SOLUTION BRIEF

# Offload SSL Decryption to Extend Firewall Life

## Deployment Scenario: Inline Network Visibility

According to NSS Labs, up to 75% of all web traffic will be encrypted by 2019. This creates a significant security risk as encryption can be used to hide malware and other threats. Gartner believes that starting in 2017 more than 50% of enterprise network attacks will use encrypted traffic. According to NSS Labs, 50% of enterprise applications are now encrypted using either the secure sockets layer (SSL) standard or its updated version called transport layer security (TLS). Many firewalls (up to 80%) don't include the ability to decrypt traffic. At the same time, replacing firewalls can become an expensive activity. One solution is to use a network packet broker (NPB) to direct SSL-based traffic to a purpose built decryption device and then forward the unencrypted data to the firewall and other security appliances for analysis.

**Solution Components:**

- Keysight's Network Packet Brokers
- SSL Decryption tool

## Benefits

- Extend the life of your existing firewalls
- Easily segment out encrypted data for decryption
- Avoid network equipment changeout pains

## Solution Overview

This network visibility solution allows you to:

- Extend the life of your security tools by using an NPB in combination with an external decryption device
- Use an inline network packet broker to aggregate encrypted traffic and relay that data to dedicated decryption devices
- Improve system traffic latency by decrypting data once
- Avoid the headache of an unnecessary changeout of existing firewall equipment

KEYSIGHT TECHNOLOGIES

## The Value of Offloading SSL Decryption

Payload encryption is a common technique used to thwart security attacks and hackers. Unfortunately, many firewalls do not support this feature. In addition, feature upgrades and equipment replacement is expensive. The Security architect is then forced to decide whether SSL decrypt capability is really worth the replacement costs and aggravation of a new firewall solution.

An alternative, cost-effective solution is to capture incoming encrypted, traffic before it gets to the firewall solution 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 firewall for processing.

Many firewalls (up to 80%) don't include the ability to decrypt traffic. With up to 50% of enterprise traffic now being encrypted, this creates a significant security risk.

## 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
- Remove extraneous data, if necessary
- Forward 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.

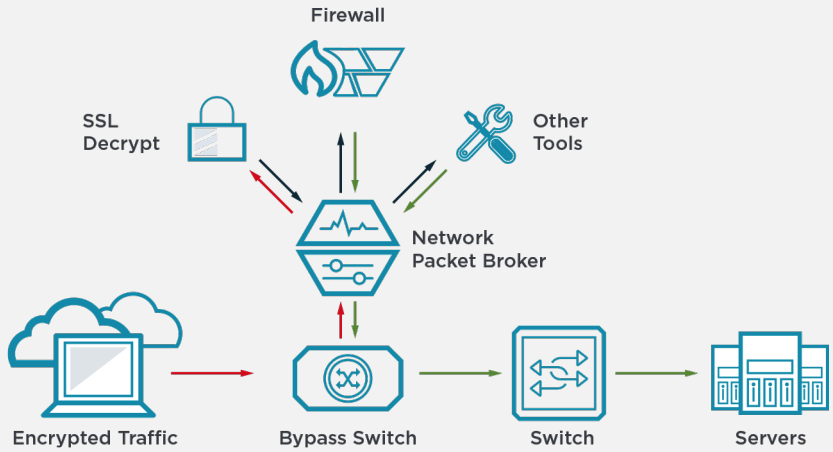


Figure 1. Example of a visibility architecture using inline SSL decryption

## Summary

Capture of encrypted traffic for firewalls and forwarding that data to purpose-built decryption devices allows you to extend the life of your existing firewalls. Instead of replacing the firewall at a high cost, a lower cost NPB can be added to the network to analyze traffic types and direct the data

to different locations, as needed. 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 significantly more costly and become very complex during the firewall changeout process.

## 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