APPLICATION NOTE

Quick Tips to Improve Network Security

Network security is one of, if not THE, most important topics for anyone in IT. This is true from the security engineer all the way to the chief information security officer (CISO), chief information officer (CIO), and even the chief executive officer (CEO). Everyone wants to improve it. The question though is, “What can you really do to improve it?” One solid answer is to strengthen the deployment of inline security tools. This is critical to an architecture where someone is trying to maximize their defenses and maximize reliability.

Network visibility is the key to the solution. You cannot secure what you cannot see. A network visibility architecture empowers the security engineer with information to quickly isolate security threats, making visibility a central component of network security. This allows you to improve your security architecture activities by:

- Optimizing the availability and reliability of inline security devices
- Isolating and capturing the right kind of data for the security tools to process
- Performing Active SSL decryption for improved data inspection and simplification of the decryption infrastructure
- Improving the efficiency and accuracy of the current security architecture

A visibility architecture is an end-to-end infrastructure which delivers network, application, and security visibility. This visibility is what allows you to optimize your network data capture and analysis techniques. A visibility architecture typically yields immediate benefits like the following: eliminates blind spots, improved data flow to security tools, and maximum network and tool availability.

Overview

This brief reviews techniques to improve network security activities.

Additional Resources:

- How to improve network security Podcast
- Best practices for network monitoring

KEYSIGHT TECHNOLOGIES

There are three layers to a visibility architecture. The first layer is data access. This is where you will want to insert taps and bypass switches into the network between the network data flow and your monitoring tools (or network packet broker) to improve the quality of monitoring data and time to data acquisition. The external bypass switch uses heartbeat messages to communicate directly with inline security tools. Should any security device fail, the bypass switch can automatically fail open or close, depending upon how it is configured. Once the bypass switch detects that the security device is back online (through the use of continual heartbeat message checking), the bypass switch will reinstate a normal flow of operation—no manual intervention is required.

The external bypass switch uses heartbeat messages to communicate directly with inline security tools. Should any security device fail, the bypass switch can automatically fail open or close.

The second layer is the monitoring data manipulation layer. This is where you will want to deploy network packet brokers (NPBs) between those bypass switches or taps and the security and monitoring tools. The packet broker allows you to optimize the data sent to the tools. Once installed, you can perform out-of-band data filtering, SSL/TLS decryption, deduplication, packet slicing, header stripping, and many other functions to optimize the data before it is sent to your monitoring and security appliances. Load balancing and high availability options deliver even more architecture reliability.

The third layer of a visibility architecture consists of the monitoring and security appliances. Examples include intrusion prevention systems (IPS), intrusion detection systems (IDS), web application firewalls (WAF), security information event and management (SIEM), data loss prevention (DLP), etc.

While many organizations have placed an emphasis in the last several years on simply picking the security functions needed and vendor selection, deploying a visibility architecture itself has additional benefits. For instance, once you have your visibility architecture in place, there are several possible ways to optimize your security defenses and workflows. Here are some examples:

- Insert external bypass switches between the network and security tools to improve network availability and reliability during normal operation
- Use external bypass switches instead of internal bypass devices for fast replacement of security devices and/or any associated hardware and software upgrades
- Deploy inline security tools, like an IPS, to inspect incoming data and improve threat detection and isolation without fear of a device failure causing a network failure
- Perform SSL/TLS decryption within an NPB to save time and simplify your security architecture
- Insert network packet brokers to improve security device availability by using either n+1 load balancing or High Availability technology
- Filter out necessary data and distribute it to out-of-band tools (like a DLP) for data packet inspection
- Improve the efficiency of out-of-band security devices, like an IDS, by up to 35% simply by filtering out unnecessary application data being sent to the appliance

Visibility Architecture Solutions from Keysight

In the end, any regulatory compliance strategy is only as good as the quality of data that is being fed to the tools. The most important part of your regulatory compliance plan will be the architecture, as this piece will determine what, if any, policies and procedures are being adhered to.

Keysight's network visibility solution involves using network packet brokers in conjunction with application filtering and taps. Learn more about Keysight's **Taps, Network Packet Brokers, AppStack,** and **Hawkeye** technology along with the solutions that our technical partners offer.

Network visibility solutions allow you to get a better understanding of your security architecture—how it is performing, where potential holes (blind spots) exists, and how you can better optimize your security strategy.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES