WHITE PAPER

The Role of Active SSL Decryption in Network Monitoring

New Monitoring Challenges Result from Data Encryption

Secure Sockets Layer (SSL) technology significantly impacts the way IT departments monitor their networks. In 2016, Sandvine Research estimated that almost 70% of internet traffic is encrypted.[1] Data was once captured and sent to security and monitoring tools for analysis. Those tools can no longer read that data. This situation creates network blind spots that include hidden sources of security threats operating without your knowledge.

SSL technology significantly impacts the way IT departments monitor their networks. Data that was once captured and sent to security and monitoring tools for analysis is now unreadable by those tools.

While decrypting the data is the most obvious answer, most IT organizations struggle with the following problems:

- Possessing multiple tools, often more than three, that need to see decrypted (cleartext) traffic causes a significant burden
- Decrypting (and re-encrypting) data has a high CPU resource tax, making it inefficient to run the SSL function on multiple security tools
- Serial chaining multiple security tools together while properly handling and protecting cleartext traffic is difficult
- Maintaining the isolation of cleartext traffic for regulatory compliance is difficult

Technology, such as a network packet broker (NPB) with SSL decryption capability, addresses these problems. An NPB decrypts network data; aggregates, removes, and masks data as needed; and distributes it to the proper security and monitoring tools for analysis. The NPB then re-encrypts the data without impacting tool performance or causing compliance issues.

HTTPS — The Solution for Online Privacy

HTTPS, which includes both the original SSL standard and the updated version Transport Layer Security (TLS) standard, is intended to secure internet-based communications. In 1994, Netscape developed SSL for encrypting internet data, but the standard did not go mainstream until Facebook adopted it in 2013. In 2014, Google began penalizing the rankings of business websites that did not

[1] "2016 Global Internet Phenomena Report," Sandvine Inc., 2016.

KEYSIGHT TECHNOLOGIES

use the protocol. In addition, web applications, Office 365, and cloud-based traffic have accelerated the adoption of SSL encryption.

Other drivers include regulatory and compliance initiatives. One example is the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which mandates the use of TLS 1.0 or higher. The Payment Card Industry (PCI) also mandated the use of TLS in its PCI-DSS standard. PCI required migration to a more secure version of TLS (TLS 1.1 or higher) by June 30, 2018.

Improvements to SSL technology, such as the use of ephemeral keys (where the server and clients exchange new encryption keys for each session), increased the security and effectiveness of data encryption. These improvements also increased adoption of the technology. All these factors increased the proliferation of SSL for security in online browsing and data storage. However, as we shall see, the use of encryption is not without its perils.

The Problem with SSL Encryption

While the use of SSL helps encrypt data from prying eyes, bad actors use it to obscure security threats. In a May 2016 study, "Hidden Threats in Encrypted Traffic," the Ponemon Institute found that 41% of cyberattacks leveraged SSL encryption to bypass traditional security solutions.[2] Gartner predicted that more than half of security attacks would use SSL and TLS by the end of 2017 to cover up malware threats and command and control transmissions.[3]

For security and troubleshooting purposes, organizations must examine the traffic on their networks. Unfortunately, firewalls, intrusion prevention systems (IPS), monitoring tools, and other equipment do not understand encrypted traffic. So, to inspect the traffic, you must decrypt it before analysis. This process often draws a significant performance penalty.[4] Depending on where and how this decryption takes place, it will create different, sometimes significant, burdens on the network infrastructure. The key to avoiding this decryption pitfall is to create a visibility architecture that can effectively decrypt the necessary data and efficiently deliver it to where it needs to go — without causing a performance burden or significant time delay.

Overcoming the SSL Security Threat

To overcome the encryption security threat, businesses need to decrypt the traffic crossing their networks and analyze it. There are two popular methods to achieve this: active decryption and passive decryption. Here is a review of both approaches.

