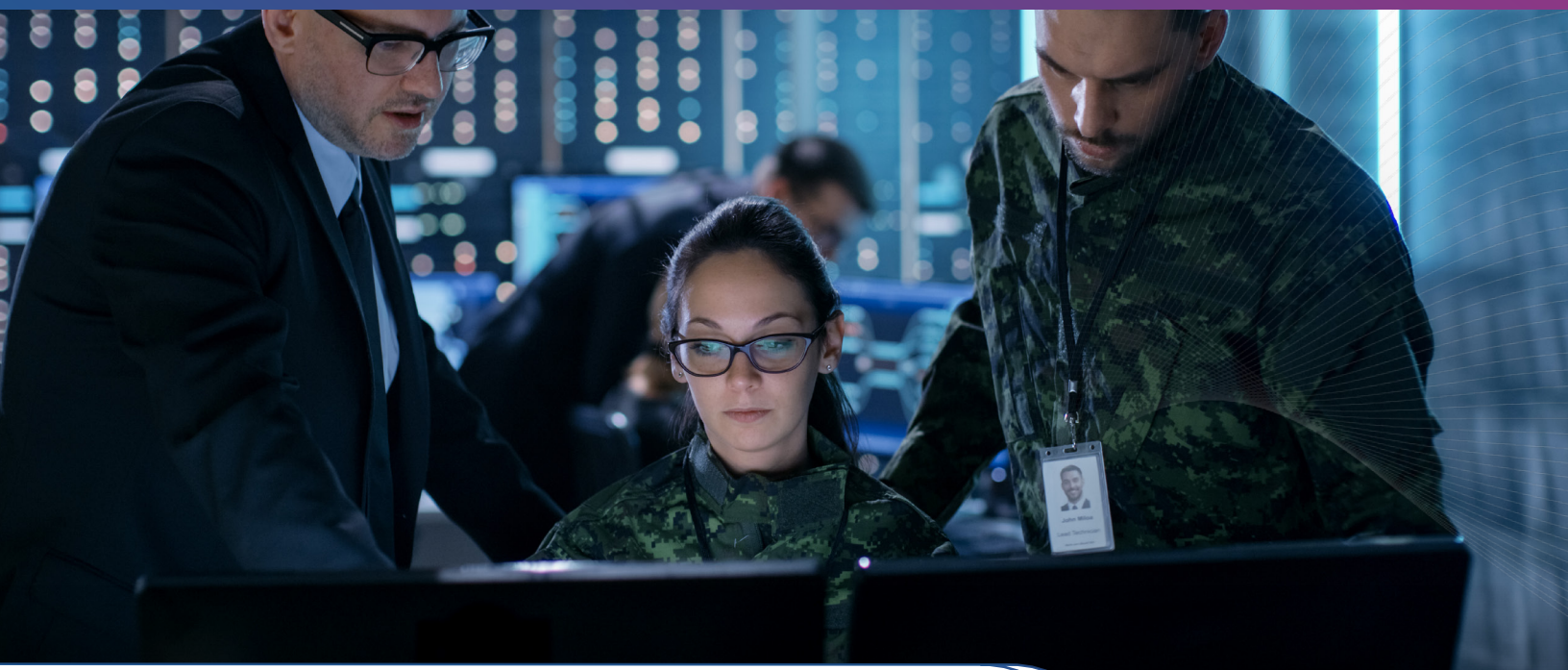

CASE STUDY

Federal Agency Fortifies Its Network Against Cyberattacks

As critical infrastructure becomes more connected and complex, cyberthreats put US security at risk. To address this issue, the National Institute of Standards and Technology (NIST) created a framework to guide organizations in preventing, detecting, and responding to cyberattacks.

In part to comply with the NIST cybersecurity architecture, a US federal government agency instituted a department-wide initiative to achieve notable improvements to its cybersecurity posture. The agency conducted an internal network and risk mitigation assessment for cybersecurity monitoring, threat detection, and automated response capabilities.

