WHITE PAPER

# Best Practices For Monitoring Encrypted Data

## Introduction

Once used to increase the security of Internet traffic, encryption can actually make some types of security monitoring more difficult. Many firewalls and other security tools do not understand encrypted traffic, and many organizations have chosen to pass encrypted traffic into their networks without security inspection just to keep communication flowing. Unfortunately, this creates blind spots in network visibility—areas where the organization is unaware of the traffic moving inside and exiting its network.

Knowing that blind spots exist, criminals have increasingly encrypted their attacks to avoid detection and cover their tracks. In a May 2016 study, "Hidden Threats in Encrypted Traffic," Ponemon Institute found that 40% of cyber-attacks leveraged secure sockets layer (SSL) encryption to bypass traditional security solutions[1]. It's no coincidence that, despite the introduction of more sophisticated prevention and detection solutions, cyberattacks and data loss continue.

Analysts say 40% of malware threats come from deliberate, sophisticated use of SSL encryption and organizations are not doing enough to inspect this traffic.

[1] "Uncovering Hidden Threats within Encrypted Traffic," Ponemon Institute and A10 Network, 2016.

KEYSIGHT TECHNOLOGIES

## Approaching a 100% Encrypted Internet

Back when Amazon was still a bookseller, the percentage of encrypted traffic was relatively small. Encryption was generally reserved for financial transactions, such as ecommerce and banking. Part of the reason was that encryption was relatively expensive. The certificates required were not cheap, and Web servers had to use a lot of their processing power to perform encryption and decryption functions. Websites typically opted for speed over privacy, except when sensitive data was involved.

Today, the situation is different. Complete encryption—and not just with sensitive data—appears to be where we are headed. Even data we considered trivial just a decade ago, like Internet searches, are encrypted. Popular sites, like Google and Facebook, are now making SSL encryption the default. In December 2016, Gartner reported that encrypted traffic represents 30–40% of enterprise Web traffic, and some of its clients in the finance and legal sectors are dealing with peaks of more than 70%[2].

And, certificates are not expensive anymore. Sites like Let's Encrypt provide them for free, although not without controversy. Free certs are not automatically trusted by many browsers and can result in customers receiving scary warning messages. Many people believe the transformation to total encryption can be traced to 2013, when leaked documents revealed that the National Security Agency of the United States was gathering personal data transferred over the internet. Whatever the reason, Hyper Text Transfer Protocol Secure (HTTPS) encryption is quickly becoming the default, and websites without encryption now face being penalized in Google searches.

## Security Tools Need Traffic Decrypted

If all SSL traffic were legitimate, you could pass it in and out of your network without bothering to decrypt. Unfortunately, you cannot assume this is the case. To keep your defenses strong, you need to inspect HTTPS traffic just as you do nonencrypted traffic. The deep packet inspection performed by firewalls, intrusion prevention systems (IPSs), and other security appliances requires plain text, so the first step is to convert encrypted packets into a form your security devices can work with. The most efficient way to do this is to decrypt the packets one time and make the plain text available to all security tools, before re-encrypting and passing the traffic along. No matter what device is used for decryption, it will need to have access to the cryptographic key used to encrypt the packet (see Figure 1).

[2] "Predicts 2017: Network and Gateway Security." Gartner, 13 December 2016.

