Introduction

In the realm of network security, the use of encryption can be considered a double-edged sword. On one hand, the ability to encrypt traffic between systems and applications provides us with confidentiality and privacy, enabling online commerce and the ability to conduct sensitive transactions. On the other hand, security analysts who need to monitor the network environment for signs of attacks and intrusions are stymied by encrypted traffic because they can’t see the contents without help.

The attacker community (including criminals, malicious insiders, nation states and terrorists) leverages encryption to its full extent today. Malware and attack toolkits commonly hide payloads, commands and outbound sensitive data within SSL traffic, which most network monitoring tools are blind to. One example of malware actively leveraging SSL for command and control (C&C) channel communication is the TDL-4 botnet documented by Kaspersky Labs, which encrypts commands, encodes with Base64 and then creates encrypted SSL tunnels to send the commands to and from bot systems.¹

The growing volume of SSL traffic compounds the problem, as well. According to a Palo Alto Networks report from May 2011, roughly 40 percent of the application traffic they observed within large enterprise networks was capable of using SSL, and 36 percent of the overall bandwidth consumed was from SSL traffic.²

In response to these more advanced threats, modern network monitoring and security intelligence tools are beginning to include SSL decryption features, providing visibility into SSL-encrypted tunnels. This is a positive step for security teams. However, SSL decryption latency, scalability and interoperability have been so problematic that organizations aren’t putting these tools inline, or aren’t using the SSL decryption features at all.

This paper discusses the impact of encrypted protocols and data traffic on monitoring and visibility, including identifying the stress points. It also discusses means to mitigate those stress points with optimized network monitoring to facilitate real-time parsing of data, decryption and deep packet inspection capabilities that support intrusion prevention, threat mitigation and network forensics.

¹ www.readwriteweb.com/archives/one_botnet_to_rule_them_all_kaspersky_labs_finds_i.php
Options for SSL Inspection

There are a number of options available today for inspecting SSL traffic on the network. Each of these options has definite pros and cons for security and network teams—some more operational in nature, and others related to performance.

To adequately monitor encrypted traffic, network security tools (such as Intrusion Detection and Intrusion Prevention Systems), firewalls and perimeter gateways must be able to identify the encrypted packets, then either decrypt them on the same platform or forward this traffic to their security and traffic inspection devices. Neither of these options are easily accomplished in high-speed networks. Several steps, which can be challenging, are involved in the process. Some of those steps are outlined in the options described for deploying network-based inspection with parsing and decryption.

**Option 1: Integrated SSL Decryption in Network Monitoring Tools**

The first option available today for decryption of SSL traffic is to use native features in modern network security devices. This option tends to be most prevalent in security and network devices and platforms that handle inline traffic, such as firewalls, proxies and Intrusion Prevention Systems (IPSs). There are a number of different vendors providing this kind of functionality.

- **Next Generation intrusion prevention platforms.** Certificates can be copied onto these platforms, or root Certificate Authority (CA) keys can be used from internal systems.

- **SSL decryption platforms.** Some security vendors offer a separate SSL decryption platform that is intended for use with IPS and other monitoring devices.

- **Next Generation Firewalls.** Next Generation Firewalls (NGFW) can store SSL keys locally for decryption of traffic.

Examples of companies that make products in these categories include Palo Alto Networks, Juniper, and Sourcefire. Each of these tools is focused on decrypting the traffic to perform specific monitoring and/or access control functions. There are definite pros and cons to this approach. The primary benefit of using the native, integrated SSL decryption capabilities in tools is simplicity. By integrating the certificates into an existing platform, security teams can simply evaluate and control the new traffic using existing policies and rules.

This works for the traffic that is already passing through the device. Unfortunately, this approach has a number of downsides.

- SSL evaluation is process-intensive in its own right.

- Evaluating SSL on the same platform that is performing numerous other intensive functions can be very expensive.

