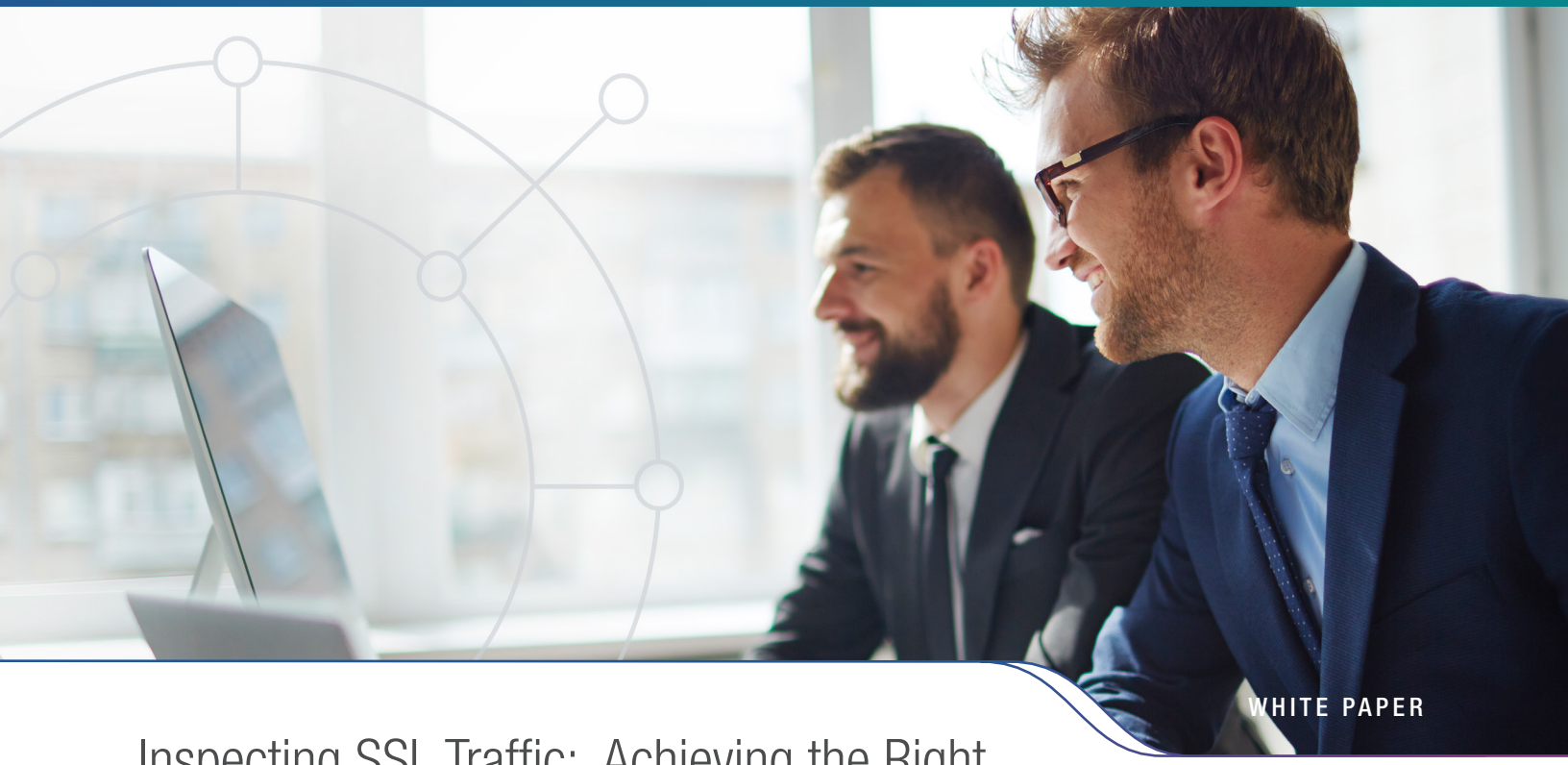


WHITE PAPER

Inspecting SSL Traffic: Achieving the Right Balance of Visibility and Security

A delicate balancing act is taking place on organizations' networks globally. It is the balance between visibility and security: achieving the complete and accurate organizational view that is essential to make good decisions, versus applying the strong protective measures that are essential to keep sensitive data safe. It is a balance between protecting against known IT security threats — and unintentionally concealing new IT security vulnerabilities. And it all centers on SSL encryption.

