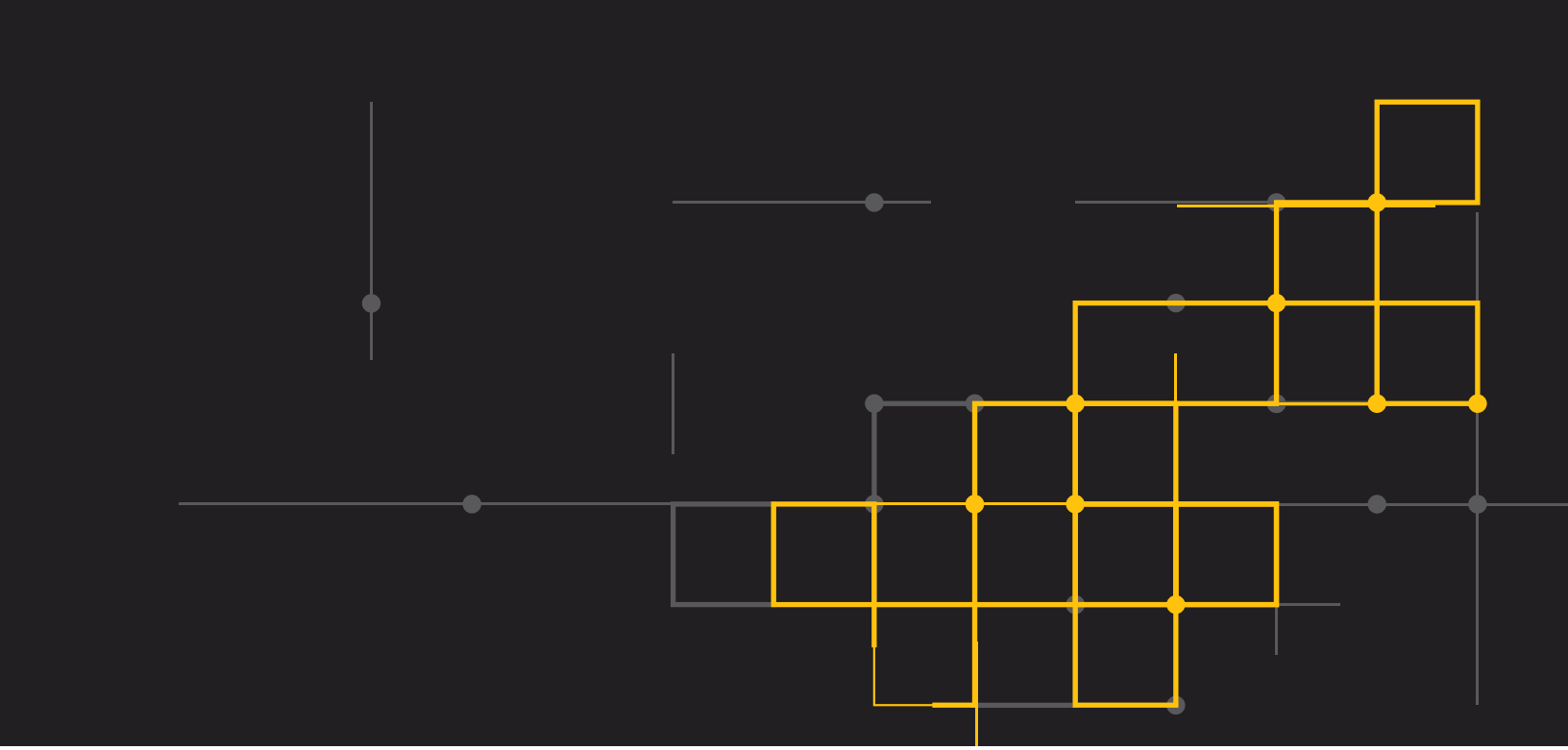

Cost-Effective, Flexible Visibility and Control of SSL/TLS Network Traffic

Five reasons to use an SSL Visibility Appliance instead of your NextGen Firewall (NGFW) or Application Delivery Controller (ADC)

The Critical Choice for Visibility into SSL Traffic

Cybersecurity experts agree that to protect enterprise data and networks from hackers and cybercriminals it is essential to inspect network traffic encrypted with the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols.[1] Corporate employees use SSL-encrypted applications for social media and entertainment, for both sanctioned and unsanctioned corporate collaboration, and for a wide variety of private and corporate ecommerce and business apps. All of these uses provide vectors into the network for malware and malicious network traffic. They also expose protected personal data and confidential corporate information. The stakes will only get higher: industry analysts estimate that by the end of 2017 70% of global Internet traffic, and 50% of network attacks, will be encrypted, mostly using SSL.[2]

[1] For simplicity we will use "SSL" to refer to all varieties of SSL and TLS.
[2] Sandvine: *2016 Global Internet Phenomena Spotlight: Encrypted Internet Traffic and Gartner: Are Cyber-criminals Hiding in Your SSL Traffic?*
[3] The Sprawl: tls and ssl cipher suites.