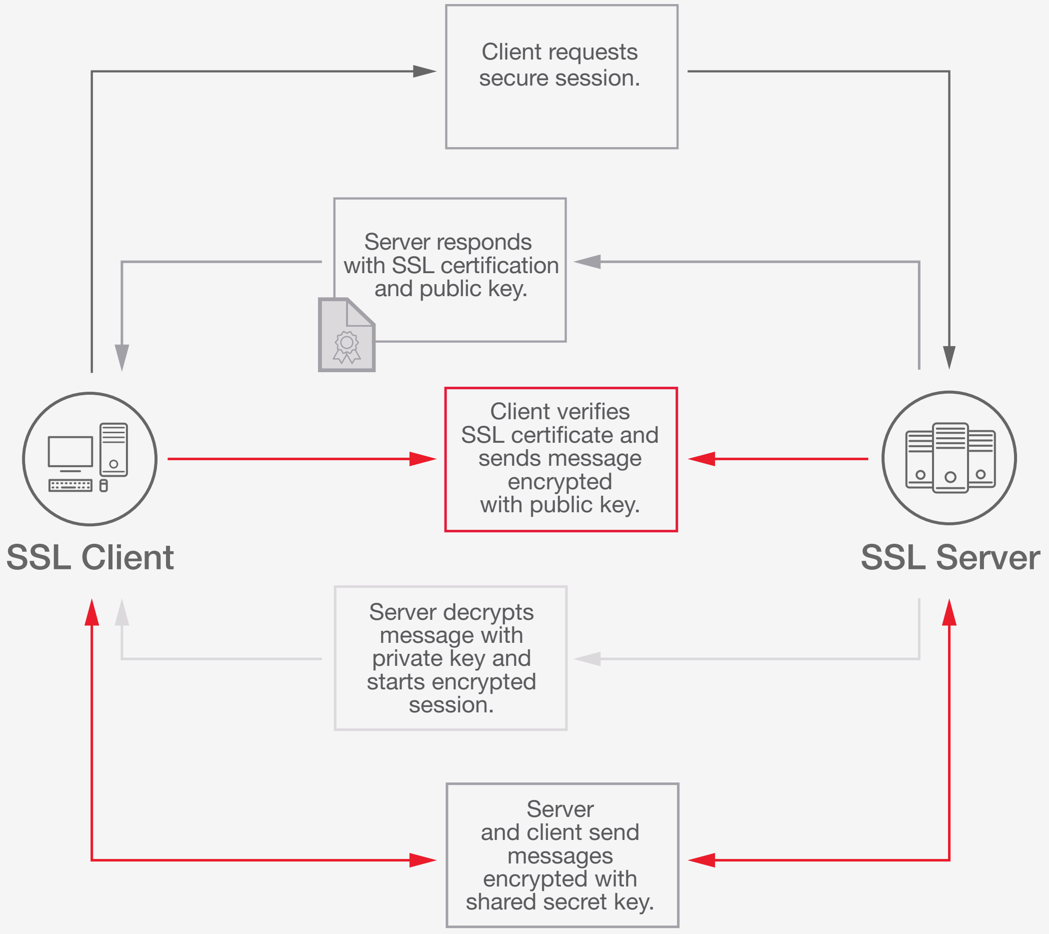

Client requests secure session.
Server responds with SSL certification and public key.
Client verifies SSL certificate and sends message encrypted with public key.
SSL Client
SSL Server
Server decrypts message with private key and starts encrypted session.
Server and client send messages encrypted with shared secret key.

**Figure 1. Understanding SSL/ TLS Transactions.**

## The Burden of Encryption

Cybersecurity experts agree that, to protect enterprise data and networks from hackers and cybercriminals, it is essential to inspect all encrypted network traffic. On the practical side, however, decoding requires intense processing, and encryption algorithms are becoming more complex with longer key sizes to strengthen their ability to withstand hacking. Current practices also dictate the use of perfect forward secrecy (PFS) in which the encryption system generates a random secret key for each session, to ensure that a compromised key in on instance cannot compromise other messages. A widely-publicized test performed by NSS Labs several years ago found that moving from 1024- to 2048-bit ciphers caused an average performance loss of 81% on the eight leading firewalls[3]. Experiences like that are probably why organizations not yet

[3] NSS Labs Analyst Brief "SSL Performance Problems," Pirc, John W., 2013.

inspecting encrypted traffic report that their number one concern is performance degradation[4]. This is particularly true for monitoring live network traffic where disruptions can lead to loss of revenue and customer dissatisfaction.

On the other hand, not inspecting secure traffic and allowing blind spots to develop can be equally costly. Organizations that are slow to adopt decryption will be exposed to more targeted malware and ransomware that leverages encryption. Analysts believe that by 2020, more than 60% of organizations will still fail to decrypt HTTPS efficiently, putting their business at risk[5]. The challenge is figuring out the most effective and cost-efficient way to perform the inspection.

## Strategies For Cost-Effective Monitoring

Here are four strategies that companies are currently using to overcome visibility blind spots.

### Strategy 1. Remove as much malicious traffic as possible before decrypting

Is it possible to stop encrypted malware from entering your network without decryption? Yes, if you can determine the packet is bad even before knowing what it contains. A relatively new appliance called a threat intelligence gateway can block traffic it identifies as malicious before it enters your network. Instead of looking at the payload of the packet to identify a threat signature, a threat intelligence solution looks at the Internet Protocol (IP) address in the packet's header and compares it to a large and constantly updated database of addresses known to be involved in current attacks. Since packet headers are clear text, decryption is unnecessary. If the IP address matches any in the database, the packet is dropped immediately or sent to a sandbox tool for further analysis.