SSL encrypted traffic is between 15%-25% of enterprise web traffic.

What is SSL Encryption?

Secure Socket Layer (SSL) encryption is a standard technology for transmitting private information, protecting data packets from being read or corrupted by non-authorized users. It uses 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). It was developed in the 1990s and has rapidly become an industry-standard tool in the battle against malicious hackers and accidental data loss.

For most organizations, SSL traffic is already a significant proportion of their total web traffic. In 2015, Gartner estimated that on average, between 15% and 25% of enterprise web traffic was SSL encrypted, rising to more than 50% in many

KEYSIGHT TECHNOLOGIES

sectors[1]. Many vertical market segments are subject to rigorous compliance protocols that actively demand SSL encryption, such as PCI-DSS and HIPPAA. Such regulations aim to protect sensitive data in transit travelling to banking, merchant and healthcare-related websites.

What is more, many critical business applications like Microsoft Exchange, Salesforce.com and Dropbox are also heeding the calls for greater data privacy by enabling SSL. A range of hugely popular web destinations such as LinkedIn, Twitter, Facebook, Google, Yahoo, WebEx, Exchange, SharePoint, and others are also enabling SSL.

Many critical business applications are enabling ssl.

But just as SSL encryption protects bank details and medical records, it can also conceal and protect malicious cyberthreats. Sophisticated malware, as well as more subtle but business-critical indicators of potential cyber-attacks, can be hidden in SSL encrypted traffic. And as SSL traffic volumes grow, so too does the risk of threats hiding within the encrypted data stream. This means it is essential that organizations decrypt and inspect SSL traffic, so that they can be sure it is not being used as a conduit for hackers to smuggle and propagate malware.

Why Is Network Visibility So Essential?

Lack of visibility and monitoring into 10% of data traffic creates a significant blindspot.

An organization's network is always vulnerable — and yet always growing. New technologies and new applications, increasing demand for mobile access and hungry bandwidth are all placing unprecedented pressure on organizations' infrastructures. Complete visibility of all traffic is essential if performance problems — or critical security issues — are to be quickly identified and resolved. Even a lack of visibility and monitoring into 10% of data traffic creates a significant blind spot, leaving networks vulnerable to malicious attacks, noncompliance, and damaged performance.

So what may be stealthily lurking within SSL encrypted data? There are two key risks that businesses need to be aware of: tangible threats and more subtle threat indicators.

Risk Factor 1: Tangible Threats

50% of malware threats will come from deliberate, sophisticated use of SSL traffic.

Direct, tangible threats within SSL encrypted traffic means malicious code like benign SSL traffic disguised by the encryption process. If an employee, for example, is lured in by a spear phishing attack and clicks on a bad link which downloads malware to their computer, that malware can potentially propagate across the corporate network within SSL-encrypted traffic.

A small proportion of malware is specifically designed to attack organizations via SSL encrypted traffic — this malware is particularly sophisticated and likely to be part of an

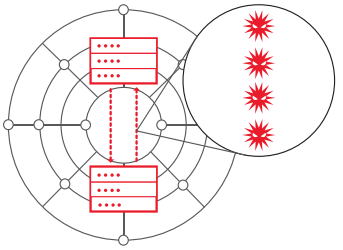
1. Cybercriminals Hiding in Your SSl Traffic, Gartner Research, 2015

advanced, sustained attack on an organization. For example, in 2014, Dyre malware was found to be capable of capturing and transmitting data before encryption occurs. Another current example is the Zeus botnet, which uses SSL communications to upgrade itself.

Gartner Research's report 'Security Leaders Must Address Threats From Rising SSL Traffic' argues that by 2017, 50% of malware threats will come from deliberate, sophisticated use of SSL traffic. This is a serious blind spot for businesses.

Risk Factor 2: Threat Indicators

Threat indicators are signs that a malicious party is probing or scanning the network looking for vulnerabilities. They are evidence of potential hacks or network intrusion attempts. They include anomalies in network traffic flows such as traffic travelling a path it would not normally or an unusual traffic volume. Without being able to see what is in said traffic — because it has undergone encryption — it is far more difficult to identify these anomalies.