Symantec™

Examples of Applications Using SSL

Social Media and Entertainment
Facebook, Twitter, YouTube, LinkedIn

Collaboration and Office Productivity
Google Apps, Microsoft Office 365 and SharePoint, Box, WebEx, Slack, HipChat

Ecommerce and Business Apps
Online banking, healthcare, government, ADP Payroll, Salesforce.com, GitHub

Networking
Virtual private networks (VPNs), secure FTP

The "why" of SSL traffic inspection is settled. But the "how" remains a big question.

At first glance, the easiest option would seem to be performing SSL decryption on existing security devices. Many Next Generation Firewalls (NGFWs) now include SSL decryption as one security feature among many. Some application delivery controllers (ADCs) can decrypt and re-encrypt SSL traffic, in addition to their load balancing and traffic acceleration features. There should be advantages to leveraging these existing investments.

On closer examination, however, most of these advantages turn out to be illusory. SSL decryption dramatically reduces the capacity of multi-purpose security devices. That means IT organizations need to buy, install and manage more devices – sometimes many more. In addition, ADCs require complex scripting and testing to deploy SSL decryption, and often networks must be reconfigured.

In practice, dedicated SSL Visibility Appliances can provide SSL encryption that is far more cost effective and easier to manage, as well as more secure, more flexible, and better for policy and privacy compliance. This paper describes how to effectively manage encrypted traffic and achieve these results;

1. Superior Performance and Cost Effectiveness
2. Simplified Management and Configuration
3. Strong Security
4. Comprehensive Policy and Privacy Compliance
5. Unmatched Flexibility and Integration

The Technical Challenges

Providing visibility into SSL traffic in an enterprise environment is not as simple as merely tapping into a network pipe, finding the right key, and decrypting packets. In fact, there are many complex challenges to providing strong security with SSL traffic. An SSL security solution must be able to:

- Handle traffic encrypted using different versions of the SSL and TLS protocols, with several key exchange algorithms, including RSA and Diffie-Hellman (DHE and ECDHE), as well as a wide range of cipher suites such as AES, AES-GCM, DES, 3DES, CHACHA and RC4. Over 200 SSL and TLS protocols have been cataloged,3 and while most of them are obsolete technically, many can still be found in use, and new ones are being introduced all the time.
- Monitor SSL traffic arriving through any port; not only standard ports, such as 443, 465, 990, 993 and 995, but obscure ports used by new application types and by hackers trying to evade traditional security devices.
- Decrypt outbound as well as inbound traffic, in order to identify hacker command and control (C&C) communications originating inside the network, and to enable data loss protection (DLP) products to inspect information leaving the network via webmail and other encrypted applications.
- Share decrypted traffic with multiple security solutions, such as DLP, intrusion prevention systems (IPS), malware analysis and sandbox products, forensics tools and others.
- Decrypt SSL traffic selectively, to conform and comply with regulatory and corporate policies mandating that healthcare, financial and other types of protected personal information always remain encrypted while "in motion."
- Preserve data integrity by preventing hackers from modifying traffic "in flight"; that is, between the time it is decrypted for inspection and the time it is re-encrypted for transmission to the destination.
- Provide detailed logs of SSL sessions and events, in case audit or information chain of custody issues arise.

Figure 1 illustrates two scenarios that support these requirements using dedicated appliances for SSL visibility. Figure 2 shows the architectures when ADCs and NGFWs are used to decrypt SSL traffic.

The next sections of this paper explore how SSL Visibility Appliances, NGFWs, and ADCs compare for meeting goals such as performance and cost-effectiveness, management, security and policy compliance.

Expert Opinions

"…organizations which need to decrypt substantial network traffic tend to quickly crush the performance of existing security devices if they try to decrypt on them… If you have plenty of performance headroom on existing devices you can afford the overhead of decryption. If you don't you will need to look at another device to offload decryption load, in order to let your security devices do what they do best: inspect traffic, apply policies, and monitor or capture traffic."

