WHITE PAPER

THE ULTIMATE GUIDE TO SSL/TLS DECRYPTION:

Six features to consider when evaluating SSL/TLS inspection solutions

TABLE OF CONTENTS

DISCLAIMER

EXECUTIVE SUMMARY

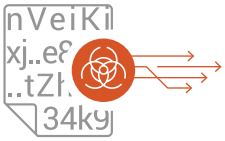
Encrypted traffic accounts for a large and growing percentage of all internet traffic. While the adoption of Secure Sockets Layer (SSL), and its successor, Transport Layer Security (TLS), should be cause for celebration – as encryption improves confidentiality and message integrity – these protocols also put your organization at risk as they create encrypted blind spots that hackers can use to conceal their exploits from security devices that are unable to inspect SSL/TLS traffic.

The threat of SSL/TLS blind spots is a serious one. According to a Ponemon survey[1], legacy security infrastructure is not built to take care of these evolved, hidden attacks, and almost two out of three organizations1 are not able to decrypt and inspect their SSL/TLS traffic.

To stop cyberattacks, you need to gain insight into encrypted data; to gain insight into encrypted data, you need a dedicated security platform that can decrypt SSL/TLS traffic and send it to the security stack for inspection in cleartext. This paper describes six features to consider when evaluating an SSL/TLS inspection platform. With this information, you will be able to easily define evaluation criteria and avoid common deployment pitfalls.

It is predicted that as much as

70% of cyberattacks will use encryption as part of their delivery mechanism by 2019.[3]



THE CURRENT STATE OF INSECURITY

Worldwide spending on information security will exceed a staggering $124 billion in 2019[2] as organizations stack up security products around their network perimeters. Unfortunately, as SSL traffic increases, our collective $124+ billion investment in security is falling far short of protecting all our digital assets.

Attackers are wising up and taking advantage of this gap in corporate defenses. In fact, as much as 70% of cyberattacks[3] will use encryption as part of their delivery mechanisms by 2019. As a result, companies that do not inspect SSL communications are providing an open door for attackers to infiltrate defenses and steal data.

Cybercriminals can use encryption to hide the delivery of malware as well as the extraction of data, which leaves legacy security devices blind to data breaches. Such breaches can have a disastrous impact on your company's reputation and brand, and you could be subject to disciplinary action and fines. For instance, over 200,000 computers worldwide were affected by last year's WannaCry[4] ransomware attack most notably, Britain's National Health Service (NHS), causing serious disruptions in the delivery of health services across that nation. To prevent cyberattacks, enterprises need to inspect all traffic and encrypted traffic in particular, for advanced threats such as WannaCry.

1 A10 survey by Poneman, Uncovering Hidden Threats Within Encrypted Traffic, January 2018
2 Gartner Forecast: Information Security, Worldwide, 2016-2022, 2Q18 Update
3 Cisco Blog: Enterprise Networks A Guide for Encrypted Traffic Analytics, October 2017
4 WannaCry, What is WannaCry ransomware, how does it infect, and who was responsible?, August 2018

EXISTING SECURITY SOLUTIONS CAN'T HACK IT

While some security solutions can decrypt SSL/TLS traffic, many are collapsing under growing SSL/TLS bandwidth demands and SSL key lengths. Today, the use of 2048-bit SSL keys has become common, and the impact is startling.

NSS Labs looked at how decryption impacts performance in its 2018 SSL/TLS Performance Tests[5]. They measured product performance with a Next Generation Firewall (NGFW) with decryption turned on versus turned off and found significant performance degradation and increased latency in the tested products.

- A 92% drop in the average connection rate. Connection degradation ranged from 84% to 99%.[5]
- An increase in latency in the average application response time of 672%. Latency ranged from 99% to 2,910%.[5]
- A 60% drop in the average throughput. Throughput degradation ranged from 13% to 95%.[5]

NSS Labs reports a

60% Drop in the average throughput of tested products.Throughput degradation ranged from **13% to 95%**.[5]

THE IMPORTANCE OF BEING EARNEST…WHEN EVALUATING SSL/TLS INSPECTION PLATFORMS

To eliminate the SSL/TLS blind spot in corporate defenses, you should provision a solution that can decrypt SSL/TLS traffic and enable all security products that analyze network traffic to inspect the encrypted data. You must carefully evaluate all the features and performance of your SSL/TLS inspection platform before selecting a solution. If you deploy an SSL/TLS inspection platform in haste, you might be blindsided later by escalating SSL bandwidth requirements, deployment demands or regulatory implications.