**Doesn't your firewall do this?** Traffic blocking is pretty straight-forward and you are probably using your current firewall to do some of this already. Using your firewall, however, requires you to manually create rules and keep them updated as conditions change. A threat intelligence solution, however, is designed to automatically block communications using a real-time database of problem sites. No manual rules need to be created and no staff person needs to be involved. Threats are blocked without delay. Automation also reduces the risk that an outdated rule may cause a false positive, in which your firewall blocks traffic that represents a legitimate business transaction. In addition, firewalls are limited in the number of configuration rules they can process. Typical 1Gb firewalls support about 10,000 IP ranges and 10Gb versions support about 40,000. That may sound like a lot, but with over 4.3 billion IPv4 addresses

#### Milestones in Data Encryption

- **2013:** Facebook adopts secure browsing by default.
- **2014:** Google announces it will start penalizing a website's search result ranking if encryption is not used.
- **2015:** HTTP/2, a major revision of HTTP, is finalized in February 2015. All major browsers have stated they will only support HTTP/2 when it is used over an encrypted connection, essentially making encryption mandatory.
- **2016:** NetFlix starts expanding encryption beyond customer information, search queries, and other confidential data to also include transport of video content.
- **2016:** Google demonstrates that 85% of its online traffic is encrypted. The goal is 100%.
- **2017:** Google's Chrome browser begins marking HTTP pages that collect passwords or credit cards as "not-secure."

[4] "Uncovering Hidden Threats within Encrypted Traffic," Ponemon Institute and A10 Network, 2016.
[5] "Predicts 2017: Network and Gateway Security." Gartner, 13 December 2016.

and an ever-growing number of IPv6, firewalls are not equipped for the reality of today's Internet. When your firewall or intrusion prevention system (IPS) begins to approach the upper limit of their blocking capacity, performance is impacted. In the worst-case scenario, packets can get dropped, and risks go undetected.

**Intelligence without limits.** In contrast, a threat intelligence solution is designed for the sole purpose of keeping track of and blocking a very large number of IP addresses and geolocations without any performance degradation. The solution uses a high-performance hardware appliance, connected to a remote data feed, which automatically provides intelligence on the latest cyber threats and attacks (see Figure 2).

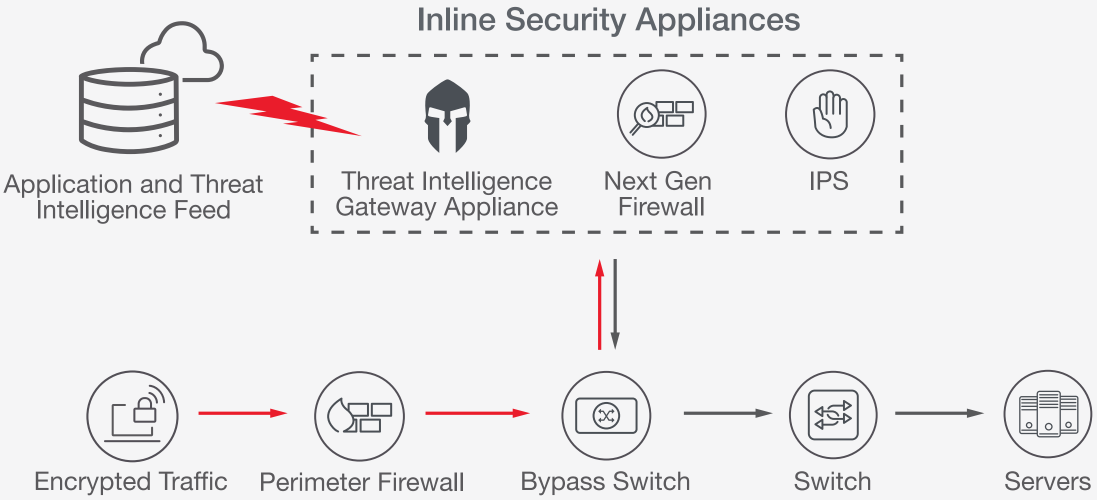
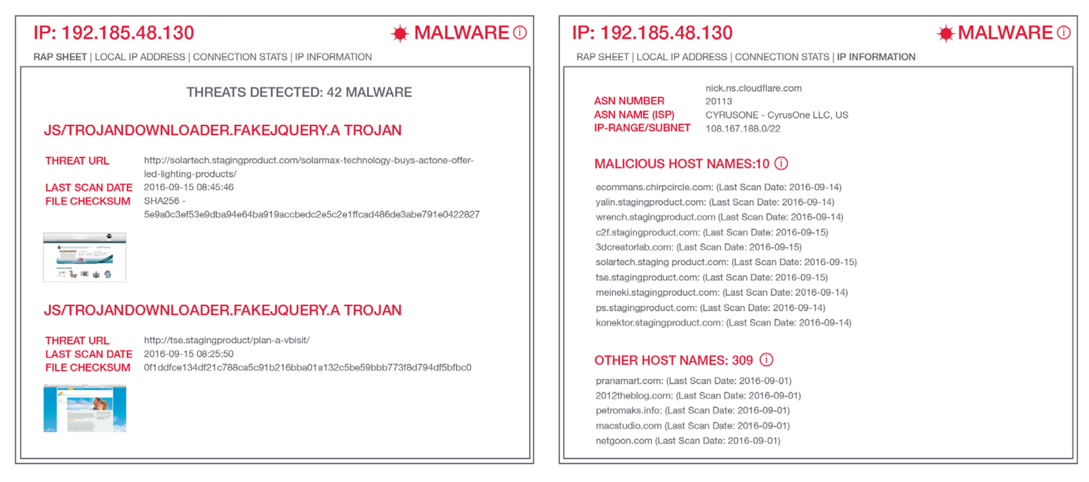

