CHALLENGES

- Even with recent focus on application and web security, many websites still have weak implementations of SSL/TLS.
- Main reasons for weak SSL implementations include lack of infrastructure and browser support, performance penalty, and implementation complexity.
- Legacy hardware load balancers cannot scale elastically, and are capped at speeds that are punitively tied to acquisition costs.

SOLUTION

- The Avi Vantage Platform natively implements server name indication (SNI) infrastructure, HTTP Strict Transport Security (HSTS), RSA and Elliptic Curve Cryptography (ECC) certificates, and Perfect Forward Secrecy (PFS) with point-and-click features.
- Avi leverages instructions within current generation CPUs for AES-NI (New Instructions), providing stronger performance and dramatic improvements in SSL TPS numbers.

BENEFITS

- Avi Vantage elastically autoscales its Service Engines (SEs), distributing compute-intensive workloads (like SSL processing) across multiple SEs and their CPU resources.
- Avi is currently able to process 5 million SSL TPS with ECC certificates, and expects that number to double within a year and to double again every few years afterwards.

SSL EVERYWHERE

Best Practices for improving enterprise security without impacting performance

Although increased attention has been focused on application and web security recently, many websites still have weak implementations of Secure Socket Layer (SSL) / Transport Layer Security (TLS). Lack of infrastructure and browser support, performance penalty, and implementation complexity have been the primary reasons for the dearth of stronger SSL implementations. However, with recent advances in the SSL protocol, as well as significant performance improvements of SSL on commodity x86 platforms, stronger SSL can be – and should be – everywhere. Avi Networks Application Delivery Controller (ADC) natively supports these new capabilities to maximize application security without sacrificing performance.

NEW ACRONYMS IN THE WORLD OF SSL

Server Name Indication (SNI)

Virtual hosting with SSL is a chicken-and-egg problem. The client sends an SSL Hello, and the server must send back the SSL public key. If there are multiple domain names attached to the same IP address, a client that supports Server Name Indication (SNI) sends the hello along with the requested domain name. The server can now send back the proper SSL response. Other workarounds have existed for this, such as wildcard certificates, but all have had limitations. SNI has now become prevalent enough among client browsers that it has become safe to utilize.

Avi Networks Implementation: A parent virtual service (VS) is created, which contains the SNI default certificate. It also contains pointers to child virtual services. If the client's SSL Hello matches the domain for the child, that will be used; if not, the parent VS is used. This allows statistics to be tracked on a per (child) VS basis, as well as across the entire SNI infrastructure (parent, which includes the child VS stats).

HTTP Strict Transport Security (HSTS)

This feature indicates to client browsers that they should only access this site via HTTPS, not HTTP. This is used to mitigate man-in-the-middle attacks, particularly from open Wi-Fi connections. HSTS is sent to client browsers via an HTTP header, along with a length of time HSTS should be considered true (See Figure 1).

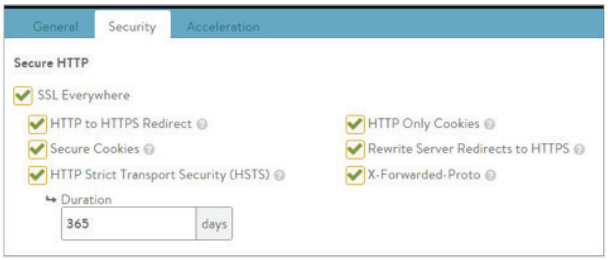

Figure 1: Configuration of SSL Everywhere on Avi Networks ADC

Avi Networks Implementation: HSTS is a simple way to increase the SSL security of a site. Within the application profile, simply enable the HSTS checkbox, or just click the SSL Everywhere checkbox to enable SSL best practices (Fig. 1).

Elliptic Curve Cryptography (ECC)

Historically, SSL/TLS has been performed using RSA certificates. Elliptic Curve Cryptography (ECC) certificates are based on newer algorithms – which are significantly more secure, less computationally expensive, and now supported by every current browser. Most hardware-based crypto accelerators do not support ECC, though, so legacy environments may be required to upgrade before utilizing the newer certificates.