As part of this effort, the agency realized the need for enhanced visibility to properly support its security architecture. The project included an evaluation of network packet brokers (NPBs). The goal was to start with an out-of-band deployment and later add inline security monitoring to its architecture. The agency wanted one future-proof solution that would satisfy both objectives.

The customer chose Keysight's Vision ONE series of NPBs and Flex Taps as the solution. The Keysight SecureStack feature set provides Secure Sockets Layer (SSL) / Transport Layer Security (TLS) decryption. Keysight's AppStack feature set provides application-layer filtering and NetFlow offload.

Company:

- US federal agency

Key Issues:

- immediate need to fortify out-of-band network security
- a future-proof solution able to support inline security

Solutions:

- Vision ONE NPBs to filter data to DLPs and IDS
- passive SSL / TLS decryption for improved data inspection
- Flex Taps and iBypass external bypass switch

Results:

- 15% increase in detection of malware
- 20% decrease in mean time to detection of security threats
- simplified data filter creation with GUI

KEYSIGHT TECHNOLOGIES

The Key Issues: Data Visibility and Concurrent Features

At the start of the NPB solution analysis, the customer thought all NPBs were the same and could perform the same functions. The truth ended up being much different. The agency tested the top NPB vendors for performance and throughput and came up with an unexpected result: While the Keysight NPB did not drop any packet data, other NPB vendors did. In addition, those missing packets had a clear impact on the intrusion detection system (IDS) and data loss prevention (DLP) tool. Both of these security appliances missed threats in the non-Keysight NPB scenario. This situation illustrates the primary reason every government agency needs lossless visibility.

The customer also wanted to run multiple features at one time. Some manufacturers can't support running concurrent features. This surprised the agency's engineers. One of the vendors that dropped packets also had a feature-blocking issue. In contrast, the Keysight Vision ONE solution can run all of its features (such as deduplication, header stripping, and NetFlow) concurrently and at full speed, all the way up to 100GE. If you can't use your equipment to its fullest potential, then why buy it?

The Keysight architecture enables the non-blocking capability by using field-programmable gate arrays to process data instead of a CPU running software. The CPU-software combination has inherent issues because every line of code steals bandwidth.

Ease of use

Ease of use was another concern. Again, the customer thought all NPBs were the same — until it saw the Keysight graphical user interface (GUI). The Keysight interface ended up being more than two times faster at creating data filters. In addition, the interface was so intuitive, engineers did not require any training. They clicked, double-clicked, and drew lines from one point to another to create filters. They needed no command line interface or menu-driven interface.

The Solution: Vision ONE NPBs with SSL / TLS Decryption

The solution the customer deployed consists of five Vision ONE packet brokers with the PacketStack feature set, which performs packet deduplication and header stripping for the agency's 10G and 40G links. The customer deployed the SecureStack feature set to provide passive SSL / TLS decryption initially. This capability allows the agency to inspect traffic in its out-of-band configuration.

The customer also deployed the AppStack feature set. It includes support for NetFlow generation, allowing NetFlow to be offloaded from the network Layer 2 and Layer 3 switches. Offloading NetFlow increased performance by close to 25%.

The solution also included Flex Taps and iBypass VHD to perform initial data capture. Since the agency had some legacy links, it needed a mixture of copper and optical interfaces on the taps.

