WHITE PAPER

Uncover Threats in SSL Traffic: The Ultimate Guide to SSL Inspection

Table of Contents

Executive Summary

Encrypted traffic accounts for a large and growing percentage of all network traffic. While the adoption of SSL, and its successor, Transport Layer Security (TLS), should be cause for celebration – as encryption improves confidentiality and message integrity – it also puts organizations at risk. This is because hackers can leverage encryption to conceal their exploits from security devices that do not inspect SSL traffic.

How serious is the threat? According to a recent Gartner survey, "less than 20% of organizations with a firewall, an intrusion prevention system (IPS) or a unified threat management (UTM) appliance decrypt inbound or outbound SSL traffic."[1] This means that hackers can evade over 80% of companies' network defenses simply by tunneling attacks in encrypted traffic.

To stop cyber attacks, organizations must gain insight into encrypted data, and to do this, they need a dedicated security platform that can decrypt inbound and outbound SSL traffic. This paper describes five features that organizations should consider when evaluating SSL inspection platforms, enabling IT security teams to rapidly define evaluation criteria and avoid common deployment pitfalls.

The Current State of Insecurity

Worldwide spending on information security will reach a staggering $71.1 billion in 2014[2], as organizations stack up firewalls around their network perimeters and inspect incoming and outgoing traffic with an array of security products. Unfortunately, as SSL traffic increases, our collective $70+ billion investment in security is falling far short of protecting digital assets.

Attackers are wising up and taking advantage of this gap in corporate defenses. In fact, researchers at Gartner predict that "in 2017, more than half of the network attacks targeting enterprises will use encrypted traffic to bypass controls, up from less than 5%."[3] As a result, organizations that do not inspect SSL communications are providing an open door for attackers to infiltrate defenses and steal data. To prevent cyber attacks, enterprises need to inspect all traffic, and in particular encrypted traffic, for advanced threats.

Existing Security Solutions Can't Hack It

While some security solutions can decrypt SSL traffic, many are collapsing under growing SSL bandwidth demands and SSL key lengths. The transition from 1024- to 2048-bit SSL key lengths was triggered by NIST publication 800-131A, and the impact is startling. Analysis by NSS Labs reveals that decrypting traffic with 2048-bit SSL ciphers "caused a mean average of 81% in performance loss"[5] for seven leading next-generation firewalls. If organizations wish to repurpose their firewalls for SSL decryption, they must consider the performance impact on those firewalls.

The Importance of Being Earnest…When Evaluating SSL Inspection Platforms

To eliminate the SSL blind spot in corporate defenses, organizations should provision solutions that can decrypt SSL traffic – both inbound traffic to corporate servers and outbound traffic from internal users to the Internet – and allow all security products that analyze network traffic to inspect encrypted data.

Organizations must carefully evaluate the features and performance of SSL inspection platforms before selecting a solution. If IT security teams deploy SSL inspection platforms in haste, they 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. But it's not just the web giants that are encrypting communications; 48% more of the million most popular websites used SSL in 2014 than a year earlier.[7]

With SSL traffic accounting for a growing percentage of all Internet traffic, IT security teams must factor in performance needs and future bandwidth usage when evaluating SSL inspection solutions. They should also make sure that their proposed architecture will comply with regulatory requirements like the Health Insurance Portability and Accountability Act (HIPAA).

[1] Gartner, Security Leaders Must Address Threats from Rising SSL Traffic, December 2013
[2] Gartner, Forecast: Information Security, Worldwide, 2012-2018, 3Q14 Update
[3] Gartner, Security Leaders Must Address Threats from Rising SSL Traffic, December 2013
[4] Gartner, Security Leaders Must Address Threats from Rising SSL Traffic, December 2013
[5] NSS Labs, SSL Performance Problems, June 2013
[6] NSS Labs, SSL Performance Problems, June 2013
[7] Netcraft, January 2014 Web Server Survey

5 Features to Consider When Selecting an SSL Inspection Platform

Because SSL inspection potentially touches so many different security products – from firewalls and intrusion prevent systems (IPS) to data loss prevention (DLP), forensics, advanced threat prevention and more – organizations must develop a list of criteria and evaluate SSL inspection platforms against these criteria before selecting a solution. This paper describes five features that all SSL inspection platforms should provide, enabling IT security teams to rapidly define evaluation criteria and avoid common deployment pitfalls.

SSL inspection platforms should:

1. Meet Current and Future SSL Performance Demands

Performance is perhaps the most important evaluation criteria for SSL inspection platforms. Organizations must assess their current Internet bandwidth requirements and ensure that their SSL inspection platform can handle future SSL throughput requirements.

While IP traffic is predicted to grow 21 percent per year between 2013 and 2018,[8] organizations must also factor in SSL traffic growth. SSL traffic currently accounts for between 25 and 35% of all Internet traffic and reaches upwards to 70% for some networks.[9] Moreover, encrypted traffic is increasing faster than overall IP traffic growth, and more and more sites are using computationally intensive 4096-bit SSL keys and Diffie-Hellman ciphers.