The Performance Problem

IT teams must decrypt and inspect SSL traffic, ensuring that malware is not making its way into the organization and that attackers are not probing the network for vulnerabilities. This is where a host of key weapons in the IT team's arsenal come into play:

- **Firewalls**, which decrypt and scan SSL traffic. They also protect against intrusion attempts according to the organization's bespoke security policies. It is, however, worth underlining that the Gartner report referenced above found that fewer than 20% of firewalls, UTM, and IPS deployments actually support decryption and there is a capability gap here.
- **Application monitoring tools**, which check the behavior of crucial organizational tools and software.
- **Antivirus**, which inspects for malicious code by comparing the decrypted traffic against a known bank of malware.
- **Anti-bot security software**, which detects bot-infected machines and prevents further damage.
- **Intrusion Prevention Systems (IPS)**, which monitor network traffic to detect and prevent vulnerability vulnerabilities.
- **URL filtering tools, which allow**, block, or filter access to particular websites according to organizational policies.
- **Application control systems**, which protect against unauthorized applications.

But these sophisticated capabilities come with a significant caveat. Implementing encryption and decryption is not a simple, low-cost fix, especially when using the 2048-bit RSA cipher keys mandated since January 2014.

SSL inspection generates a significant performance overhead on security and monitoring tools.

SSL inspection generates a significant performance overhead on security monitoring, application monitoring and security analytics tools. As the list of security and monitoring tools grows ever longer, inspecting encrypted traffic consumes more and more computing time. This in turn runs the risk of the security suite becoming a bottleneck, acting as a brake on the network or requiring a complete security suite upgrade in order to deliver the performance demanded by the business.

Research by Enterprise Strategy Group (ESG) in 2015[2] found that 24% of businesses said their networking team was suspicious of technology that might disrupt critical traffic or damage performance. Yet the processing overheads inherent in using security gateways to decrypt SSL traffic data, in addition to their normal duties, will usually have a significant performance impact — particularly as both the business and data volumes grow.

Next generation firewall experienced an average performance loss of 74% when using 512b and 1024b ciphers.

A test of seven next-generation firewalls conducted by NSS Labs[3], showed just how severe these performances problems are when inspecting SSL traffic in typical deployments:

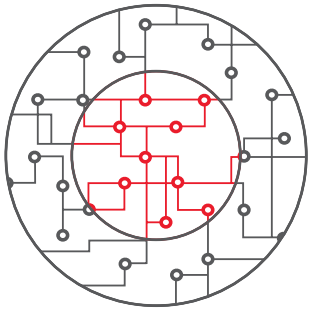
- The seven devices experienced an average performance loss of 74% when using basic 512b and 1024b ciphers, and 81% when using 2048b ciphers, which, as outlined above, have now become the mandated industry standard.
- The seven devices experienced an average transactions-per-second (TPS) loss of 86.8% with a 512b cipher, rising to 92% with a 2048b cipher.

Turning on encryption/decryption capabilities costs organizations dearly, both in performance losses and in terms of higher infrastructure costs.

Internal communications may constitute 80% of the encrypted traffic on your network.

Additional Challenges

And the challenges of encryption and decryption do not stop there. Additional operational and technical problems include difficulties in integrating SSL decryption and packet filtering technologies, and typically a lack of collaboration and cooperation between the IT security and the network management teams. SSL can also simply be a complex technology for even an expert IT security team to manage; certificate management, for example, can be a lengthy and difficult process.



Matters get even worse when you consider that firewalls, IPS and other typical security devices are usually only deployed at the edge of enterprise networks. This often leaves the internal network communications between servers, and between servers and clients, to go unexamined — and these internal communications may constitute 80% of the encrypted traffic on your enterprise network.

If malware should get inside the network, the SSL encryption will camouflage its activities. The business may not discover the infection for weeks or months: data could

2. http://www.networkworld.com/article/2890876/cisco-subnet/challenges-associated-with-ssl-tls-traffic-decryption-and-security-inspection.html
3. https://www.nsslabs.com/linkservid/13C7BD87-5056-9046-93FB736663C0B07A/

be stealthily exfiltrated, viruses and worms can be released, or malicious code can be installed. This is why enterprises need to look both at internally encrypted traffic as well as externally encrypted. Constant vigilance is now an essential requirement.

