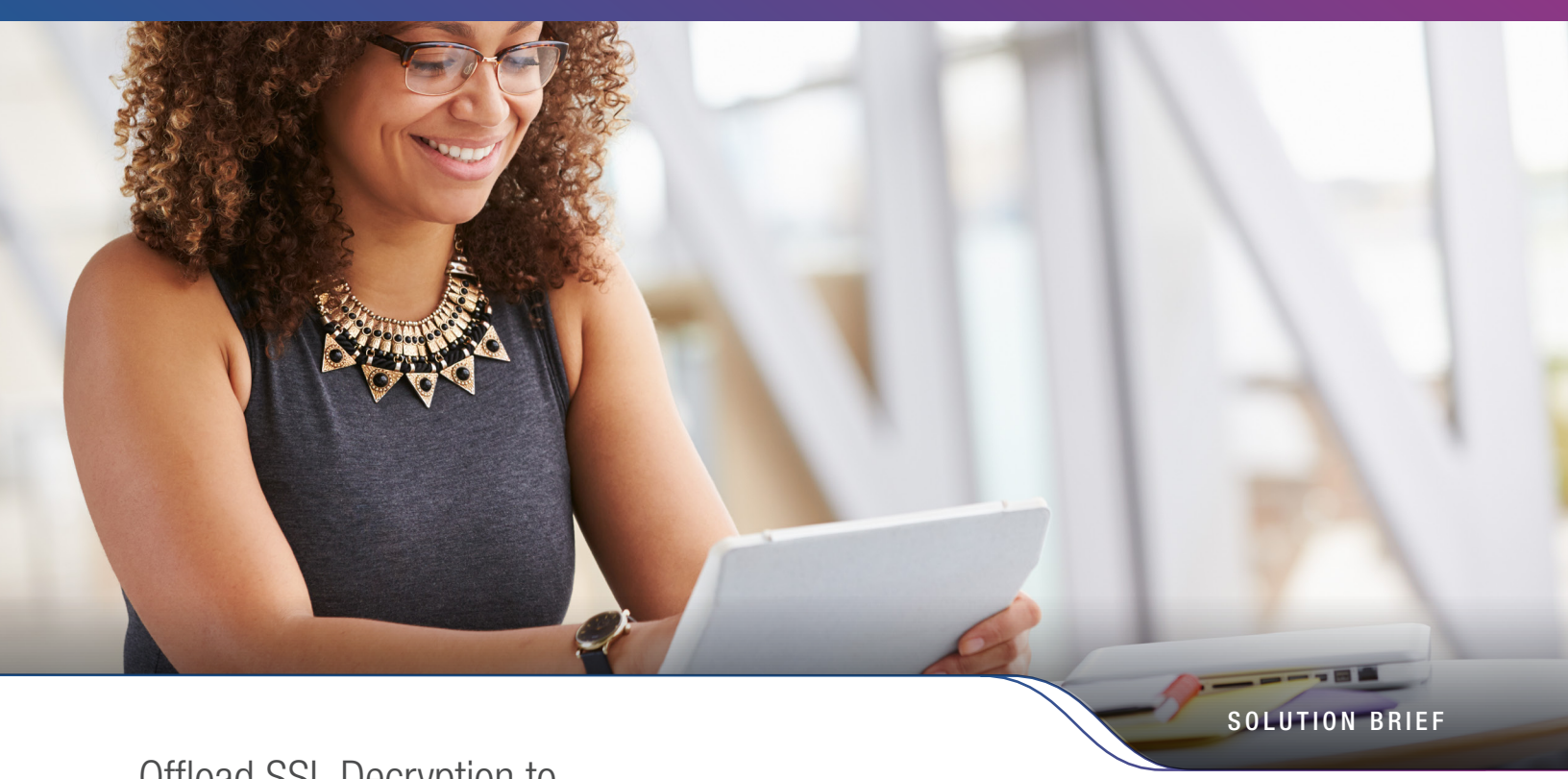


Offload SSL Decryption to Improve Security Tool Performance

Deployment Scenario: Inline Network Visibility

Most enterprise applications are now encrypted using either the secure sockets layer (SSL) standard or its updated version called transport layer security (TLS). While many security tools include the ability to decrypt traffic so that the incoming data can be analyzed for security purposes, this comes at the expense of CPU performance and can dramatically slow (up to 80%) a security appliance's processing capability. One solution is to use a network packet broker (NPB) to offload the SSL functionality to a purpose built decryption device and then forward the unencrypted data to one or more security tools for analysis.

