SOLUTION BRIEF

Offload SSL Decryption to Extend Monitoring Tool Life & Value

DEPLOYMENT SCENARIO: OUT-OF-BAND NETWORK VISIBILITY

Use of encryption to hide malware is growing rapidly. Many enterprise applications are now encrypted using either the secure sockets layer (SSL) standard or its updated version called transport layer security (TLS). In fact, Google's 2016 Transparency Report showed that 77% of Google server requests are now encrypted and NSS Labs' 2016 "TLS/SSL: Where Are We Today?" study states that 50% of enterprise application traffic is now encrypted. Unfortunately, many monitoring tools cannot understand encrypted traffic nor can they decrypt the traffic themselves. This often results in two options – either ignore the encrypted traffic or upgrade to more expensive tools that can process the encrypted traffic. A third, more cost-effective, option is to deploy a network packet broker (NPB) with integrated decryption capability.

BENEFITS

- Extend the useful life of security and monitoring tools that cannot support encrypted traffic
- Save money by delaying costly upgrades
- Improve tool performance
- Expose malware and encrypted threats
- Easily implement out-of-band passive decryption

SOLUTION COMPONENTS:

- Ixia's Network Packet Brokers
- Ixia ATI Processor
- Ixia SecureStack technology

ixia
A Keysight Business

915-8149-01-4071 Rev A

SOLUTION OVERVIEW

This network visibility solution allows you to:

- Use an NPB with integrated SSL decryption capability to deliver unencrypted data to monitoring tools which extends the useful life of those monitoring tools and saves you money
- Strengthen network security by exposing SSL-encrypted malware and other threats
- Improve tool performance by sending the right type of data to your tools
- Easily implement out-of-band passive decryption where necessary

According to NSS Labs, 50% of enterprise applications are now encrypted. Many monitoring tools cannot understand encrypted traffic nor can they decrypt the traffic themselves. This increases your security risk.

THE VALUE OF INTEGRATED SSL DECRYPTION

Many monitoring tools cannot handle SSL-encrypted traffic. Traffic with encrypted payloads sent to these tools is discarded, either immediately or after the CPU has spent valuable processing capabilities and time on the traffic just to determine that it cannot, in fact, process the traffic. This decreases productivity and results in a higher security risk for the company due to potential missed security threats.

In some cases, security and monitoring tools can process encrypted data. Unfortunately, this is usually a costly feature upgrade or the SSL inspection generates a significant performance overhead on security tools. In other cases, network monitoring mechanisms for SSL decryption involve using a special appliance to capture data packets, decrypt them, and then forward those packets on to special purpose tools for analysis. However, unless you have a high volume of traffic that needs to be decrypted, the use case just mentioned can end up being a slower, more costly solution than using a network packet broker with integrated decryption capabilities.

OUT-OF-BAND DATA DECRYPTION EXAMPLE

In an out-of-band solution, the decryption methodology works such that the decrypted data is just a copy of the network data, not the original data. So it does not need to be re-encrypted after being analyzed. It can also be discarded if not needed. For example, this capability can be used to decrypt SMTP mail traffic and hand it off to an antiviral tool for virus/malware inspection. Other data can be decrypted and sent off to a data loss prevention (DLP) device for deep packet inspection.

A NPB equipped with integrated SSL/TLS decryption capability offloads this burden at minimal cost without impacting your security and monitoring tool performance. This solution provides these value-added functions:

- Capture the requisite data packets
- Decrypt the payload data with passive decryption
- Filter the data to remove extraneous data
- Forward the data on to the appropriate tool(s)

At the same time, the NPB-processed traffic has no impact on application or analysis performance on the tools. This decryption capability can be used on out-of-band security and monitoring tools.

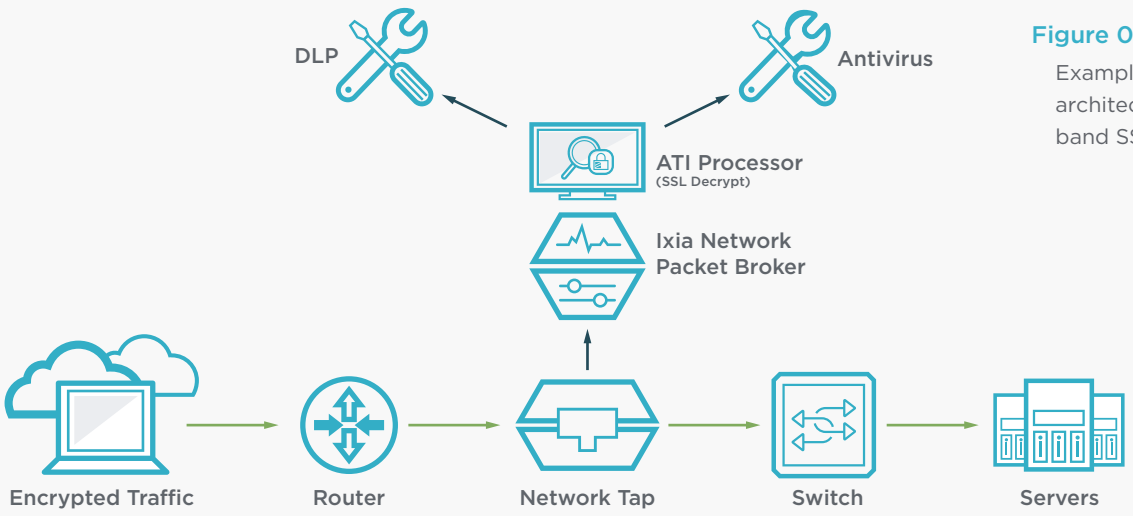

Figure 01
Example of a visibility architecture using out-of-band SSL decryption

The solution presented here allows you to postpone expensive monitoring tool upgrades and extend the life of your existing tools.

SUMMARY

An NPB with integrated SSL decryption capability can be used to quickly and cost-effectively deliver unencrypted data to monitoring tools. This type of solution also saves you money by extending the useful life of existing security and monitoring tools that do not support integrated decryption capabilities. Integrated decryption capability within an NPB allows the NPB to quickly perform this function and forward the clear data to the right troubleshooting tools for analysis, making it easier and faster to examine suspect data.

SSL SOLUTIONS FROM IXIA

Ixia's solution for integrated SSL decryption involves using NPBs in conjunction with an the ATI Processor for SSL decryption and application filtering. Learn more about Ixia's Network Packet Brokers, ATI Processor, and SecureStack Technology.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127