WHITE PAPER: August 2024

# 3 Myths that Cloud the Path to Modern SSL / TLS Encryption

vmware by Broadcom

## Table of Contents

## ABOUT THIS DOCUMENT

This whitepaper shows the critical importance of modern SSL / TLS encryption. In busting three popular myths, this paper examines the use of hardware vs. software for encryption, the selection of network performance monitoring tools, and the performance and security implications of RSA versus ECC. Avi Load Balancer not only provides the latest SSL / TLS encryption, but also delivers enterprise-grade visibility, ease of use, and reliability for all use cases.

## EXECUTIVE SUMMARY

As security breaches and vulnerabilities increase, enterprises must ensure their data is protected. As SSL / TLS encryption standards have improved significantly over the past few years, hardware load balancers cannot always provide the strongest protections with scale, security and visibility. This whitepaper examines three SSL / TLS myths, and shows how VMware® Avi™ Load Balancer easily enables SSL / TLS security while providing visibility, ease of use, and security for all use cases.

- Myth #1: Software cannot perform SSL / TLS encryption at scale.
- Myth #2: Security does not affect network performance monitoring.
- Myth #3: If I use RSA, my applications are safe.

## WHAT ARE SSL AND TLS?

Today, HTTP is mostly only used to redirect clients to HTTPS. Browsers now consider HTTP to be considered insecure and warn users accordingly. Secure sockets layer (SSL) and transport layer security (TLS) are cryptographic protocols that safeguard digital communication by authenticating website identities and encrypting data between clients and servers. Although the terms SSL and TLS are used interchangeably, technically SSL is deprecated and TLS refers to an updated, more secure version of SSL.


Figure 1: Load Balancer Acts as the SSL Proxy

SSL / TLS plays a critical role in load balancing. Load balancers act as a SSL / TLS proxy, terminating the client encrypted traffic in order to make load balancing decisions based on underlying application information such as HTTP cookies or URI paths. (see Figure 1)

Load balancers must support SSL / TLS and the dynamic landscape of frequently changing security threats to the SSL / TLS protocol. Additionally, they must do this at very high scale, able to handle unpredictable capacity to adapt to the changing needs of the business.

Even with heightened security protocols, however, hardware and traditional appliance models remain a bottleneck for load balancers to meet modern SSL / TLS requirements.

This paper will explore three common myths that cloud the path to modernizing SSL / TLS.

## MYTH #1:
## Software cannot perform SSL / TLS encryption at scale.

Initially, high-end (e.g. Apache) servers performed 12-17 SSL transactions per second with a 512-bit RSA key. However, early SSL encryption did not allow for much scale until the first hardware-based acceleration of SSL with the iPivot, which processed 300+ SSL transactions per second on a 1u appliance.

The innovation continued until the standardization of Octeon chips used for SSL processing – Octeon chips were eventually adopted by all load balancer vendors on their hardware appliances. However, today's applications advance at a pace much faster than what hardware can deliver, with increasing requirements for scale and security. Besides, the largest internet sites like Google, Amazon use software-based encryption.

## TRUTH #1:
## The largest internet sites rely on software-based encryption because:

### A) Software-based encryption is more secure.

Over the years, SSL / TLS capabilities and technology standards have updated after significant breaches. However, the fact that SSL processing chips are "hardcoded" to a version of hardware appliances makes it prohibitively costly to upgrade each time new security technology or updates are introduced. Inevitably, enterprises are stuck with hardware several generations behind, leaving load balanced applications vulnerable for attacks. Vulnerabilities only worsen as security breaches, and associated risks, increase in frequency.

**TECH CORNER**

Avi is software! Avi easily updates and runs the latest and most secure ciphers, standard revisions and tools. Users can instantly update to newer versions of TLS or from RSA to ECC (see Myth #3).

### B) Software-based encryption is more scalable.

Hardware load balancers cannot easily scale the number of SSL transactions performed unless additional hardware capacity is acquired. Capacity management and procurement processes slow down the ability to support the application growth and traffic spikes. With software load balancers, on the other hand, a single click is all it takes to automatically scale out or scale in on demand.

**TECH CORNER**

Avi can instantly scale from zero to millions of SSL transactions per second within minutes by scaling out the number of service engines – literally creating new load balancers (on the fly) that are all conveniently managed from the Avi Controller.