Inline Security Appliances
Application and Threat Intelligence Feed
Threat Intelligence Gateway Appliance
Next Gen Firewall
IPS
Encrypted Traffic
Perimeter Firewall
Bypass Switch
Switch
Servers

**Figure 2. Threat intelligence solution positioned to remove malicious SSL traffic.**



IP: 192.185.48.130 MALWARE ⓘ

RAP SHEET | LOCAL IP ADDRESS | CONNECTION STATS | IP INFORMATION

THREATS DETECTED: 42 MALWARE

JS/TROJANDOWNLOADER.FAKEJQUERY.A TROJAN

| | |
|---|---|
| THREAT URL | http://solartech.stagingproduct.com/solarmax-technology-buys-actone-offer-led-lighting-products/ |
| LAST SCAN DATE | 2016-09-15 08:45:46 |
| FILE CHECKSUM | SHA256 -<br>5e9a0c3ef53e9dba94e64ba919accbedc2e5c2e1ffcad486de3abe791e0422827 |

JS/TROJANDOWNLOADER.FAKEJQUERY.A TROJAN

| | |
|---|---|
| THREAT URL | http://tse.stagingproduct/plan-a-vbisit/ |
| LAST SCAN DATE | 2016-09-15 08:25:50 |
| FILE CHECKSUM | 0f1ddfce134df21c788ca5c91b216bba01a132c5be59bbb773f8d794df5bfbc0 |

IP: 192.185.48.130 MALWARE ⓘ

RAP SHEET | LOCAL IP ADDRESS | CONNECTION STATS | IP INFORMATION

| | |
|---|---|
| | nick.ns.cloudflare.com |
| ASN NUMBER | 20113 |
| ASN NAME (ISP) | CYRUSONE - CyrusOne LLC, US |
| IP-RANGE/SUBNET | 108.167.188.0/22 |

MALICIOUS HOST NAMES:10 ⓘ

ecommans.chirpcircle.com: (Last Scan Date: 2016-09-14)
yalin.stagingproduct.com: (Last Scan Date: 2016-09-14)
wrench.stagingproduct.com (Last Scan Date: 2016-09-14)
c2f.stagingproduct.com: (Last Scan Date: 2016-09-15)
3dcreatorlab.com: (Last Scan Date: 2016-09-15)
solartech.staging product.com: (Last Scan Date: 2016-09-15)
tse.stagingproduct.com: (Last Scan Date: 2016-09-15)
meineki.stagingproduct.com: (Last Scan Date: 2016-09-14)
ps.stagingproduct.com: (Last Scan Date: 2016-09-14)
konektor.stagingproduct.com: (Last Scan Date: 2016-09-14)

