CASE STUDY

Bank Reduces Security Threats by Using SSL Decryption

Financial institutions like banks are high profile targets for security attacks. Network security is mission-critical as any breach can be a public relations nightmare. To reduce the risk of security threats entering the customer's network, this customer chose to deploy inline Secure Sockets Layer (SSL) and Transport Layer Security (TLS) decryption so they could inspect incoming traffic for various types of malware.

This customer turned to Ixia for the solution because they needed help to deploy the SSL decryption cost-effectively with minimal complexity. They also needed to operate at line speed to reduce any time delays.

Why Use Inline Security Appliances

Inline security appliances, such as intrusion prevention systems (IPS), data loss prevention (DLP) tools, and web application firewalls (WAF) all have one very attractive quality — they enable proactive security threat analysis. This is because the security appliances are directly in the path of active incoming Internet protocol (IP) traffic entering the business network. A network packet broker (NPB) should sit between a bypass switch and the inline security tools to facilitate data capture. The NPB solution provides the perfect opportunity to inspect all traffic and either remove or quarantine anything that looks suspicious without the complexity of serially connected appliances.

Company

Large universal financial institution in Europe

Key Issues

- Inspect incoming encrypted data traffic for security threats
- Deploy SSL/TLS decryption with minimal complexity

Solutions:

A comprehensive visibility solution, consisting of:

- Sixteen Vision ONE network packet brokers (NPB) deployed inline
- Ixia SecureStack application for decryption/encryption
- 192 fiber taps

Results

- Inline network visibility platform with integrated SSL decryption exposed hidden malware attack
- Integrated SSL decryption within the NPB reduced decryption cost and complexity by $120K
- Future ability to use Vision ONE NPBs to deliver filtered traffic to performance monitoring solutions

KEYSIGHT TECHNOLOGIES

If inline security appliances are not deployed, the data traffic must be inspected at a later point. Because the data has already entered the network, this is an “after the fact” check for malware and means that the malware has already had the opportunity to launch the intended attack. Therefore, the location of security appliances is a very important decision.

The Need for Decryption

SSL and TLS encryption are standards-based technology for transmitting private information by protecting data packets from scrutiny or corruption by non-authorized users. They use a combination of public key and symmetric key encryption to create an encrypted link between a server (typically a website or mail server) and a client (typically a browser or a mail client). For most organizations, SSL traffic is already a significant proportion of their total web traffic.

> “Catching that one piece of malware showed my boss how important an inline NPB and security tools are. That justified the whole purchase.”
>
> – Senior Security Architect

Bad actors have also taken notice of this technology. SSL encrypted traffic can contain direct, tangible threats including malicious code disguised by the encryption process. This malware is particularly sophisticated and likely to be part of an advanced, sustained attack on an organization. For example, Dyre malware can capture and transmit data before encryption occurs. Another example is the Zeus botnet, which uses SSL communications to upgrade itself.

An easy and effective solution is to use an NPB to pass encrypted traffic to an inline SSL decryption appliance. This solution offers complete visibility and control of encrypted traffic without requiring the re-architecture of your network infrastructure. You can add policy-based SSL inspection and management capabilities to your network security architecture to remove encrypted traffic blind spots.

The Value of Integrated Decryption

While most NPBs can aggregate data and send that data to an external decryption appliance, more sophisticated models can perform decryption functions within the NPB itself. An integrated decryption approach performs data decryption within the NPB, and then the NPB forwards the data straight to special purpose tools. This integrated decryption capability provides an easy and cost-effective way to examine suspect data. For instance, there is no wasted time and energy on trying to correlate information from multiple sources, direct data to/from decryption tools, and then track the flow of information to security and analysis tools.

At the same time, the NPB has no impact on application performance. For example, this capability can decrypt simple mail transfer protocol (SMTP) mail traffic and hand it off to an antiviral tool for virus/malware inspection. No resources on a firewall or other device are necessary.

Encryption also makes troubleshooting and performance monitoring much more difficult. Integrated decryption capability allows the NPB to quickly perform this function and forward the clear text data to the right troubleshooting tools for analysis.

The customer saw an immediate $120,000 cost savings by not deploying an external decryption solution.

Bank Network with Integrated Decryption

The bank decided to deploy redundant NPBs with integrated decryption between the bypass switches and the inline security tools; IPS, DLP, and WAF. The bypass switch shunted off to the packet broker where the NPB captured network data, decrypted the data, and then distributed the data to the various security tools for analysis. Since the NPB includes decryption capability, there was minimal processing time as the data only required decryption and re-encryption once within the NPB.

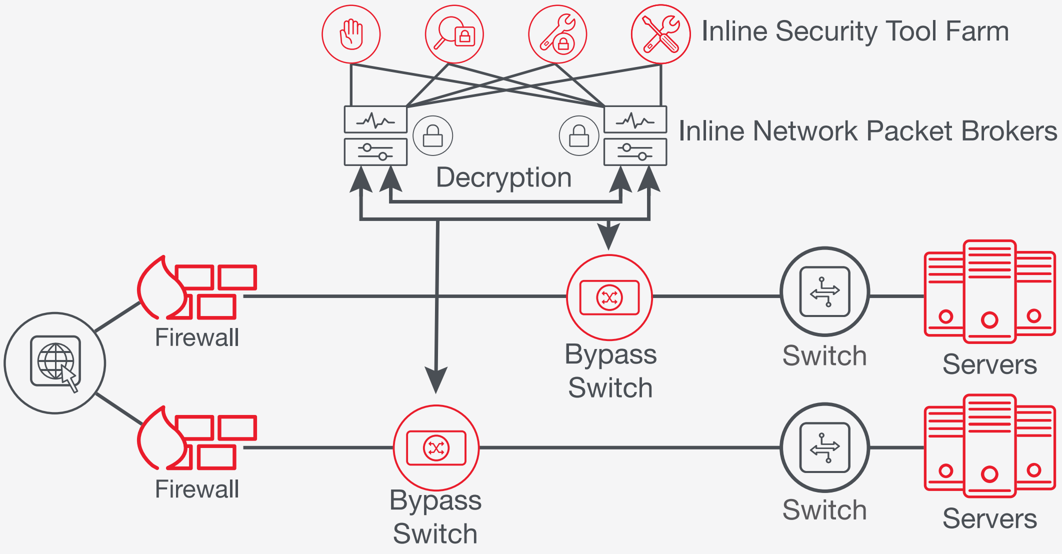

Figure 1. Customer deployment using integrated SSL/TLS decryption.

Summary

This international bank customer chose an Ixia NPB visibility solution with integrated SSL/TLS decryption. The customer realized an immediate $120,000 cost savings by not deploying an external decryption solution. In addition, they caught a piece of malware two weeks later that could have severely damaged their network — should the encrypted malware have bypassed the IPS for inspection.

According to the senior security architect, “Catching that one piece of malware showed my boss how important an inline NPB and security tools are. That justified the whole purchase.”

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