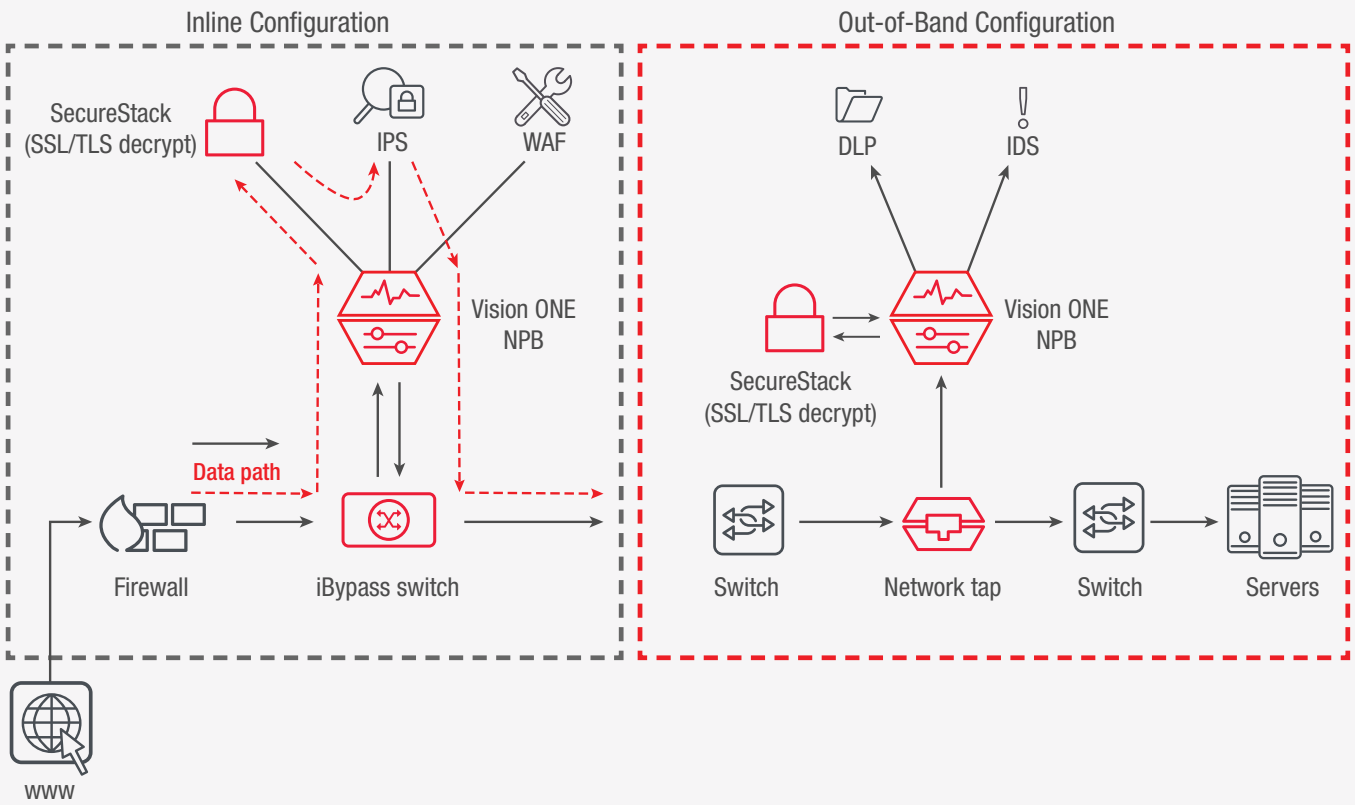

Figure 1. Inline vs Out-of-Band Network Configurations

The Results: More Threats Detected Faster

The ability to decrypt packet data immediately resulted in the detection of 15% more threats and a 20% decrease in time to detection. These threats previously hid within encrypted data, essentially making the agency blind to this type of traffic. Now the security appliances can see all the threats. Once the agency deploys Vision ONE packet brokers inline, SecureStack will be able to provide active (man-in-the-middle) SSL / TLS decryption as well.

“Vision ONE with SSL decryption enabled 100% visibility into the network so that we could see more threats than before,” the agency’s deputy CISO said. “I had a concern that there was a problem but never could access the network the way I needed to isolate and remove the problem. Now I have full control.”

In the end, this federal agency was able to notably increase network security and improve efficiency while reducing programming and maintenance efforts.

Resources

Learn more about Keysight Network Packet Brokers:
https://www.keysight.com/us/en/products/network-visibility/network-packet-brokers.html

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

This information is subject to change without notice. © Keysight Technologies, 2020, Published in USA, July 30, 2020, 7120-1223.EN