OTHER HOST NAMES: 309 ⓘ

pranamart.com: (Last Scan Date: 2016-09-01)
2012theblog.com: (Last Scan Date: 2016-09-01)
petromaks.info: (Last Scan Date: 2016-09-01)
macstudio.com (Last Scan Date: 2016-09-01)
netgoon.com (Last Scan Date: 2016-09-01)

**Figure 3. Example of an intelligence "rap sheet" generated by Keysight's ThreatARMOR.**

The intelligence database is maintained by a dedicated staff using a variety of techniques to continually verify and document the status of each IP address. Daily verification is important to remove sites that have been cleaned up from the database and to avoid false positives. To provide assurance that the threat intelligence solution is adding value, choose a solution that documents each action taken and how each problem address was verified.

**See all actions taken**. Included in Figure 3 is an example of threat intelligence verification documentation. The figure shows two pages of a "rap sheet" generated by Keysight's ThreatARMOR™ solution. With a threat intelligence solution in place, you can block a significant amount of encrypted traffic related to malicious sites from entering your network. Depending on your industry and how often you are targeted for attack, you can see up to an 80% reduction in encrypted traffic[6].

In addition to reducing the risk of a cyberattack, you are also reducing the volume of overall traffic that needs to be processed by your security appliances. This has the added advantage of helping your security appliances operate more efficiently and can delay the need to purchase additional capacity.

[6] Keysight case study "Hyper Box Tackles Attack Traffic with Keysight ThreatARMOR," June 2016.

## Strategy 2. Build an architecture that will scale cost-effectively

Once you've removed the encrypted traffic from suspicious IP addresses, the remainder must be converted to plain text for your security appliances to inspect. If only a small portion of your overall network traffic was SSL, it might not make much difference where decryption was executed. But as SSL increases, it will have more of an impact on the performance of your security infrastructure and your overall network.

**Decrypt once, serve all monitoring tools**. Some of the newer firewalls, IPSs, and unified threat management solutions offer SSL decryption as an additional feature. This may seem like the easiest way to unlock the information you need, but decryption is a process-intensive function that slows the performance of deep packet inspection tools and can potentially create serious bottlenecks. If you use your tools for decryption, you will end up needing to upgrade capacity much sooner than you otherwise would. And when you run out of on-board capacity upgrades, you may have to load balance between multiple devices, increasing operating complexity as well as capital expenses. Finally, traffic decrypted by one tool is not easily shared with other tools that also require plain text packets.

If you need to provide plain text to multiple tools, it is much more efficient to perform the decryption one time and send the decrypted traffic to all the tools that require it. This minimizes the CPU cycles devoted to decryption and lets the information be quickly delivered to multiple tools at the same time. With decryption centralized, it is also much easier to scale it cost-effectively as the volume of encrypted traffic grows.

**Leverage your network visibility solution.** With a decrypt-once strategy, the next step is to choose the type of appliance that offers the best return on investment. Some organizations choose a dedicated SSL appliance, deployed behind an external bypass switch, which offloads the monitoring tools. A different option is to use the decryption function of a network packet broker (NPB). These devices are already deployed in many organizations to increase tool efficiency by sorting through all the network traffic, identifying relevant packets for each tool, and distributing the traffic to tools at high speed. An NPB that uses hardware acceleration techniques and a dedicated cryptographic processor will provide the fastest decryption, without impact to the other packet processing functions.

Some vendors let you activate decryption as a field upgrade to an existing NPB and pay for the volume of decryption required. For organizations without a packet broker, purchasing a new device can be easy to justify based on its ability to increase tool efficiency, extend tool lifespan, and load balance between similar tools. Some solutions even provide fault-tolerant delivery of network traffic to security appliances and assist with troubleshooting by isolating packets based on user, device, application, or geolocation. NPB-based decryption is easy scaled as needs change.

**Build an inline serial appliance chain**. NGFWs are designed to decrypt SSL traffic only for their own internal security inspections. They cannot share live traffic with other inline security appliances from other vendors. An NPB, however, lets you chain together multiple appliances operating inline for maximum efficiency (see Figure 4). Administrators use the NPB's remote interface to specify the flow of live traffic from one device. A threat intelligence gateway allows you to remove packets from malicious IP addresses. This high-performance device can move packets through your entire security architecture with speed and processing efficiency.