Solution Components:

- Ixia's Network Packet Brokers
- SSL Decryption tool

Benefits

- Increase network efficiency by decrypting data once
- Prevent security tool performance issues due to decryption
- Maximize unencrypted data analysis by using an NPB
- Eliminate decryption appliance port contention by using an NPB

KEYSIGHT TECHNOLOGIES

Solution Overview

This network visibility solution allows you to:

- Reduce the CPU strain on your firewall significantly by offloading CPU-intensive data decryption functions
- Use a network packet broker to pass encrypted traffic and relay that data to dedicated decryption devices
- Improve system traffic latency by decrypting data once

While several types of security appliances (like firewalls, IPS, etc.) include the ability to decrypt traffic so that the incoming data can be analyzed for security purposes, this comes at the expense of CPU performance and can dramatically slow a security appliance's processing capability.

The Value of Offloading SSL Decryption

Payload encryption is a common technique used to thwart security attacks and hackers. Unfortunately, this causes a significant load on the CPU for devices like firewalls, web application firewalls (WAF), intrusion prevention systems (IPS), and other security appliances that have integrated decryption capabilities. The processors for these devices are busy analyzing data packets for security threats like cross-site scripting (XSS), SQL injection, hidden malware, and security threats. When encrypted traffic is encountered, it needs to be decrypted first before that data can be inspected by the security appliance(s). This creates extra loading on the CPU. It can slow the throughput of some devices by 80%, depending on encryption key length, algorithm type, and if re-encryption of the data is needed.

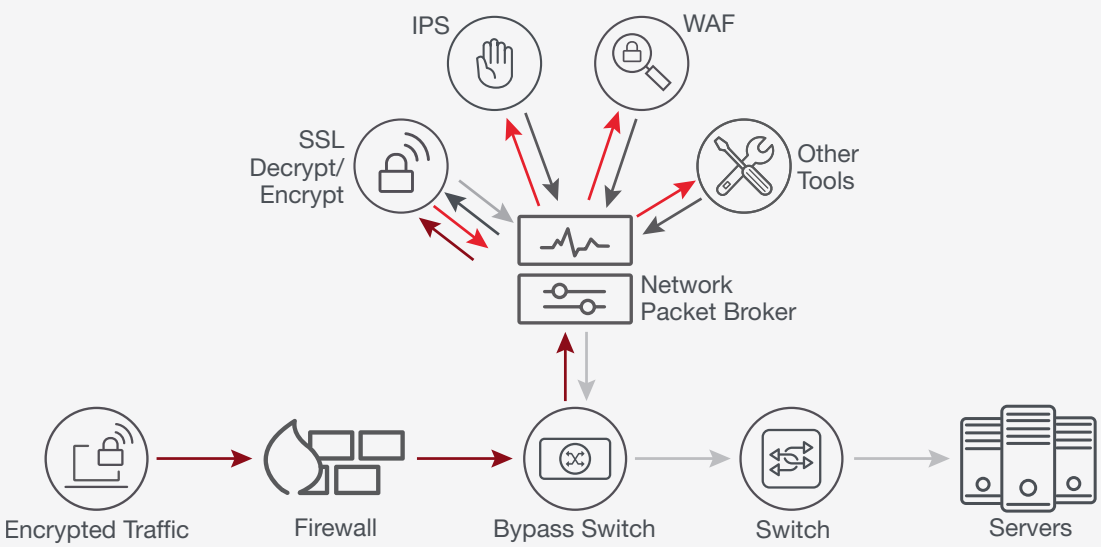
An alternate configuration is to use an NPB to pass incoming encrypted (e.g. HTTPS) traffic before it gets to the security appliance (e.g. Fortinet, Imperva, Baracuda, etc.) and redirect that SSL/TLS traffic to a purpose built decryption solution (e.g. BlueCoat, A10, etc.). Once the traffic is decrypted, it is sent back to the NPB which then relays that specific traffic to the IDS, WAF, etc. for processing.

Data Decryption Example

A visibility architecture equipped with packet brokers that use application intelligence can perform the following value-added functions:

- Capture the requisite data packets with an inline NPB
- Forward the data to one or more decryption tools
- Decrypt the payload data with active (man-in-the-middle) or passive decryption
- Pass the data on to the appropriate firewall tool(s) for analysis
- Return the inspected traffic to the network for propagation downstream

The following diagram shows an NPB sitting inline in the flow of traffic.



Note: All the arrows in the diagram all represent packets flowing between the element.

Figure 1. Example of a visibility architecture using inline SSL decryption.

Summary

Offloading encryption from security tool appliances allows those devices to process data faster. It also helps prevent overloading of these security tools by allowing the security architecture to focus on its main objective, not network configurations and device throughput. An inline NPB facilitates the capture and redirection of the encrypted data to the decryption device. Without an NPB, this type of solution would be very difficult and complex.

External SSL Solutions From Keysight

Keysight's solution for dedicated, external SSL decryption involves using NPBs in conjunction with an SSL decryption application for either passive or active decryption (depending upon how configured).

Learn more about Keysight's Network Packet Brokers technology.

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