- Adding this additional overhead can significantly detract from available CPU and memory on the platform, which may, in turn, cause significant network degradation.
To illustrate this type of performance degradation with proxy-like systems such as NGFWs and other traditional perimeter security devices, Network World conducted a lab test in April 2012 that examined a number of attributes of these systems under peak loads. The report concludes, “SSL traffic poses a dual problem for NGFWs: If traffic is encrypted, applications cannot be inspected, but if traffic is decrypted there may be a very high performance cost. In fact, the SSL decryption tests turned out to be the biggest differentiator in this comparison...” The report goes on to outline rates for leading vendors like Check Point, Palo Alto, SonicWall, and Barracuda, all of whose platforms experienced extraordinary performance impacts from SSL decryption, sometimes over 10 times less traffic throughput!

Leveraging existing tools to decrypt SSL is also somewhat limited. It can be difficult to integrate this decryption holistically without additional evaluation tools and methods. All the assessment needs to be done on this one platform, which doesn’t scale in large environments. In addition, having multiple platforms handling inline SSL inspection can be very challenging to manage and configure.

**Option 2: Integrated SSL Decryption in Network Proxies**

Another option for decrypting and monitoring SSL traffic is to leverage built-in decryption capabilities in network proxy platforms. Many of the major proxy devices available today for outbound (traditional proxy) and inbound (reverse proxy) web traffic control include some sort of SSL inspection engine. Some well-known solutions that fall into this category include the following:

- **Network security gateways.** Many Universal Threat Management (UTM) platforms can perform intrusion prevention and antimalware functions, among others, but many organizations leverage UTMs as a forward or reverse proxy with content filtering.

- **Network proxies.** Several companies sell caching and content filtering proxies, primarily for outbound traffic acceleration and monitoring.

- **Content filtering gateways.** Products in this category are a cross between a proxy and a security gateway and are primarily focused on content filtering as an outbound filtering and monitoring platform.

Vendors that produce products in these categories include Microsoft, BlueCoat, Websense, F5, Riverbed, and Radware. All of these product types are intended to handle web traffic, most commonly from internal users who are browsing the Internet. Common capabilities offered by these tools include website caching to improve browsing speed and traffic control, site content filtering to block malicious sites and those forbidden by corporate policy, and application filtering for web application attacks and malicious code that may be present on sites visited by users. These types of proxies work in a similar fashion to the security filtering and access control platforms described in Option 1, where certificates are stored locally and used to decrypt user sessions traversing the devices.

---

Proxy platforms also have a number of pros and cons. One of the major benefits proxy platforms have with regard to SSL traffic is overall visibility, because most SSL traffic will likely pass through them. This can, in some cases, help security teams identify malicious traffic either generated purposefully by inside attackers or malware that is trying to communicate with control servers on the Internet. Data exfiltration is also more visible, and teams dealing with fraud and data leakage scenarios can gain insight into who is doing what under the covers of SSL-encrypted tunnels. This visibility is also prevalent when monitoring user behavior for policy violations (sending sensitive data to personal e-mail accounts, for example).

One shortcoming with these types of platforms and SSL decryption solutions is a lack of SSL inspection on ports other than TCP/443. Most proxy platforms assume port 443 is used for SSL, and that is becoming less true all the time, particularly for malicious use of SSL. Another drawback to platforms in this category is that organizations are often forced to rely on different options for inbound and outbound traffic.

For example, a traditional web proxy that performs SSL decryption and content inspection is likely in place for outbound traffic from the internal network. However, new inbound traffic (exclusive of the users’ returning web traffic) is usually directed in a different way via a separate route. This traffic likely passes through routers, firewalls and load balancers, which often have SSL decryption capabilities, as well. Decryption and inspection of messages sent through this process would require an entirely separate SSL decryption capability in one or more of those platforms.

Another significant drawback to these systems, in general, is that performing SSL decryption can significantly degrade performance in a similar manner to the network monitoring platforms listed in Option 1.

**Option 3: Brokering Encrypted Packets as Required**

When networked systems forward SSL-encrypted traffic, some type of traffic capture device (such as taps) must then direct the traffic to a separate physical port for monitoring. Once the traffic has been redirected, it will be sent to an accelerated decryption platform that can rapidly decrypt the traffic using a stored certificate or other key. Once decrypted, the traffic must then be assessed by security or network monitoring tools such as Intrusion Detection Systems (IDSs) or flow analysis platforms. Once the traffic has been assessed, it can ultimately be sent on to its destination, usually after re-encrypting.