SSL traffic is growing, and it will continue to increase in the foreseeable future due to concerns about privacy and government snooping. Many leading websites today, including Google, Facebook, Twitter and LinkedIn encrypt application traffic. With SSL traffic accounting for a growing percentage of all internet traffic, you should factor in performance needs and future bandwidth usage when evaluating an SSL inspection solution. However, you should also make sure that your proposed architecture will comply with regulatory requirements such as the European Union's (EU's) General Data Protection Regulation (GDPR) or healthcare's Health Insurance Portability and Accountability Act (HIPAA).

5 NSS Labs, NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports, July 2018

TRAFFIC ENCRYPTION RATES TODAY

85%	90%	75%
Percentage of internet traffic in North America currently protected by encryption[6]	Percentage of pages loaded over HTTPS in Google Chrome[6]	Percentage of encrypted traffic through Mozilla Firefox[7]

SIX FEATURES TO CONSIDER WHEN SELECTING AN SSL/TLS INSPECTION PLATFORM

Because SSL/TLS inspection potentially touches so many different security products from firewalls and intrusion prevent systems (IPS) to data loss prevention (DLP), forensics, advanced threat prevention (ATP), and more, you should develop a list of criteria and evaluate SSL/TLS inspection platforms against these criteria before selecting a solution. An SSL/TLS inspection platform should:

#1

MEET CURRENT AND FUTURE SSL/TLS PERFORMANCE DEMANDS

Performance is one of the most important evaluation criteria for an SSL/TLS inspection platform. You need to assess current internet bandwidth requirements and ensure the inspection platform can also handle future SSL throughput requirements.

- Encrypted traffic is increasing faster than overall IP traffic growth, and more and more sites are using computationally intensive 2084-bit and 4096-bit SSL keys along with complex Elliptic-Curve Cryptography (ECC). Today, up to 85%[8] of the internet in North America is encrypted and that percentage is growing, so you should factor SSL traffic growth into your criteria.
- Test SSL/TLS inspection speeds with 2048-bit and 4096-bit SSL keys.
- Evaluate a mix of traffic with Diffie-Hellman and ECC for perfect forward secrecy (PFS).
- Make sure the SSL/TLS inspection solution has the ability to re-negotiate ciphers, especially weaker or deprecated ciphers to stronger ones, for continued security and availability.
- Ensure the SSL/TLS inspection platform can handle throughput requirements with extra headroom for traffic peaks.
- Ensure the SSL/TLS inspection platform can decrypt traffic across multiple ports and protocols.
- Analyze appliance performance with essential security and networking features enabled. Testing SSL/TLS decryption speeds without considering the impact of deep packet inspection (DPI), URL classification, or other features enabled will not provide a clear picture of real-world performance.

Basing an evaluation on these performance benchmarks should prevent surprises in your production environment.

6 Google Transparency Report, HTTPS encryption on the web, September 2018
7 *Let's Encrypt, Let's Encrypt Stats, September 2018
8 Google Transparency Report, HTTPS encryption on the web, September 2018

#2 SATISFY COMPLIANCE REQUIREMENTS

Privacy and regulatory concerns have emerged as one of the top hurdles preventing some organizations from inspecting SSL traffic. While your security team may have deployed a wide array of products to detect attacks, data leaks, and malware, and rightfully, so you have to walk a thin line between protecting your company's intellectual property without violating employees' privacy rights.

- Companies that don't comply with these regulatory rules can be subject to hefty fines and lawsuits. In a study by Ponemon Institute, 36%[9] of surveyed companies said compliance/regulatory failure was a major factor in justifying funding of their organizations' IT security budget. Forrester Research also recently reported that as many as "80% of companies will fail to comply with GDPR".[10]

To address regulatory requirements like GDPR, HIPAA, Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), and Sarbanes-Oxley (SOX), an SSL/TLS inspection platform should be able to bypass sensitive traffic, such as traffic to banking and healthcare sites. Once sensitive traffic is bypassed, you can rest easy knowing that confidential banking or healthcare records will not be sent to security devices or stored in log management systems.