### C) Software-based encryption is less expensive.

Due to their lack of scale, legacy load balancers are sized and purchased based on projected SSL / TLS requirements. As a result, overprovisioning and low utilization is not uncommon. Enterprises must purchase load balancers in anticipation of peak traffic, even if most hardware sits idle during normal traffic.

**TECH CORNER**

Unlike its hardware counterparts, Avi does not force enterprises to decide how many SSL transactions per second they will require five years from now; instead, Avi allows enterprises to flexibly scale according to real-time needs.

## MYTH #2:
## Security does not affect network performance monitoring.

Perfect Forward Secrecy (PFS) refers to a key agreement protocol that prevents "man-in-the-middle" attacks (see Figure 2). Without PFS, one private key is used for all client connections and can be used to decrypt traffic after the fact. For example, TCPdump or packet captures can be decrypted if hackers or government agencies acquire the private key. With PFS, the private key is used to generate an ephemeral session key, which is discarded immediately at the end of the session. Since the discarded session key cannot be recreated, traffic encrypted with PFS cannot be decrypted after the fact.

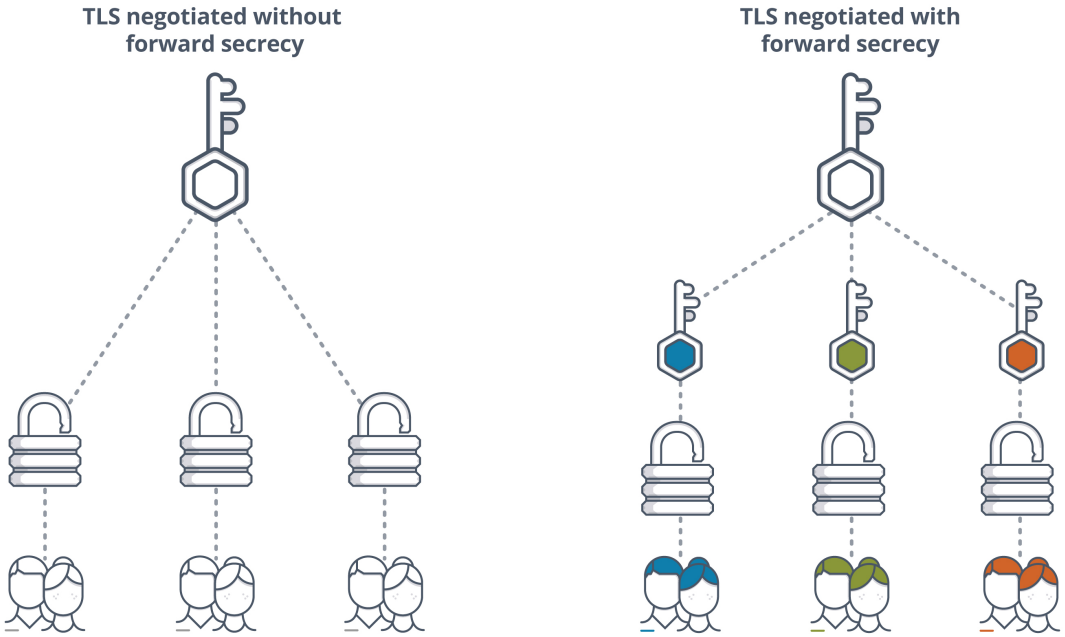


Figure 2: TLS negotiated with or without PFS

As a side effect, however, PFS also blinds traditional cipher / intrusion detection system (IDS) / intrusion prevention system (IPS) tools, making real-time monitoring and troubleshooting difficult (see Figure 3).