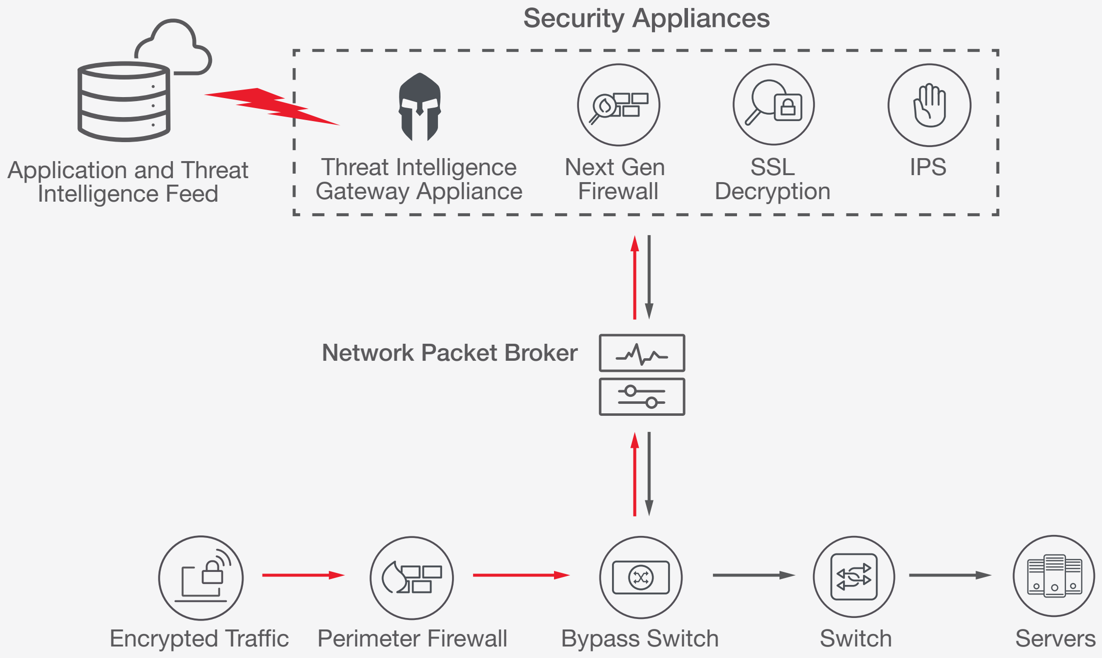


**Figure 4. Architecture for SSL decryption of inline traffic.**

**Increase efficiency of out-of-band monitoring tools.** In addition to inspecting live traffic, your security infrastructure also uses tools to perform forensic analysis (see Figure 5). This type of monitoring is good at detecting multi-stage attacks that do not necessarily set off a red flag until two or more events are considered together. Again, many of these monitoring tools are not able to understand SSL-encrypted traffic and encrypted payloads are either discarded immediately or after the tool has spent valuable processing cycles to determine it cannot, in fact, process the traffic. The most efficient way to operate monitoring tools is to filter aggregated traffic with a network packet broker and only forward copies of the data each tool requires. A high-performance NPB equipped with integrated SSL/TLS decryption capabilities can provide decrypted traffic at minimal cost.

