Use Case

Connecting Multiple Security and Monitoring Tools to Critical Links

Agency of the United States Government Chooses Network Critical to Connect Multiple Security and Monitoring Tools in Data Center

Summary

Government agencies are among the top targets of cyber criminals. Motivations for cracking these networks are as diverse as the information they contain. Therefore, it is particularly important for government agencies to understand, utilize and execute industry best practices for network protection and security. To that end, the Federal Information Security Modernization Act (FISMA) has codified information security practices that federal agencies must follow. Continuous Monitoring and Utilization of Security Controls are two FISMA minimum requirements for federal networks that mandate the use of specialized security tools.

The Challenge

A large U.S. government agency is tasked with connecting seven specific security and monitoring tools to network links. Security tools such as sensors, SSL proxies, IPS and firewalls require real time access to live network traffic. Monitoring equipment such as probes, SiLK tools, network analytics, access decoders and others require only a copy of network traffic. Connecting seven independent appliances directly to a single link can severely impact network reliability if any of those tools goes off line for any reason. Further, it is not economically feasible to connect all seven tools directly to every link in a large complex network.

The real time security tools must have live traffic flowing through the tool in order to take immediate remediation action if malicious traffic is identified. These four tools are called the "live stack." Monitoring tools that do not require real time access are called the "passive stack." Both groups of tools, however, need to be connected and receive traffic from the same links. Both groups of tools also need to see 100% of the traffic on the link 100% of the time. SPAN ports are not capable of connecting security tools in the active stack because they only pass a mirror copy of traffic and also may drop packets impacting accuracy of the passive stack information.

> **"Our network requires connection of seven different security and monitoring tools on critical links in order to comply with FISMA regulations. We can't put all these tools on every link. Network Critical TAPs allow us combine links and help us stay within our budget guidelines."**
>
> Information Technology Specialist

Network Critical
The Window to your Network™

> **"We base our deployment on NIST best practices. Using specialized tools to secure our infrastructure and maintain information privacy, our network remains in line with accepted standards. The Network Critical platform allows us to connect all the right tools while maintaining the highest level of reliability."**
>
> Data Management Systems Analyst

Network Critical Solution

Using two independent modular SmartNA-XL TAPs to connect seven tools to a single critical link provides this government agency with the ability to send the right traffic to the right tools at the right time. Network Critical SmartNA-XL is a flexible modular platform that has a variety of access port modules that can be utilized in a common chassis. The agency deploys real time bypass access modules to connect four live stack security tools. All four tools will be connected to the link by a single TAP chassis. Bypass modules take in live traffic, pass the traffic through security tools then back to the network. This allows the tools to take immediate action when needed blocking malicious traffic before damage is done. If any of the tools go off line, the TAP will automatically bypass the tool keeping network traffic flowing.

The three passive stack tools are connected to a SmartNA-XL chassis with a different set of modules that pass a mirror copy of live traffic to the tools. The passive tools will receive 100% of all the traffic on the link including incomplete or retransmitted packets. This allows the tools to provide perfectly accurate traffic data analysis. The SmartNA TAPs also provide fail-safe technology protecting live traffic even if power to the TAPs is lost.

Both the passive and active stacks of tools are accessing traffic from the same link with complete protection against any tool going off line and taking down the link. Different tools with different missions can perform their tasks utilizing the same stream of network traffic.

Solution Benefits

Government agencies are required to provide important services to their internal clients as well as their citizen constituents. As a result, they must be internet accessible while complying with a panoply of privacy and security regulations. Network Critical provides a simple solution for the complex problem of managing these conflicting objectives. The unique flexibility of Network Critical SmartNA-XL TAPs connecting links to a variety of specialized security tools provides the foundation for government regulatory compliance within a government allocated budget without sacrificing the highest standard of network reliability.

About Network Critical

Network Critical is an industry leader in network access technology. Our quality 1/10/25/40/100G modular TAP and Packet Broker solutions ensure that our customers have continuous network visibility. Network Critical products eliminate any concerns of downtime and our unique scale-out capabilities enable simple, cost effective expansion, as network and port density requirements grow.

The health of your network is always secure with Network Critical products. Our fully flexible range of TAPs and Packet Brokers are used with IDS, IPS, network traffic monitoring tools, sniffers and many other mission critical appliances, to provide 100% network visibility with zero packet loss.

With over 20 years experience, a number of industry "firsts" and a reputation for excellent customer service, Network Critical's solutions are widely used in global networks across a wide range of sectors including Finance, Telco, Government, Energy and Healthcare. For more information, visit http://www.networkcritical.com.

For more information, visit www.networkcritical.com

Network Critical
The Window to your Network™

www.networkcritical.com