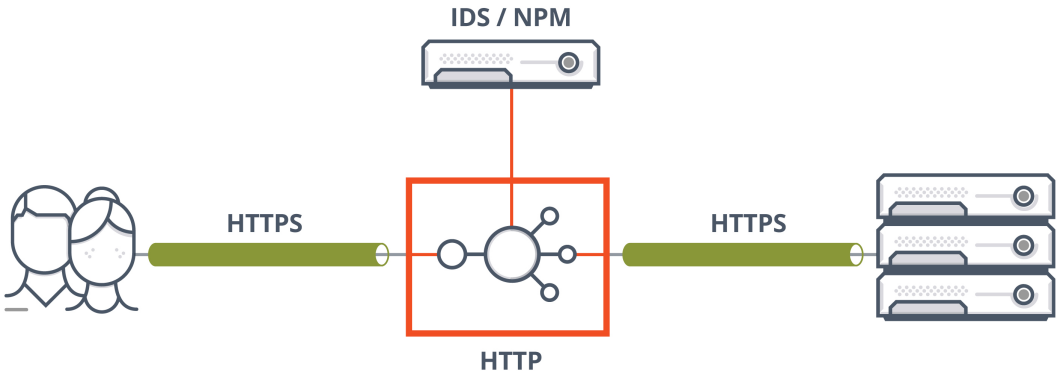


Figure 3: Analytics and monitoring tools are blinded by PFS

## TRUTH #2:
## Security increases influence on monitoring tools selection because:

### A) Hardware-based SSL termination prevents PFS adoption.

Increasingly, many security standards – including the latest version of TLS (1.3) – require PFS. For older ASICs that cannot perform PFS, SSL termination has to be done in software on CPUs.

**TECH CORNER**

Avi not only performs SSL termination completely in software, but also takes advantage of enhancements like the Intel Advanced Encryption Standard New Instructions (AES-NI) that significantly improve performance.

### B) Load balancers complement NPM / APM while securing applications.

Although Avi Load Balancer does not completely replace all network performance monitoring (NPM) / application performance monitoring (APM) capabilities, it complements NPM/APM with built-in telemetries from the distributed Avi Service Engines (data plane), while the Avi Controller acts as the central encryption/decryption point in the network.

**TECH CORNER**

Avi provides significant visibility and analytics for enterprises:

- Hundreds of metrics for every virtual service
- As many as billions of data points per day on traffic that can be exported directly
- Ability to mirror traffic from peer either unencrypted or re-encrypted with connection to IDS or NPM, which can then decrypt the connection and read client's traffic

## MYTH #3:
## If I use RSA, my applications are safe.

Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are the two most widely used public-key encryption algorithms. RSA has been around longer (first published in 1977), and it is dramatically more susceptible to padding attacks and side channel attacks during secure key negotiation between client and server. This is a primary factor in TLS 1.3 removing more RSA operations from the TLS key exchange process. Future TLS versions will deprecate RSA altogether.

As the new kid on the block, ECC entered widespread use circa 2004-2005. ECC is not necessarily free from all attacks or completely secure, but:

- ECC is substantially more secure. Default ECC uses 256-bit keys, which provides equivalent strength of an 3k RSA key. ECC also provides better support for PFS.
- ECC provides 2.5 - 3x better performance for negotiating new connections, especially on the server side (where the load balancer is). Enterprises can achieve 3,000 TSL transactions per second per CPU core with ECC certificates, versus 1,000 with RSA certificates (exact numbers will depend on CPU).
- ECC is less expensive to compute. A typical ECC certificate uses a 256-bit key, whereas a typical RSA certificate uses a 2048-bit key.

## TRUTH #3:
## Enterprises need to use ECC because:

As indicated above, RSA is slowly going defunct. In fact, TLS 1.3 already started deprecating components of RSA – although RSA certificates are still usable, key exchange and other elements are slowly being replaced. TLS 1.3 requires load balancers to support ECC and PFS. Moreover, enabling PFS has a lesser effect on performance (~15%) when ECC is used, rather than when RSA is used (~40%).

Certificate authorities still hand out RSA certificates by default, but enterprises can simply indicate that ECC is desired. All internet browsers already support ECC.

**AVI TECH CORNER**

Avi prioritizes ECC by default, but enterprises can customize preferences by reordering ciphers. Avi also allows for concurrent RSA and ECC certificates on virtual services.

## HOW AVI LOAD BALANCER PROVIDES ADVANCED SSL

VMware Avi Load Balancer delivers multi-cloud application services with elastic application delivery, security, and pervasive analytics across data centers and clouds (see Figure 4). Avi makes it easy to apply load balancing, web application firewall and service mesh to any application.