Securosis: *Security and Privacy on the Encrypted Network*

"Another choice [as an alternative to SSL-inspection appliances] is using a multifunction gateway that can also perform decryption. The advantage is a reduction in the number of devices an organization must buy and manage. The downside is that, given current processor limitations, asking one device to do too many tasks can and does slow down network performance or the detection of possible threats. This is particularly true when decryption is involved."

SANS Analyst Whitepaper: Finding Hidden Threats by Decrypting SSL

"NSS has concerns for the viability of SSL inspection in enterprise networks without the use of dedicated SSL decryption devices."

NSS Labs Analyst Brief: SSL Performance Problems

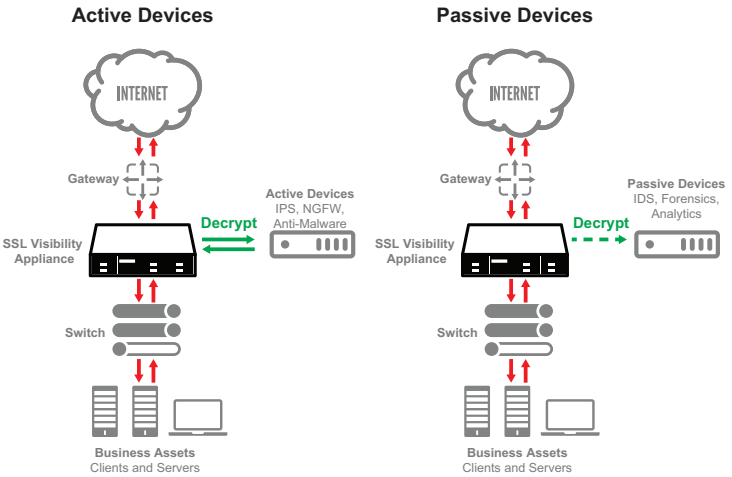

Figure 1: SSL Visibility Appliance decrypts SSL traffic and feed multiple active and passive devices

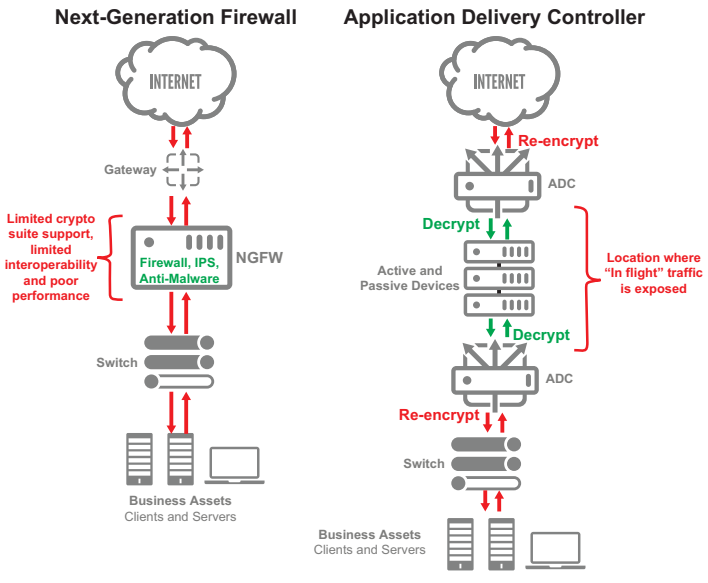

Figure 2: NGFWs and ADCs can decrypt SSL traffic, but NGFWs can't share data with other active devices, and decrypted traffic between ADCs is exposed and vulnerable to modification.

Performance and Cost-Effectiveness

SSL visibility appliances are designed and optimized for one task: encrypting and decrypting SSL traffic based on established policies with maximum efficiency. In contrast, NGFWs and ADCs are general-purpose devices that are optimized for their primary tasks, such as processing firewall and IPS rules (NGFWs) or load balancing network traffic (ADCs).

The best known laboratory test of the impact of decryption on next generation firewalls found that enabling 2048 bit ciphers on eight leading NGFWs caused an average performance loss of 81%. For three of the tested systems the performance loss exceeded 90%.[4] Another recent test of a leading NGFW found that simply adding 50% HTTPS to the mix of traffic degraded throughput by 83%.[5]

These studies indicate that SSL decryption reduces the peak traffic supported by a NGFW to less than 20%, meaning that up to five units are required to handle the same level of traffic as advertised by the vendor.

SSL visibility appliances also offer significant cost advantages over ADCs. A single SSL visibility appliance can decrypt and re-encrypt traffic for multiple security devices simultaneously. As shown in Figures 2, ADCs are typically configured with one unit decrypting traffic before inspection and a second unit re-encrypting traffic before transmission to the destination. Enterprises have to purchase, configure, and manage multiple units – incurring increased cost and complexity.

Management

As noted in our earlier discussion of technical challenges, most enterprises need to be able to decrypt SSL traffic selectively, based on policies, to avoid violating regulatory and corporate privacy rules. Policies can also produce major performance improvements by allowing "safe" traffic to bypass encryption and inspection.

SSL Visibility Appliances include tools to create and manage sophisticated policies with a simple, point-and-click graphical user interface (GUI). Most NGFWs and ADCs don't have a comparable feature. The only way to implement sophisticated policies is with complex scripts. Writing, deploying and updating these scripts can be a major burden for administrators. Executing the scripts also consumes significant processing power on devices.

In addition, SSL visibility appliances allow for extremely granular SSL session logs, including complete records of each SSL handshake and cipher suite used, and logging of exceptions related to dropped sessions, SSL failures, invalid certification, and sessions not decrypted for policy reasons. These detailed logs are valuable for audits, for forensics, and for network trouble-shooting and capacity planning. NGFWs and ADCs typically only provide detailed logging in debug mode or with complex scripts.

Security

SSL visibility appliances are designed to detect and decrypt SSL traffic entering and leaving through all ports, regardless of the protocol uses. Most NGFWs and ADCs only monitor SSL traffic that comes through "standard" ports and that matches the expected protocol for each port (e.g. HTTPS on port 443, SMTPS on port 465, FTPS on port 990, IMAP over SSL on port 993, and POP3 over SSL on port 995). NGFWs and ADCs have no visibility into protocols they don't support, so they are blind to SSL communications used by new types of web, cloud and mobile applications and by hackers seeking to avoid detection.

NGFWs are designed to decrypt SSL traffic only for their own internal security modules, as shown in Figure 2. They cannot share traffic with external active devices such as IPSs and anti-malware packages from other vendors. Some have a limited ability to share decrypted traffic with passive devices through a tap, but others can't. For the most part, organizations that rely on NGFWs for SSL decryption lock themselves into a single security vendor and are unable to take advantage of best-of-breed solutions from other sources.

Many NGFWs support only a limited range of cryptographic ciphers and key management schemes. In contrast, leading SSL visibility appliances support 70 or more cipher suites – virtually all of the ones that most enterprises will encounter.

Because decryption degrades NGFW performance so quickly, attackers can launch a denial of service (DOS) attack simply by targeting a NGFW with high volumes of SSL traffic. SSL visibility appliances protect against these DOS attack, because they can decrypt high volumes of SSL traffic before it reaches the firewall.

[4] NSS Labs: Analyst Brief – SSL Performance Problems.
[5] Tests performed by Symantec.

SSL Visibility Appliances can be configured to prevent SSL sessions from being established if they use weak or obsolete cipher suites such as SSL v3.0, DES and RC4. This ensures that only traffic encrypted with up-to-date, secure methods will be forwarded.

SSL Visibility Appliances have no IP address on network ports, so they cannot be targeted by hackers for denial of service attacks like NGFWs and ADCs.

Finally, ADCs can create data integrity gaps. As shown in Figure 2, there is a vulnerability gap between the location traffic is decrypted for inspection by the first ADC, and the location it is re-encrypted for transmission to the destination by the second ADC. In between, an attacker can modify the traffic "in flight" by altering packets or injecting malware code. For example, a banking transaction transferring a million dollars to bank account 123456789 could be changed to divert the funds to account 987654321. A cybercriminal could accomplish this by compromising one of the devices between the ADCs, or even by compromising a script on the first ADC. The second ADC will re-encrypt and forward whatever packets it receives; it has no way of validating them against the original traffic decrypted by the first ADC.

SSL Visibility Appliances are not vulnerable to this type of attack, because they do not re-encrypt and forward the packets that have flowed through the active security devices. Rather, if the active devices provide a verdict that traffic is safe, the SSL Visibility Appliance re-encrypts and forwards the original packets, which have never left the appliance.

In addition, the SSL Visibility Appliance re-encrypts the sessions using the same key exchange and protocol suite as the original web server. This makes the entire decryption, inspection and re-encryption process more secure as there is no cypher suite downgrade.

These capabilities not only improve security, they also allow organizations to demonstrate data integrity if audit or chain of custody questions arise.

Policy Compliance

Not surprisingly, SSL Visibility Appliances are designed to make it as easy as possible to create and manage policies for decrypting SSL traffic. This includes an intuitive graphic user interface to define policies based on:

- Detailed characteristics of the SSL traffic stream, such as source IP address, destination IP address, certificate authority status, and destination TCP port
- White lists and blacklists
- The category and reputation of the sending or destination web site

These capabilities are extremely important for meeting privacy and compliance requirements, including explicit and implicit privacy mandates in HIPAA, FISMA, PCI DSS, SOX and other standards. In many cases, certain types of traffic must remain encrypted across an entire organization, for example, employee communications with healthcare and personal banking web sites. In other cases, policies must be applied selectively, for example, to business units in nations with more rigorous privacy policies, or to groups like HR and legal that handle protected data and insider information.

Most NGFWs and ADCs do not allow for decryption to be applied selectively at a granular level. Others can enforce sophisticated policies only with the use of complex command line scripts that are difficult to create and maintain. Many of these vendors expect customers to rely on online communities for support. Online communities are an improvement over writing scripts from scratch, but they force administrators to search for, test, support and update scripts themselves, rather than having a pre-built, supported solution from the vendor.

Flexibility

SSL Visibility Appliances are designed to fit into a wide variety of networks and address all types of SSL decryption use cases. NGFWs and ADCs were created to play specific roles in a network that, for technical or economic reasons, do not align with all use cases for SSL decryption.

For example, SSL Visibility Appliances feature a "decrypt once, feed many" design that allows them to feed both active security devices such as NGFWs, IPS, and anti-malware products, and passive devices such as DLP solutions, malware sandboxes, SIEMs and security analytics and forensics tools, all at the same time. Under some circumstances SSL Visibility Appliances can also be deployed "out of band" to decrypt incoming traffic for passive devices. Furthermore, they are designed to work with security and analytics products from different vendors, without special customization, proprietary application programming interfaces (APIs) or integration services. Enterprises can avoid being locked into security suites from any one vendor.

As mentioned earlier, NGFWs are very limited in terms of deployment options. They decrypt traffic only for their own internal security modules, and in a few cases for external passive devices. These limitations prevent customers from using best-of-breed security devices from other vendors.

In addition, SSL Visibility Appliances can be deployed quickly and easily when enterprises grow, reconfigure their infrastructure, and find new areas that require SSL decryption. They can be "dropped in" without requiring IP address or topology changes or modifications to client IP and web browser configurations.

Summary

Today it is essential to decrypt and inspect SSL traffic in order to protect enterprise data and networks from hackers and cybercriminals.

At first glance, performing SSL decryption and re-encryption on existing next generation firewalls or application delivery controllers would seem like a good way to minimize costs and complexity. On closer examination however, it can be seen that dedicated SSL visibility appliances are more cost effective and easier to manage, as well as being more secure, better for policy compliance, and more flexible.

Tests have shown that decrypting SSL traffic can degrade NGFW performance by more than 80%, multiplying the number of units that need to be purchased and managed to support a given level of network traffic. In addition, fewer SSL Visibility Appliances are needed because a single unit can feed multiple security devices and both decrypt and re-encrypt the same traffic.

For IT Security administrators, SSL Visibility Appliances offer tools to create and manage sophisticated policies with a comprehensive point-and-click interface instead of complex scripts. In addition, they provide granular SSL session logs with more information for audits, forensics, and network trouble-shooting.

For better security, SSL Visibility Appliances can detect and decrypt SSL traffic entering and leaving through all ports, using a very wide range of cryptographic cipher suites and key management schemes. Unlike NGFWS, they can feed active and passive security devices from many vendors. They ensure better data integrity than ADCs because attackers can't modify traffic "in flight" before re-encryption.

For policy compliance, SSL Visibility Appliances can enforce privacy and compliance rules at a very granular level, without having to create and maintain complex scripts.

Finally, SSL Visibility Appliances maximize flexibility, because they address all types of SSL decryption use cases, support the widest variety of security and analytics products, and are transparent to intermediate network elements, end devices, and end users.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_wp_Flexible_Visibility_and_Control_of_SSL_Traffic_EN_v1a