When evaluating SSL inspection performance, IT security teams should:

- Test SSL inspection speeds with 2048-bit and 4096-bit SSL keys.
- Evaluate a mix of traffic with Diffie-Hellman and elliptic curve ciphers.
- Ensure that the SSL inspection platform can handle throughput requirements, with extra headroom for traffic peaks.
- Analyze appliance performance with essential security and networking features enabled. Testing SSL decryption speeds without considering the impact of deep packet inspection (DPI), URL classification or other features will not provide a clear picture of real-world performance.

Those organizations that thoroughly evaluate performance benchmarks should be able to avoid surprises in their production environments.

2. Satisfy Compliance Requirements

Privacy and regulatory concerns have emerged as one of the top hurdles preventing organizations from inspecting SSL traffic. While IT security teams have deployed a wide array of products to detect attacks, data leaks and malware – and rightfully so – they must walk a thin line between protecting employees and intellectual property, and violating employees' privacy rights.

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

IT security teams should look for SSL inspection platforms that can:

- Categorize web traffic using an automated URL classification service. By categorizing web traffic, organizations can bypass communications to banking and healthcare sites and ensure that confidential data remains encrypted.
- Support manually-defined URL bypass lists with hundreds of thousands of URL entries.
- 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

Organizations must contend with a wide array of security threats from external actors and from disgruntled employees. To safeguard their digital assets, organizations have deployed 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, whereas others focus on specific applications, like web or email protocols. However, virtually all of these products need to examine traffic in clear text in order to pinpoint illicit activity.

[8] Cisco, The Zettabyte Era: Trends and Analysis

[9] NSS Labs, SSL Performance Problems, June 2013

As a result, SSL inspection platforms should interoperate with a diverse set of security products from multiple vendors. They should support transparent deployment and be able to route traffic from one security device to another with traffic steering.

Organizations should look for SSL inspection platforms that can:

- **Decrypt outbound traffic to the Internet and inbound traffic to corporate servers with multiple, flexible deployment options.** They should support transparent forward proxy configuration, transparently intercepting traffic, as well as an explicit proxy configuration, where browsers are explicitly configured to use a proxy. They should also support reverse proxy deployment to decrypt traffic to corporate servers and allow inline or non-inline security devices to inspect the traffic.
- **Intelligently route traffic with traffic steering.** The SSL 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 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.** By supporting scriptable, programmatic control over Layer 7 traffic, administrators can inspect request headers and payloads and perform any number of actions, including blocking traffic, redirecting traffic or modifying content.
- **Integrate with a variety of security solutions from leading vendors.** By validating interoperability, IT security teams can be assured that their SSL inspection platform will work together seamlessly with other security solutions and avoid surprises that could delay deployment. By integrating with a variety of security solutions, organizations can also reduce costs by eliminating the need to deploy multiple point solutions.

Organizations want to deploy best-of-breed security products from multiple vendors; they do not want to get locked into a single vendor solution. The security landscape constantly evolves to combat emerging threats. In one or two years, organizations may want to provision new security products and they need to make sure that their SSL inspection platform will interoperate with these products.

By selecting an SSL inspection platform that supports flexible deployment, traffic steering and granular traffic controls, they will be able to provision their choice of security solutions in the future.

4. Maximize the Uptime and the Overall Capacity of Security Infrastructure

Organizations depend on their security infrastructure to block cyber attacks and prevent data exfiltration. If their security infrastructure fails, threats may go undetected and users 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 network-borne 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, SSL inspection platforms should not just offload SSL processing from security devices. They should also maximize the uptime and performance of these devices. When evaluating SSL inspection platforms, organizations should look for platforms 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

SSL inspection platforms should not be another point product and they should not introduce risk to the network. Instead, they should lower risk by maximizing the availability and the overall capacity of security infrastructure. Only then can organizations unlock the full potential of their SSL inspection platforms.

5. Securely Manage SSL Certificates and Keys

Whether providing visibility to outbound or inbound SSL traffic, SSL inspection devices 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 to impersonate legitimate sites and steal data.

When SSL inspection devices are deployed in front of corporate applications to inspect inbound traffic, they may need to manage tens, hundreds or even thousands of certificates. As the number of SSL key and certificate pairs grows, certificate management becomes more challenging. Organizations constantly add, remove or redeploy servers to meet business needs. This fluid and dynamic environment makes it difficult for organizations to account for all SSL certificates at any given time and ensure that certificates have not expired.

To ensure that certificates are stored and administered securely, organizations should look for SSL inspection platforms that:

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

Conclusion

Privacy concerns are propelling SSL usage higher; businesses 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 better than standard websites, application owners are clamoring to encrypt traffic. But IT security teams face their own set of challenges as they tackle threats like cyber attacks and malware – threats that can use encryption to bypass corporate defenses.

With SSL accounting for nearly a third of enterprise traffic[10] and with more applications supporting 2048-bit and 4096-bit SSL keys, organizations can no longer avoid the cryptographic elephant in the room. If they wish to prevent devastating data breaches, they must gain insight into SSL traffic. And to accomplish this goal, they need a dedicated SSL inspection platform.

This guide describes criteria that organizations should consider before they provision SSL inspection technologies – criteria like performance, availability and SSL key management which will be critical to their success. Armed with this information, organizations can make well-informed decisions and avoid the deployment pitfalls that SSL inspection can potentially expose.

Learn More

To find out about SSL inspection solutions from A10 Networks, visit http://www.a10networks.com/products/ssl_insight.php

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-WP-21115-A4-01
Nov 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.