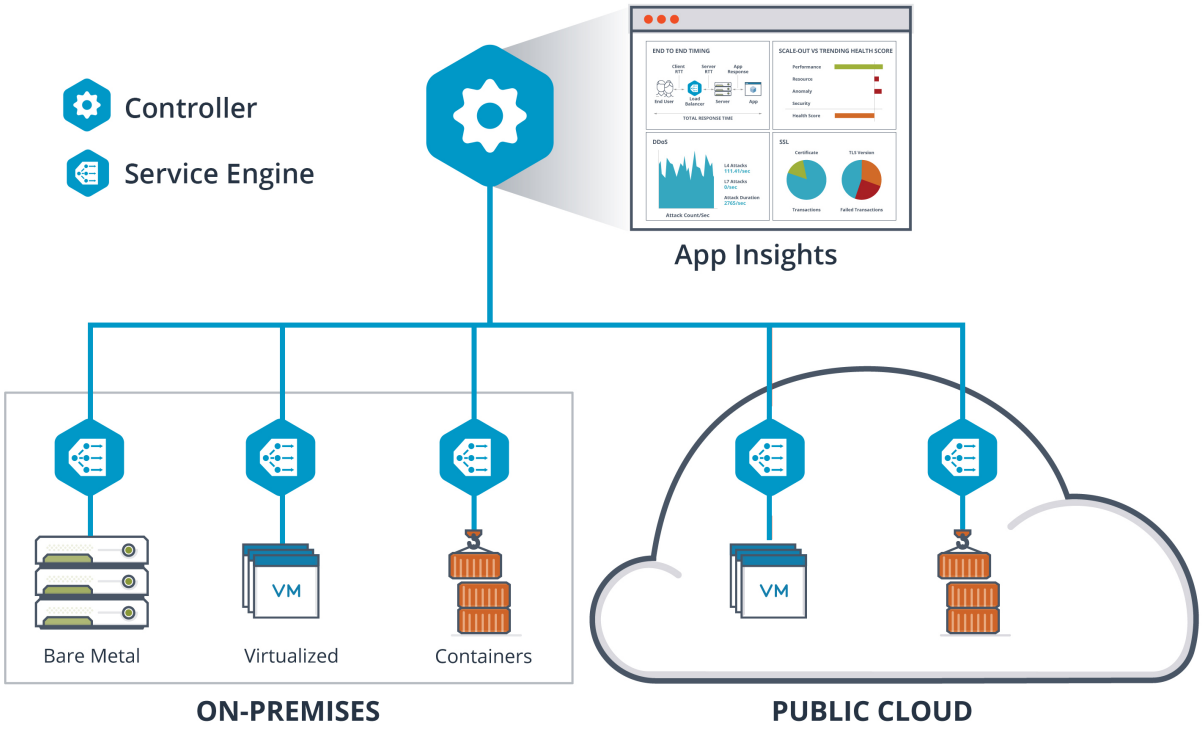


Figure 4: Multi-Cloud Load Balancing and Application Services

### Visibility and Automation

#### Log analytics

Avi Load Balancer tracks all logs of transactions and all actions taken on the site. Users can filter by specific timeframes, drill deeper in any transaction to see particular ciphers used, browser versions used, etc. Also, Avi allows users to filter by criteria like PFS support, computational support level, and compatibility. For example, percentage of clients who will negotiate with a particular SSL certificate (see Figure 5).