Look for an SSL/TLS inspection platform that can:

- **Categorize web traffic using an automated URL classification service.** By categorizing web traffic, communications to certain sites can be bypassed to ensure that confidential data remains encrypted.
- **Filter traffic based on URL categories** to block access to known harmful websites.
- **Support manually-defined URL bypass lists** with hundreds of thousands of URL entries.
- **Support automated IP reputation services** to block access to known bad resources for added security right off the bat.
- **Display a customizable message to users** the first time they access the internet informing them that web traffic and encrypted traffic may be monitored for cyber threats and unauthorized activity.

#3 SUPPORT HETEROGENEOUS NETWORKS WITH DIVERSE DEPLOYMENT AND SECURITY REQUIREMENTS

You have to contend with a wide array of security threats from external actors as well as potential malicious insiders. Therefore, to safeguard digital assets, you need to deploy an ever-increasing number of security products to stop intrusions, attacks, data loss, malware, and more.

Some of these security products are deployed inline, while others are deployed non-inline as passive network monitors. Some analyze all network traffic, while others focus on specific applications, like web or email. However, virtually all of these products need to examine traffic in cleartext in order to pinpoint illicit activity. Recently, though, the rise in SaaS adoption has caused many applications to move to the cloud. Productivity and storage applications like Office 365, Box, Dropbox, G Suite, etc., are commonly used by many companies. However, many of these applications have their own security stacks in the cloud and, in the interest of a better user experience, SaaS vendors generally recommend bypassing on-premise security stacks.

9 Poneman Institute, The Third Annual Study on the Cyber Resilient Organization, March 2018
10 Forrester Research, Predictions 2018: Cybersecurity, November 2017

Look for an SSL/TLS inspection platform that can:

- **Decrypt traffic with multiple flexible deployment options.** An inspection platform should be able to support both transparent forward proxy configuration to transparently intercept traffic, as well as an explicit proxy configuration where browsers are explicitly configured to use an upstream proxy.
- **Intelligently route traffic with traffic steering.** The inspection platform should be able to forward traffic to multiple security devices based on source IP address, protocol, file type, URL, or other parameters. By supporting advanced traffic steering, an SSL/TLS inspection platform can optimize the performance of network security devices and support complex network architectures.
- **Granularly parse and control traffic based on custom-defined policies.** The support of scriptable, programmatic control over application traffic enables the inspection of request headers and payloads, plus performance of any number of actions, including blocking traffic, redirecting traffic, or modifying content.
- **Augment growing SaaS adoption.** A modern inspection solution should be able to differentiate between SaaS and non-SaaS traffic while supporting the rising volumes of SaaS traffic. It should have the ability to bypass SaaS traffic from the on-premise security stack, as is recommended by most SaaS vendors, and should be able to modify headers to support access control enforced by these SaaS vendors in the cloud to avoid data exfiltration.
- **Integrate with a variety of security solutions from leading security vendors.** By validating an inspection platform's interoperability, you can be assured the platform you choose will work seamlessly together with other security solutions and avoid surprises that could delay deployment. Integration with a variety of security solutions will also reduce overall costs and the need to deploy multiple point solutions.

You will need the flexibility to deploy best-of-breed security products from multiple vendors to prevent getting locked into a single vendor solution. The security landscape constantly evolves to combat emerging threats, and in one or two years, your company may want to provision new security products; your SSL/TLS inspection platform needs to be able to interoperate with these new products. An inspection platform that supports flexible deployment, traffic steering and granular traffic controls will be able to provision a wide range of security solutions into the future.

#4 *MAXIMIZE THE UPTIME AND THE OVERALL CAPACITY OF YOUR SECURITY INFRASTRUCTURE*

A security infrastructure blocks cyberattacks and prevents data exfiltration. If your security infrastructure fails, threats may go undetected and your company may be unable to perform business-critical tasks, resulting in loss of revenue and brand damage.

Most firewalls today can granularly control access to applications and detect intrusions and malware. Unfortunately, analyzing network traffic for threats is a resource-intensive task. While firewalls have increased their capacity over time, they often cannot keep up with network demand, especially when multiple security features like IPS, URL filtering, and virus inspection are enabled. Therefore, your SSL/TLS inspection platform should not just offload SSL processing from security devices, but should maximize uptime and performance of these devices.