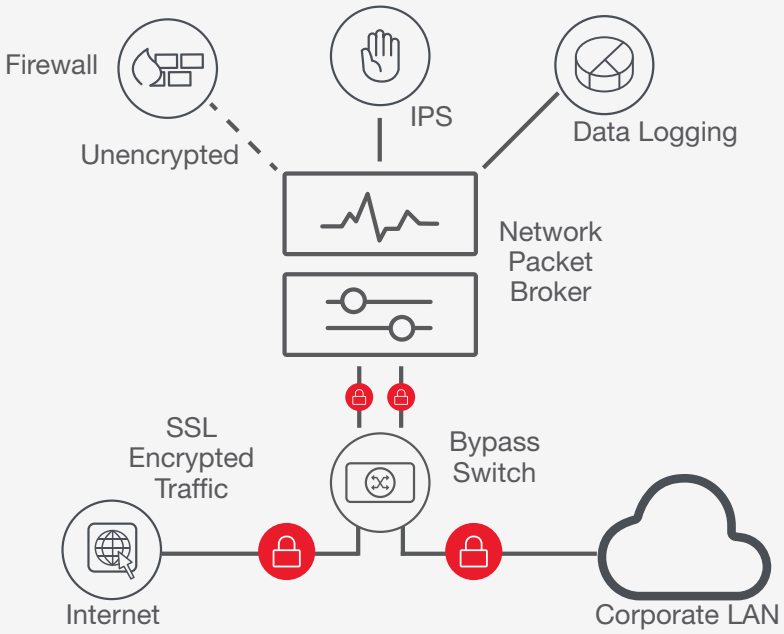
Searching For Solutions: A Network Visibility Architecture

So how can enterprises eliminate the network blind spots created by the added encryption security, and gain visibility of what might be lurking in that hidden traffic, without compromising their overall network performance? How can they ensure that internal traffic is receiving the same stringent inspections as external traffic?

The answer is a complete network visibility architecture, which collects, manages, and distributes packet streams for monitoring and analysis. This architecture must incorporate specific elements to examine SSL encrypted traffic, as follows.

Full, Unobscured Access: Stateful SSL Decryption

The key step in gaining visibility into SSL traffic is provisioning full, unobscured access to all traffic across physical, virtual and cloud environments. This is achieved by using stateful SSL decryption, which extends IT security teams' ability to look into encrypted traffic from both business and web applications, to reveal any hidden anomalies such as network reconnaissance attempts and intrusions, or malware.

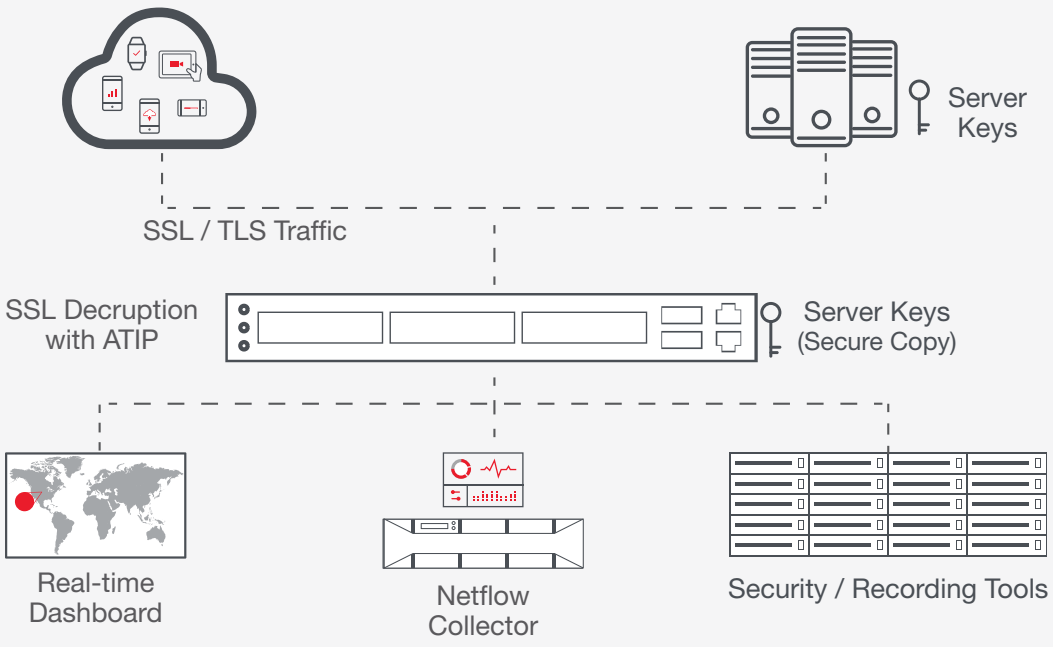


Bi-directional stateful decryption capability is essential, allowing organizations to look at both internal and external communications. Once the monitoring data is decrypted, application filtering can be applied and the information can be sent to dedicated, purpose-built security and monitoring tools (such as an IPS, IDS, SIEMs, network analyzers and so on).