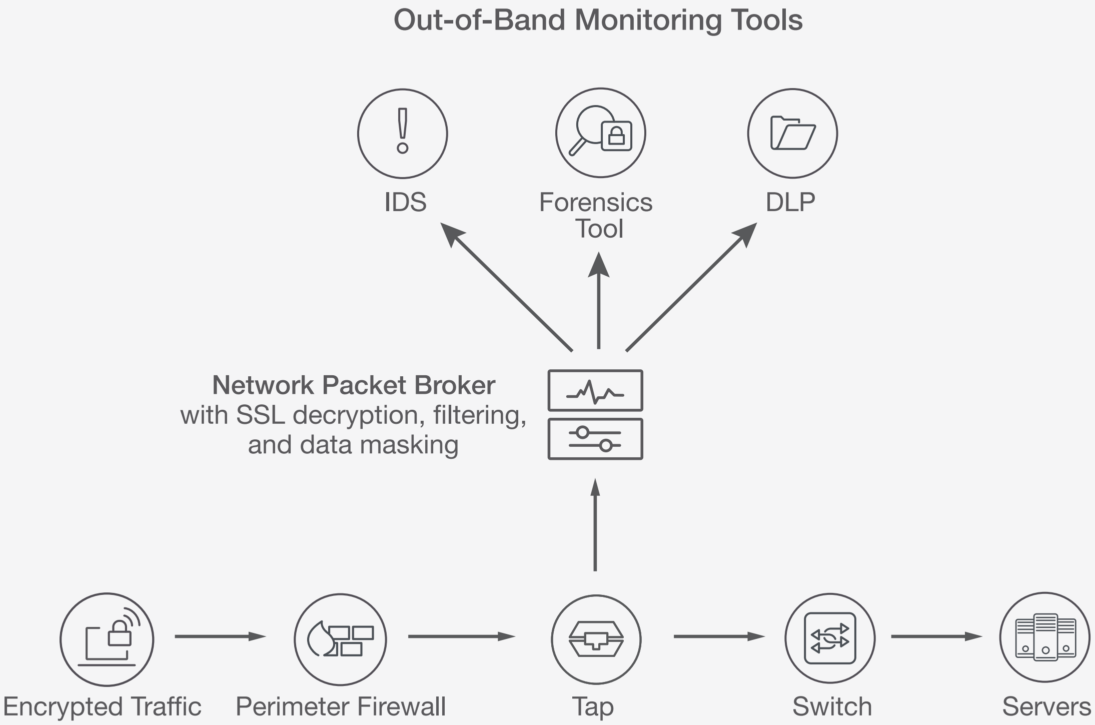


**Figure 5. Architecture for SSL decryption of out-of-band monitoring.**

## Strategy 3. Invest in high-quality decryption tools as encryption becomes the norm

As more of the Internet becomes encrypted, attacks hidden in SSL traffic will grow in popularity and sophistication. Many commonly-used security devices have added SSL decryption to their feature set, but that may not be the best approach for dealing with the growing volume of encrypted traffic. In a recent paper on how to evaluate security solutions, NSS Labs warned that some devices may not have the latest ciphers, may miss SSL communications that occur on non-standard ports, be unable to decrypt at their advertised throughput, and may even fast-path some connections without performing decryption at all[7]. These warnings should be taken seriously by any organization with a growing percentage of SSL-encrypted traffic. As the volume of SSL traffic increases, the quality of your decryption solution will become more important to achieving total network visibility.

**Standards, ciphers and keys.** Cryptography relies on continuing advances to stay one step ahead of the bad guys. To achieve visibility of live network traffic, your security solutions need to support the latest encryption standards, have access to a wide variety of ciphers and algorithms, and have the power to decrypt traffic using the larger 2048-bit keys. Since many ciphers are actually based on publicly known algorithms, protecting the key used to control the operation of the cipher is critical. As security technology grows in complexity, your visibility solution must be able to process decryption efficiently and cost-effectively—without dropping packets, introducing errors, or failing to complete a full inspection.

Because decryption can degrade the performance of an NGFW so quickly, hackers can launch a denial of service attack by simply targeting an organization with high volumes of SSL traffic. With no other solution in place, this type of attack can be highly successful. To prevent this from happening, organizations with a high percentage of SSL traffic need access to a wide range cryptographic ciphers and key management schemes to keep communications flowing.

**Operational simplicity.** Another feature of a high-quality SSL visibility solution is the ease with which administrators can create and manage policies related to decryption. This can be very important in industries that regulate privacy and compliance to comply with the mandates of Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), and other standards. Some firewalls and application delivery controllers with SSL capability do not allow decryption to be applied at a granular level. Those that do, may use complex command line scripts

### Features of Advanced Network Visibility Solutions

The following features are important in enterprise-level visibility solutions:

- Port independent filtering
- Load balancing across multiple tools
- Packet de-duplication
- Packet trimming
- MPLS stripping
- Data masking
- Graphical filter creation
- Dynamic filter automation

[7] "SSL: Enterprise's New Attack Frontier, Are your blind spots secure?," NSS Labs, 2017.

that are difficult to create and maintain. Organizations that expect the percentage of encrypted traffic to rise will find a purpose-built device to be much more efficient. In addition, an SSL visibility appliance keeps complete records of each SSL cipher used and logs all exceptions related to dropped sessions, SSL failures, invalid certifications, and sessions not decrypted for policy reasons. These detailed logs are valuable for audits, forensics, and network troubleshooting and capacity planning.