When evaluating an SSL/TLS inspection platform, look for a platform that can:

- **Scale security deployments** with load balancing.
- **Avoid network downtime** by detecting and routing around failed security devices.
- **Support advanced health monitoring** to rapidly identify network or application errors.
- **Provide better value** by supporting N+1 redundancy rather than just 1+1 redundancy.

Your SSL/TLS inspection platform should not be another point product and should not introduce risk to your network. Instead, it should lower risk by maximizing the availability and the overall capacity of your security infrastructure. Only then can the full potential of your SSL/TLS inspection platform be unlocked.

#5 SECURELY MANAGE SSL CERTIFICATES AND KEYS

When providing visibility to SSL traffic, your SSL/TLS inspection solution must securely manage SSL certificates and keys. SSL certificates and keys form the basis of trust for encrypted communications. If they are compromised, attackers can use them for snooping on encrypted traffic and stealing data.

To ensure certificates are stored and administered securely, look for an SSL/TLS inspection platform that:

- **Provides device-level controls** to protect SSL keys and certificates.
- **Integrates with third-party SSL certificate management solutions** to discover, catalog, track and centrally control certificates.
- **Supports FIPS 140-2 Level 2 and Level 3 certified equipment and Hardware Security Modules (HSMs)** that can detect physical tampering and safeguard cryptographic keys.

#6 SIMPLY AND EASILY DEPLOY AND MANAGE YOUR ENTERPRISE SECURITY SOLUTION

When investing in either a firewall or a decryption solution, two of the biggest problems are the complexity and the lack of rich usable analytics. A solution that can be easily deployed allows your organization to become operational and prevent hidden threats as soon as possible. Unfortunately, most decryption solutions are too complex to be deployed easily. If your solution is deployed quickly, usually after paying hefty professional services fees, more problems can emerge; are the analytics provided with the solution humanly consumable and useful? Is the solution providing any usable insights?

When managing encrypted traffic, rich analytics with data delivered in an easy-to-consume format is critical in order to free up valuable human analysts to make effective and informed decisions. Real-time analysis provides deep insights into anomalies and threats in encrypted traffic, so adaptive controls and policy updates can be set through behavior analysis. Products from partners like Splunk may be deployed in your security network to capture insights into the traffic flowing through network devices.

Furthermore, as your organization grows and spreads to multiple, geographically-distributed deployments, a 'single pane of glass' solution becomes necessary to provide management and analytics available at a single centralized location. Simplicity becomes a must.

When choosing an SSL/TLS inspection solution, look for a platform that:

- **Is easy to use** and can be deployed in minutes.
- **Ensures the application of security best practices,** reducing human errors introduced during deployment.
- **Provides detailed real-time analytics** that will help in advanced troubleshooting.
- **Enables troubleshooting of issues** that you might have with the platform itself, with ease.
- **Provides customizable dashboards** that deliver tailored statistics widgets.
- **Provides a centralized management option** to support your organization as it grows, allowing all your geographically distributed deployments to be managed and analyzed from a central location.

CONCLUSION

As privacy concerns are propelling SSL/TLS usage, you face increased pressure to encrypt application traffic and keep data safe from hackers and foreign governments. In addition, because search engines such as Google rank HTTPS websites higher than standard websites, application owners are clamoring to encrypt traffic. At the same time, you face threats like cyberattacks and malware that can use encryption to bypass corporate defenses.

With SSL accounting for nearly 85%[11] of enterprise traffic in North America and more applications supporting bigger keys and complex ciphers like ECC for PFS, you can no longer avoid the cryptographic elephant in the room. If you wish to prevent devastating data breaches, you must gain insight into your SSL/TLS traffic. Since legacy firewalls are inefficient at decrypting and inspecting traffic simultaneously, creating bottlenecks in your network, a dedicated SSL/TLS inspection platform that will support your existing security infrastructure is necessary.

Before provisioning an SSL/TLS inspection solution, consider criteria like performance, flexibility, analytics, ease-of-use, and secure key management, which are critical to your organization's success. Armed with this information, you can make a well-informed decision and avoid the deployment pitfalls that SSL/TLS inspection can potentially expose.

11 Google Transparency Report, HTTPS encryption on the web, September 2018

LEARN MORE

To find out about SSL/TLS inspection solutions from A10 Networks, visit a10networks.com/products/ssl-inspection.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @A10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-WP-21116-EN-03 OCT 2018