That’s a lot of steps to take. When using traditional taps or automated redirection from existing security devices, this process can take a significant toll on overall performance and network latency, which may be unacceptable in environments requiring very low latency levels. SSL offloading platforms and high-speed decryption devices can be very expensive, too, and may be difficult to configure and maintain.4

---

4 [www.sans.org/reading_room/analysts_program/analyst-vss-monitoring.pdf](http://www.sans.org/reading_room/analysts_program/analyst-vss-monitoring.pdf)
A better option might be more “intelligent” taps that are capable of directing traffic in the network at high speeds and support policy-based configuration, meshed communication and more robust and granular alerting and traffic control functions. This option manages real-time capture in both directions and should afford better control of the traffic capture process, while still allowing organizations to forward newly decrypted traffic to security tools for analysis and decision making.

These tools also allow security and network teams to be completely agnostic in many scenarios, so they can continue to leverage existing tools and relationships with network and security analysis tools and vendors in-house.

These intelligent tools can also help decrypted SSL traffic events make their way into security event management platforms for more advanced correlation. Such automation can help organizations design and meet goals for security strategies that meet the 20 Critical Controls version 3.0 recommendations. Numerous controls within this framework recommend network monitoring and access control systems to prevent attacks. Critical Control 5, “Boundary Defense,” contains a number of “Quick Wins” that rely on implementation of network intrusion detection and prevention, as well as effective firewall implementation and segmentation to deeply inspect traffic for malicious behaviors and content.5

Being able to inspect both incoming and outgoing SSL simultaneously, at the same location in the network, is another positive aspect of using intelligent taps. Now, traffic can be inspected once and sent on where it needs to go for analysis, as opposed to having to send traffic somewhere, decrypt it, and then re-encrypt the message and send it somewhere else. For this reason, intelligent SSL decrypting taps will likely be more scalable, too.

As with any tools of this type, there are benefits and drawbacks. The benefits in this case will likely outweigh the drawbacks, because there is so much more flexibility at hand when intelligent taps are deployed. Overall traffic capacity, with support for higher bandwidth and throughput, is a major consideration.

The major downside to using tools like these is the addition of an additional technical layer in the network environment. This layer may very well be embedded or installed at manufacturing by agnostic security tool vendors or by large enterprise organizations that wish to use the tools directly. In other words, there may be additional ways to tie in SSL inspection capabilities with existing equipment, minimizing disruption and the need to potentially re-architect the entire network to accommodate different traffic flows, existing security device locations and monitoring and alerting current or planned mechanisms.

5 www.sans.org/critical-security-controls
Implementing Network Packet Brokers for SSL Decryption and Inspection

Distributed traffic monitoring with packet brokers (intelligent taps) is a new way to more readily get access to large volumes of traffic moving at very high speeds and perform SSL decryption on traffic to make it accessible to monitoring tools. Aside from SSL traffic, these interconnected taps can aggregate many types of network data and send the traffic to a monitoring and management console, while providing a new level of visibility and analysis across network boundaries.

With an intelligent, distributed system, each tap (or node) can send traffic to different parts of the network where intrusion detection systems, performance monitoring tools, network forensic recording devices and other network and security tools are waiting for actionable input.

This solution can provide immediate value in most network environments because it can be overlaid on top of existing network designs without the need for extensive re-architecture. In addition, the ability to rapidly decrypt the SSL traffic and send it to monitoring tools or an existing IPS or malware analysis sandbox allows security teams to quickly gain insight into the types of traffic they have on the network—possibly leading to incident response process changes, improved network traffic behavioral profiles, and other enhancements to security programs. A distributed model that implements intelligent taps for SSL decryption and traffic handling might look something like the one illustrated in Figure 1.

Figure 1. A Simple Distributed Intelligent Tap Architecture
Any of the taps could handle SSL traffic and then forward it to the IDS in the DMZ for analysis, for example. The most logical placement of taps that might decrypt SSL traffic might include the following locations:

- **Sensitive data zones.** On the internal network, there are likely numerous zones in which sensitive data is stored in databases that may have SSL connections initiated from web or application servers. Monitoring traffic in these zones for anomalous transactions or data exfiltration attempts would be useful for security teams.

- **Egress points from the internal network.** Intercepting user traffic bound for the Internet before it hits a proxy allows security teams to see what data is being sent to the Internet over SSL tunnels. This is likely where infected end user systems transmitting bot command and control information will be detected.