**Protocols and ports**. Finally, organizations need SSL visibility solutions designed to detect and decrypt SSL traffic entering and leaving through all ports, not just standard ports that carry the majority of an organization's traffic. Hackers are constantly looking for open ports that could function as a base for launching a cyberattack. Most NGFWs and ADCs are designed to look for SSL traffic on high volume ports, such as port 443 for HTTPS, port 465 for authenticated SMTP over SSL, port 993 for IMAP over SSL, or port 995 for POP3 over SSL. These devices may not be monitoring traffic on non-standard ports that hackers might use to launch a new type of cyberattack.

## Strategy 4. Ensure sensitive plain text data is protected

When traffic is decrypted, the data is transformed back into clear text. Therefore, if you send copies of decrypted packets to out-of-band monitoring and analysis tools, the copies are also vulnerable to interception, which increases the overall "attack surface" of your network. That means login information, financial transactions, social security numbers, healthcare data, phone numbers, and anything else that was encrypted for security purposes is now readable by anyone that can intercept the traffic or access the tools that receive it. You have a legitimate reason for decrypting the traffic—to inspect the payload for malicious content. But when you decrypt the traffic, you are effectively removing the security that protected it. Even if you can ensure security during data delivery, the tools you use to monitor traffic may store the information, sometimes for extended periods of time.

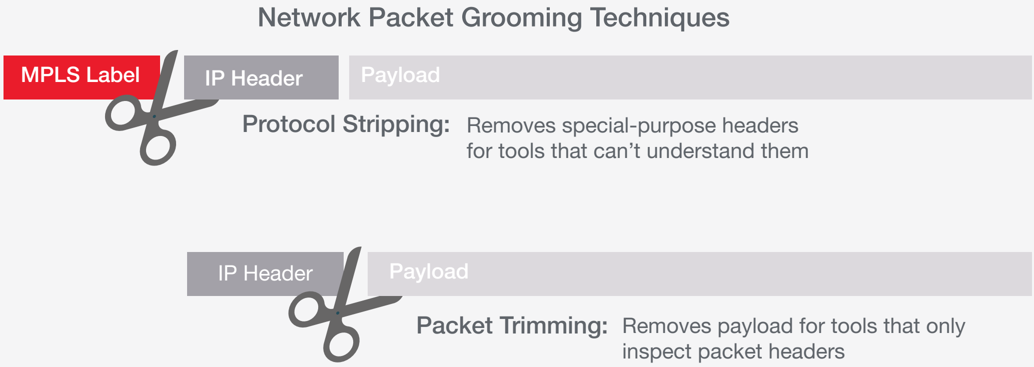

Network Packet Grooming Techniques
MPLS Label
IP Header
Payload
Protocol Stripping: Removes special-purpose headers for tools that can't understand them
IP Header
Payload
Packet Trimming: Removes payload for tools that only inspect packet headers

**Figure 6. Intelligent NPBs can minimize the size of network packets.**

**Mask data covered by privacy regulations.** There are a couple of ways to mitigate this risk. If you use a Security Fabric architecture to aggregate, filter, and distribute network traffic, you can also use that infrastructure to implement additional security measures on packets before they reach your tools. For instance, an NPB with security intelligence has the ability to scan for patterns inside the packet and identify social security or credit card numbers. The NPB can then mask these data strings by blocking all but the last several digits, the same way vendors mask your credit card number on receipts. This strategy can help you protect sensitive data inside packets that have been decrypted.

**Groom for greater efficiency.** The second way to mitigate risk after decryption is to remove or trim off any part of the packet that is not necessary to the inspection process before it is sent to your tools. Not every tool is a deep packet inspection tool. Some tools analyze only packet headers, and the payload does not need to be transmitted. Trimming can also be used in conjunction with other filtering rules to further reduce the processing workload for your tools. This helps your tools perform more efficiently and, therefore, extend the length of their useful life.

## Conclusion

As more of the Internet shifts toward encrypted traffic, hiding attacks in SSL traffic will only grow in popularity and sophistication. Cybersecurity experts agree that, to protect enterprise data and networks from hackers and cybercriminals, it is essential to inspect all encrypted network traffic. An organization that does not develop a robust approach to inspecting encrypted traffic will undermine the value of its overall network security and create an unacceptable risk of breach and data loss. Fortunately, new solutions are emerging that improve the efficiency and cost-effectiveness of SSL decryption.

## 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