Passive SSL decrytion

Passive SSL relies on static (rather than ephemeral) keys and forces the IT department to copy the encryption keys from the target servers onto the decryption device. Businesses typically use this method for decrypting inbound connections from users on the internet to internal servers. Once the decryption device has the keys, the device decrypts traffic and passes it on to security and monitoring tools (such as an IPS, data loss prevention [DLP], or web application firewall) for analysis in cleartext format. This mechanism is known as "passive" because the decryption device is not an active part of the SSL connection; it decrypts traffic by merely observing it go past.

2 "Hidden Threats in Encrypted Traffic," Ponemon Institute, 2016.
3 Johnnie Konstantas, "SSL Encryption: Keep Your Head in the Game," SecurityWeek, March 15, 2016.
4 Antone Gonsalves, "Rising SSL traffic to degrade firewall performance," CSO, June 17, 2013.

As shown in Figure 1, passive decryption in an out-of-band architecture is for inbound-only traffic monitoring scenarios and not does allow for the encryption/re-encryption of outbound communications.

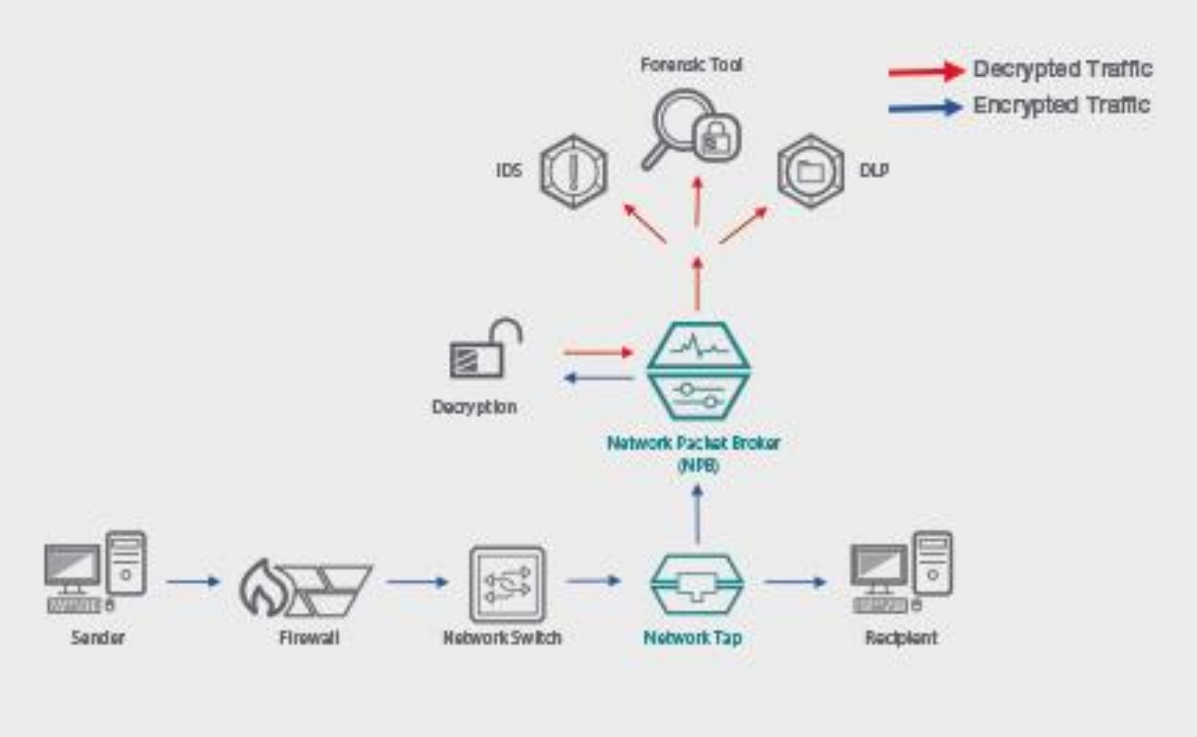

Figure 1. Passive Decryption

Active SSL decrytion

Active SSL decryption uses ephemeral keys and must occur inline in the form of a transparent proxy. This decryption process is a known and trusted part of the network. It performs inline decryption for the end-user recipients in a transparent fashion.