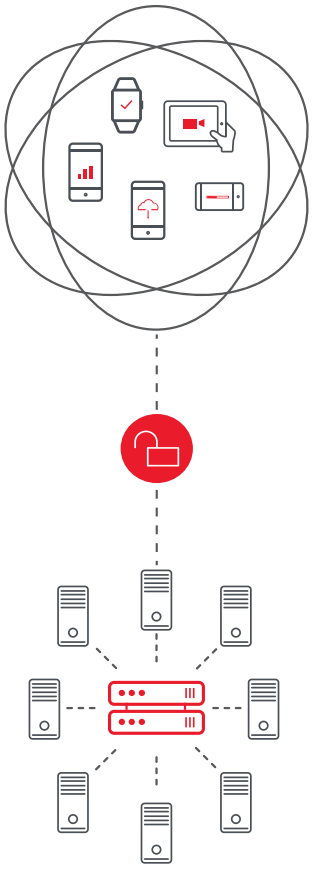
Stateful SSL decryption provides complete session information, helping IT teams to better understand the transaction as a whole and the potential start of any attacks. This is in contrast to stateless decryption that only provides the raw data packets.

The Decryption Platform: Intelligent Network Packet Brokers (NPBs)

The stateful SSL decryption should be done using a dedicated platform, such as a network packet broker (NPB), which supports application intelligence with SSL decryption. Application intelligence is the ability to monitor packets based on application type and usage. It can be used to decrypt network packets, and dynamically identify the applications running (along with any malware that may be hidden by the encrypted traffic) on a network. And since the decryption is performed on a high performance specialized platform, there is no impact on network performance, nor on the performance of firewalls or other security products.



Once the monitoring data is decrypted, application filtering can be applied and the information can be sent to the network's dedicated, purpose-built monitoring tools (such as IPS, IDS, SIEMs, network analyzers, etc.). This offloads the extra processing burden from these tools, maximizing their performance and capacity, and the applications they run, such as sandboxes and IPS by reducing their workload.



This in turn enables them to better identify and respond to targeted attacks, unlocking the full potential of security and network architectures and maximizing network availability and reliability, while giving IT and security teams full visibility of all network traffic, both encrypted and unencrypted.

Intelligent NPBs also perform a range of packet operations to preprocess data packets they pass on to monitoring tools, such as data deduplication and packet trimming, that are intended to reduce total solution cost by improving tool efficiency. An effective NPB intelligently processes all data packets — without losing any.

To summarise, using intelligent NPBs multiplies the effectiveness of existing enterprise security estates by inspecting all network traffic and transforming it into a format that the organization's existing security tools can use.

Intelligent NPBs, such as Ixia's Vision ONE which supports both inline and out of band traffic balancing can:

- Decrypt SSL traffic and feed it as stateful cleartext traffic to multiple security tools, boosting their performance.
- Identify applications using deep packet inspection, rather than just relying on protocol and port numbers that are easily faked, to send traffic to the best tool for securing a given application type.
- Process data flows to remove redundant data, such as duplicate packets that commonly occur when using multiple taps in a network, without losing any of the original information: again, removing brakes of performance.
- Support reliable use of multiple security products in an inline configuration to increase security and to match performance of different devices.

State of Inspection

SSL encryption plays a vital role in securing sensitive data against unlawful interception and hacking, enabling organizations to meet their compliance requirements. But it can also conceal security threats, and limit network teams' abilities to inspect, tune and optimize the performance of applications. It is vital that businesses protect the sensitive and customer-confidential data traffic on their networks; but it's equally essential that they eliminate the SSL encryption blind spots, and gain full visibility into what is truly happening in their networks and mission-critical applications. It is possible to achieve both with the right network visibility architecture.

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