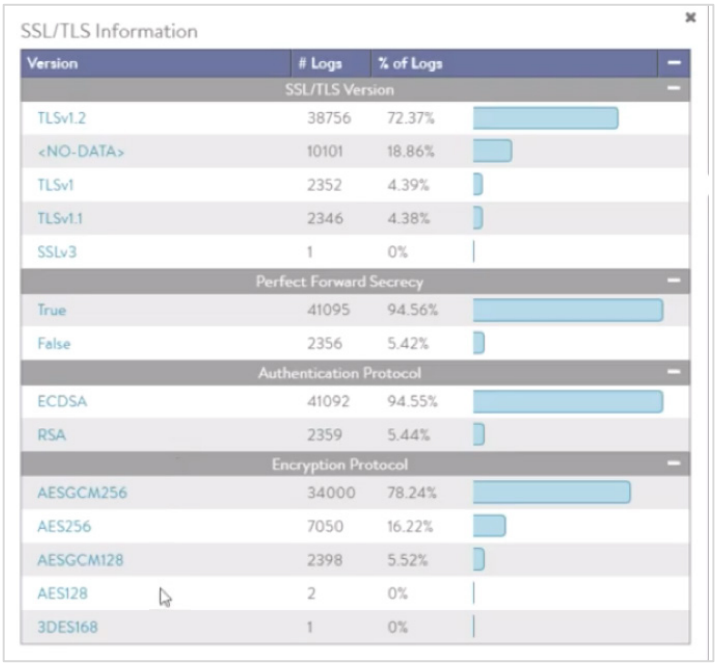


Figure 5: Security Insights from Logs

### Visibility for SSL certificates

With traditional load balancers, users are responsible for appending intermediate certificates to an intermediate certificate bundle. Incorrect certificates cause sites to load more slowly. Avi automatically builds a chain of trust without requiring manual construction of the chain or knowledge of certificate dependencies. Often, clients find that sites load faster because Avi automates this process and places certificates in the correct order (see Figure 6).

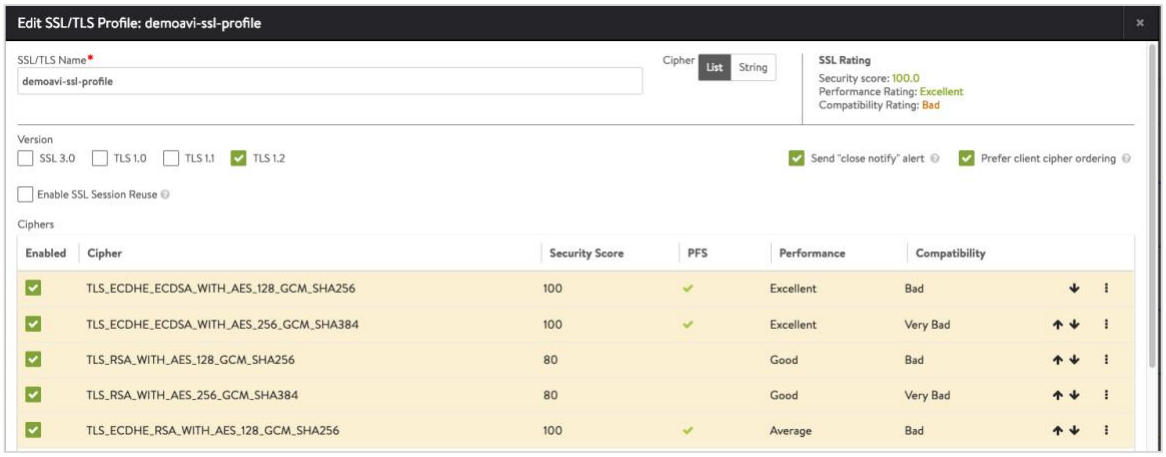


Figure 6: SSL / TLS Certificate Management

## Ease of use

### Point-and-click policy

Avi Load Balancer simplifies everything to a checkbox! Users can effectively and conveniently set guardrails around enterprise applications. Advanced data scripting allows for granular customization if desired (e.g. 301 instead of 302 status codes). Figure 8 shows examples on how to enable SSL Everywhere, including HTTP to HTTPS redirect, HSTS protocol and more with simple clicks. And see Figure 9 for more advanced customization on policy configurations.