This scenario supports decryption/encryption in both directions (for inbound and outbound network traffic), as depicted in Figure 2. This means that both inline and out-of-band security and monitoring tools can analyze network traffic. Once the cleartext analysis for security threats is complete, the good data is re-encrypted and sent to its destination within the network.

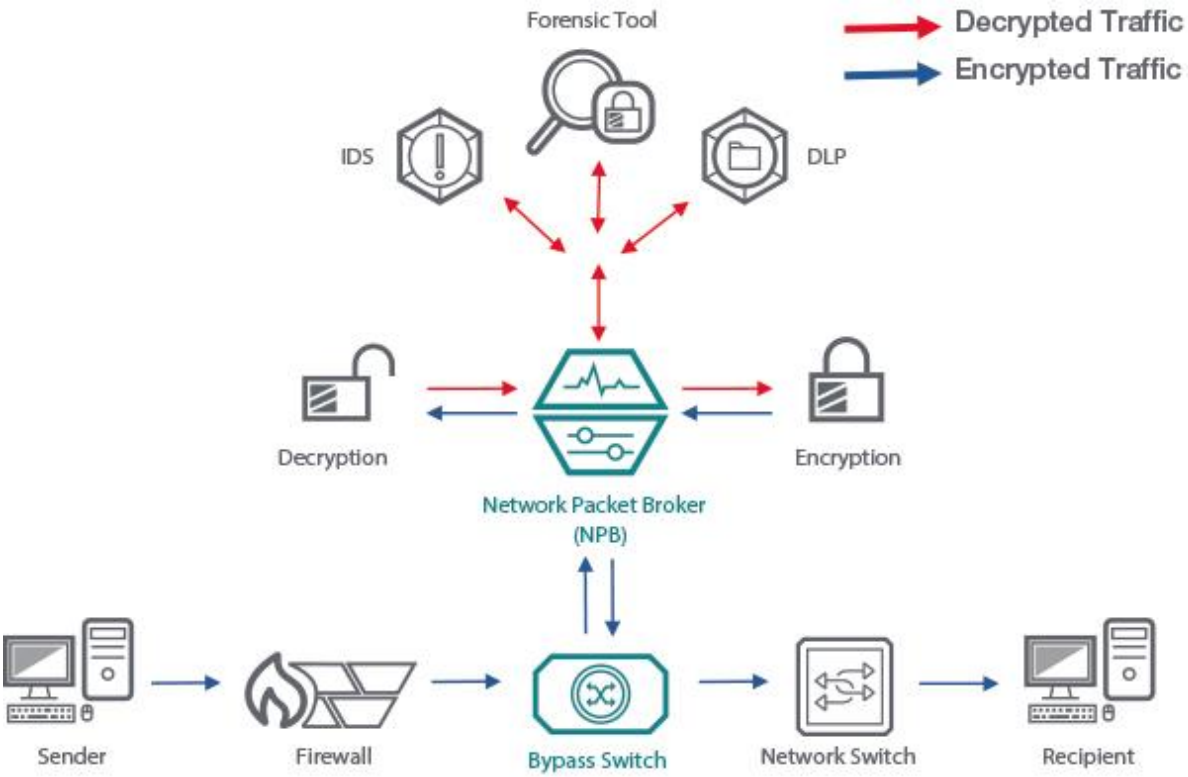

Figure 2. Active Decryption

Three Scenarios for Active SSL Decryption

Because of the exchange key simplicity (from an IT personnel perspective) of active SSL decryption and its use in inline and out-of-band monitoring architectures, active SSL decryption is the more popular decryption scenario. It is also the only solution applicable to connections using ephemeral keys. So, what are some of your options? As detailed below, there are three common decryption scenarios.

