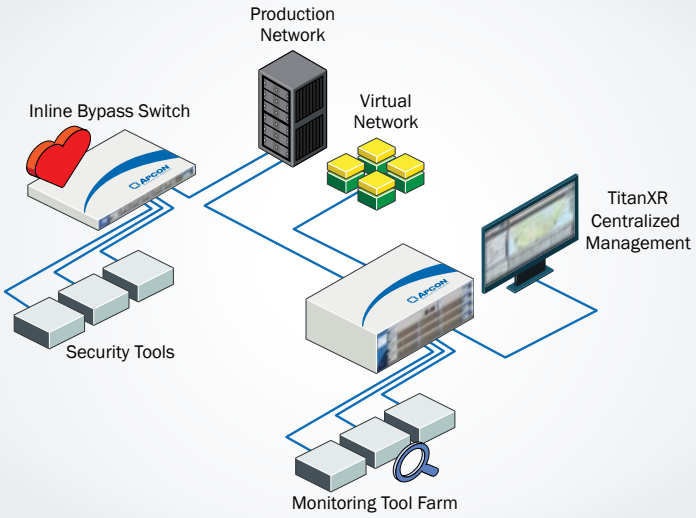
Another major concern was visibility of traffic within the data center's virtual network. Being able to selectively look at east-west VM traffic on-demand was required.

VM traffic of interest was forwarded to the monitoring systems using GRE. The customer selected IntellaStore II for locations where up to 10Gbps of GRE de-capsulation met the requirement, and deployed the HyperEngine at large data centers that can process up to 200Gbps of GRE de-capsulation per blade. After GRE removal, the VM traffic of interest is forwarded to existing security and monitoring tools for analysis. Now the customer uses the same premium tools to analyze both physical and virtual networks.

Packet Deduplication Increases Tool Efficiency

To obtain complete visibility, the monitoring systems connect to hundreds of SPANs and TAPs across the enterprise network and data center. This provides greater visibility, but also results in some duplicate packets that unnecessarily burden monitoring tools and cause reporting errors.

The customer selected APCON's HyperEngine for high speed deduplication. The HyperEngine supports deduplication of up to 200Gbps processing and has a match window size of 1ms to 500ms. The HyperEngine removes duplicate packets to improve monitoring tool efficiency and accuracy.



The healthcare customer upgraded network security with increased visibility, additional tools, virtual network monitoring and inline security system bypass.

Proactive Security Visibility

This healthcare information services provider assessed their current security architecture and decided it was time to upgrade the monitoring network and add security tools.

The key was being proactive, and not waiting for a breach. They determined several areas of their network monitoring infrastructure to update: **(1)** increase visibility across the network, including remote locations, **(2)** enable visibility of east-west traffic, **(3)** monitor inline security tools to be able to direct traffic without network downtime if a tool fails or needs maintenance, and **(4)** include packet deduplication to ensure monitoring tool efficiency.

The APCON IntellaFlex network monitoring family met their needs today, as well as providing scalability to grow with their business.

When planning security upgrades, contact APCON to see how we can help increase network visibility and improve security tool efficiency.