- **DMZ zones.** Traffic coming into extranet zones or application servers that use SSL may benefit from SSL decryption and inspection to detect incoming attacks.

There are many more locations in which enterprise security teams will likely want to inspect encrypted tunnels. Such areas are where sensitive data and users reside.

How should security and operations teams change the environment to accommodate SSL decryption within distributed taps? The good news is that speeds and feeds should generally improve with this kind of solution, because SSL decryption won't need to be enabled specifically on IDS or IPS sensors, malware analysis sandboxes, firewalls, proxies or other existing security control platforms. The only inline deployment change will be installation of the SSL inspection device. Once the device is in place, all other systems can largely remain in the same logical locations.

A key architecture and design consideration is re-encryption of decrypted traffic before sending it on its way. Enterprises will need to determine whether decryption is performed silently, with no real modification of packets, or whether packet addressing and other header fields are manipulated in some way by devices monitoring the decrypted traffic. For most organizations, performance will be optimized by modifying packets as little as possible, but this may be required for certain Network Address Translation (NAT) or Port Address Translation (PAT) configurations, particularly if load balancers are in use. Consider these issues:

- **Privacy concerns.** Modifying packet content in encrypted traffic without the knowledge of the client and/or server could introduce some privacy and legal concerns. Intelligent taps may be able to help with this by simply re-encrypting the original content received, thus preventing any modifications from actually being transmitted.

- **Traffic-handling issues.** Modification of header fields for NAT and PAT configurations could cause problems for intelligent taps re-encrypting traffic after analysis.

This type of packet brokering can provide a policy control point for all SSL traffic in the environment, regardless of whether that traffic is social media or traffic from wikis, blogs and spearphishers. For example, security and network teams can specifically disallow SSL traffic that makes use of self-signed certificates or weak cipher suites, is destined to sites that have expired certificates or uses certificates that are signed by untrusted CAs.

In general, however, organizations will want to avoid modifying packet header fields in decrypted traffic if at all possible, because the modifications will likely make decryption more complicated.
Conclusion

Based on the threat landscape today, every organization has a need to inspect SSL traffic going into and out of its networks.

Most of the major attacks we see today, especially those against end users, leverage SSL in some way. Sophisticated malware is now capable of sending command and control data exclusively over SSL channels, using sites that, in many cases, don’t raise flags from web content filters. This means we have to dig into the traffic itself and see what is actually happening.

Unfortunately, SSL traffic is usually present in such large volumes that decrypting it places a significant degree of load on the platforms performing the decryption. This is unacceptable in the best circumstances, as any additional resource overhead on network and security platforms detracts from the primary job of the systems, including filtering, inspection and other varieties of monitoring. More importantly, it competes with the primary objectives of the network team—reliability and throughput.

Fortunately, there are numerous options available to enterprise security and operations teams. To date, many have tried to leverage the built-in options, configuring network platforms with SSL certificates and managing the performance impacts the best they can. Using SSL decryption and inspection within network proxies is also a common practice, and with the proper hardware, this can be reasonably effective.

The bigger challenge is addressing both outbound and inbound SSL with these platforms. Most of the time, proxies are only configured to decrypt and inspect outbound traffic, and there are just as many inbound SSL flows that security and network teams may want to inspect.

A better option for many large organizations might be using packet broker devices that perform decryption of traffic and send it to existing network and security platforms for cleartext analysis. This approach saves resources on all platforms and can help add new control points for traffic shaping and direction within the network.

Ultimately, brokering encrypted traffic to monitoring devices for inspection can provide more optimized use of both system and network resources by allowing for flexible traffic inspection with much less overhead.
About the Author

Dave Shackleford, founder and principal consultant with Voodoo Security, is a SANS analyst, instructor and course author, as well as a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert, and has extensive experience designing and configuring secure virtualized infrastructures. He has previously worked as CSO for Configuresoft and CTO for the Center for Internet Security. Dave is the author of “Virtualization Security: Protecting Virtual Environments” from Sybex. Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently leads the Atlanta chapter of the Cloud Security Alliance and sits on the board of the SANS Technology Institute.

SANS would like to thank its sponsor:

VSS monitoring
Network Intelligence. Optimized.