Purpose-built decryption device

The first type of solution includes the category of purpose-built decryption devices. This type of solution excels in high-volume transaction scenarios at high speeds. Typically, these solutions come with a high price tag to match the high performance. Since these devices are purpose-built, once you add them to the network architecture, they create complexities. These complexities occur when forwarding the decrypted data to multiple sequential inspection tools (such as firewalls, IPS, or DLP), redirecting the data back to the decryption device for re-encryption, and reintroducing the data into the network. These purpose-built solutions typically have basic capabilities that complement their SSL engines.

Integrated decryption in security tools

In contrast to purpose-built devices, security tools such as firewalls and IPS have optional upgrades to include integrated SSL decryption capabilities. Unfortunately, studies have shown a significant performance impact (up to 81% drop in CPU processing capability) for devices that have this decryption feature turned on.[5]

This drop in processing capability impacts network performance significantly and results in costly purchases of additional security tools, such as firewalls, to process the same amount of network traffic. Because of this, only 25% of companies use SSL decryption to inspect inbound and outbound communications for potential threats. Furthermore, within that 25%, the decryption capability is not applied to all traffic, just some of it.[6]

For enterprises that have adopted the industry best practice of "defense in depth," relying on encryption built into multiple security devices has additional penalties. Forcing each inline device to decrypt and re-encrypt data has obvious performance and latency impacts.

Decryption integrated into an NPB

The third approach is to deploy a network packet broker. In contrast to the purpose-built device, an NPB delivers one-stop shopping. The NPB aggregates the data from multiple sources, decrypts it, and distributes it to the proper security and monitoring tools for analysis.

Since the NPB decryption scenario does not place any decryption responsibility on the security and monitoring tools, those tools continue to function at optimum capacity. If you need to disengage the decryption function, you can turn the feature off. There is no need to take the network down or reroute data. In inline monitoring scenarios, the NPB effortlessly reintroduces the analyzed traffic into the network for propagation downstream.

With this decryption scenario, the NPB offers a cost-effective alternative to both the purpose-built and integrated decryption security tools discussed previously. In addition, there are no network traffic performance delays like that caused by multiple serially connected devices performing SSL decryption. These multi-component delays add up and create noticeable delays for real-time traffic such as voice and video. Thus, the integrated NPB approach provides excellent value across all decryption performance ranges.

Optimizing the Monitoring Achitecture for SSL

It is important to pick the right decryption scenario for your network. The solution must be flexible as well as easily deployable. A clear set of objectives are required as well.

For instance, which of the following capabilities are required for your deployment?

- extremely high or medium-to-high data throughput for SSL decryption
- applications that require minimal data delay
- a cost-effective solution
- easy installation and maintenance
- minimal impact to network service when disengaging SSL decryption
- additional features like data aggregation, data distribution, packet filtering, load balancing, and deduplication of decrypted data
- encryption details and application data reported over NetFlow

Once you know what you need, you can select one of the three decryption methods that provides the right solution for your network at the right price.

Summary

Most enterprise applications use encryption, and SSL encryption is here to stay. While SSL provides some protection for network data and improves security and compliance initiatives, it does have drawbacks. Encryption itself introduces hidden security risks. For instance, the use of encryption to hide malware is proliferating. Encryption also makes troubleshooting and performance monitoring more difficult.

Decryption of the enterprise network is one of the newest ways to counteract this danger. NPBs play a key role in helping enterprises and service providers optimize their visibility architecture and maximize the return on their investments for the following reasons:

- Integrated SSL decryption with an NPB is simpler and easier than other alternatives
- NPBs have no performance impacts for decryption and re-encryption
- The NPB easily connects dozens of security tools to the traffic they need to inspect
- The NPB maintains isolation of cleartext traffic
- The NPB solution delivers highly resilient security processing with load balancing of tools and fail-open behavior

One of the dangers with SSL decryption is that it makes sensitive data available to anyone with access to network monitoring tools. This is a common problem for monitoring data stored in DLPs, logs, and other databases, as it often violates regulatory compliance mandates. NPBs ensure regulatory compliance by masking data that does not need to be exposed.

The combination of these capabilities allows the NPB to deliver a broad set of value-added features at a cost-effective price point.

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