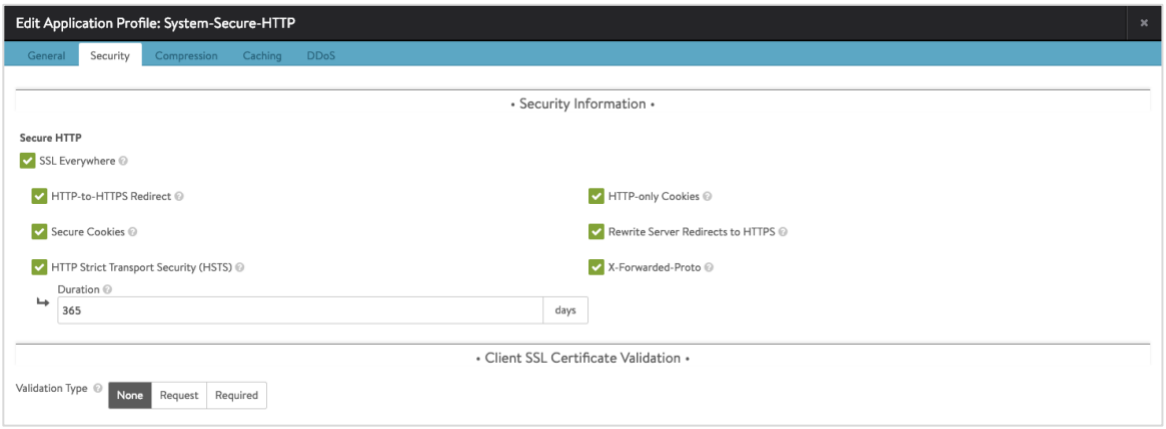


Figure 7: Security Options for SSL

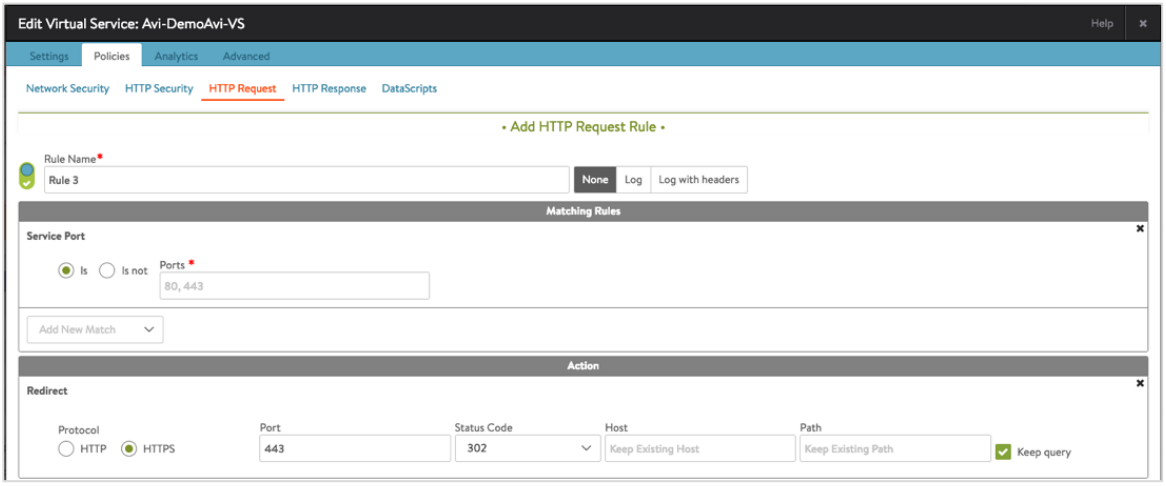


Figure 8: Policy-Based HTTP Request Customization

### Automated certificate renewal

Soon-to-expire certificates incur a security health score penalty, alerting users. Avi can send automated syslogs, Slack messages, or emails at 30-day, 7-day, or 1-day intervals. Furthermore, Avi integrates with certificate authorities and can make proper API calls to automatically renew certificates before expiration dates, and will send alerts if renewal efforts fail. For enterprises that have tens of thousands of certificates, Avi greatly simplifies the hassle of keeping track of nitty gritty details.

## Reliability

### Secure methods for viewing private keys

Avi Load Balancer stores certificates and keys in the Controller's database, not in Service Engines. Thus, attempts to obtain certificates or private keys by hacking hard drives from the load balancer SEs will prove unsuccessful. Additionally, passphrases ensure that keys are not exportable in clear text, and can only be exported by accounts with WRITE access. Unless export_key = True, private keys are always scrubbed in the GET API. An event is logged in the audit trail whenever private keys are exported. HSMs are supported for FIPs compliance.

### SSL score and security penalties

Enterprises shouldn't have to rely on third-party tools to determine if a load balancer is doing its job. Avi generates an SSL score that measures the performance and security of the site. Quickly pinpointing problems, Avi enables easier troubleshooting when users instantly know where to dive deeper. Avi also generates a security penalty that notifies of vulnerabilities with green, yellow, and red color codes. To avoid causing chaos and negatively impacting clients, Avi does not automatically drop support when vulnerabilities are detected, but allows users to retain full control.


Item No: vmw-bc-wp-tech-temp-uslet-word-2024 1/24