Avi Networks Implementation: Both RSA and ECC certificates are supported, even both at the same time (Fig. 2). Normal browsers will negotiate ECC, while older browsers will use RSA. This guarantees compatibility, while ensuring the best performance and security (See Figure 2).

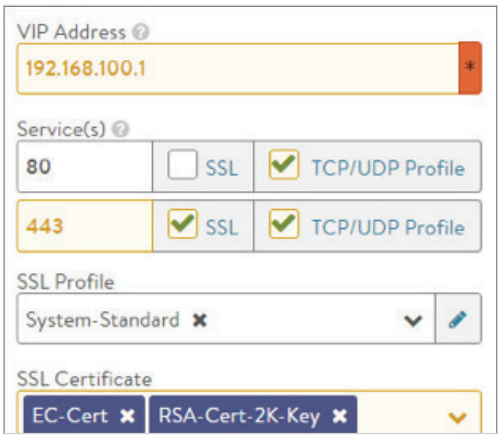

Figure 2: Configuring ECC on Avi Networks ADC

Perfect Forward Secrecy (PFS)

SSL ensures that communication between client and server is secure and encrypted. But if a session is recorded, and an attacker acquires the server certificate after the fact, the attacker can replay and decrypt recorded sessions. Recent examples include the National Security Agency (NSA) forcing companies to turn over SSL keys so that it can monitor private sessions or emails. With PFS, a master key is used to generate a unique, one-time-use key for each session. After the session, the ephemeral key is discarded, ensuring that a recorded session cannot be decrypted later. PFS has been around for a while, but using legacy RSA certificates imposes a heavy computational cost. Adoption of the newer ECC certificates allows PFS at near zero additional CPU cost.

Avi Networks Implementation: The default SSL cipher settings prioritize PFS for clients, regardless of whether they negotiate via RSA or ECC. Rather than use default settings optimized for maximum throughput, Avi Networks ADC prioritizes maximum security for SSL. If more throughput is needed, Avi Networks ADC can easily compensate by simply adding capacity on demand. Avi Networks ADC also provides rich visibility into clients' SSL interaction – you can see which browser versions are negotiating with PFS (See Figure 3).

Version	# Logs	% of Logs
Perfect Forward Secrecy		
True	595	80.73%
False	142	19.27%
Authentication Protocol		
ECDSA	595	80.73%
RSA	142	19.27%

Figure 3: Real-Time Visibility into Client SSL Interactions

SPDY

As a transitional technology towards faster internet, Google has pushed the SPDY protocol to improve the performance of HTTP. While SPDY is primarily intended to improve performance, one caveat is that it also requires SSL in order to negotiate over HTTP/1.1. This has contributed to the SSL Everywhere mantra, ensuring all web sites are utilizing SSL/TLS encryption.

HTTP/2

With the success and rapid adoption of SPDY, the Internet governing bodies have finally adopted a set of standards that comprise the next generation of the HTTP protocol. HTTP/2 is a technical extension of SPDY, with a few key differences. One difference is that the HTTP/2 RFC does not require SSL encryption. However, many of the browser vendors are unsatisfied with this decision, so browsers such as Chrome and Firefox will only negotiate HTTP/2 if the site is encrypted, otherwise they will downgrade to HTTP/1.1. This will lead to a fair bit of confusion over whether SSL is required for HTTP/2 or not. To ensure that all clients can take advantage of the performance improvements of HTTP, best practice is to encrypt all HTTP communications.

SSL PERFORMANCE

> **On our production frontend machines, SSL/TLS accounts for less than 1% of the CPU load, less than 10 KB of memory per connection and less than 2% of network overhead. Many people believe that SSL/TLS takes a lot of CPU time and we hope the preceding numbers will help to dispel that.**
>
> **Adam Langley,**
> **Google "Overclocking SSL"**

Historically, SSL TPS (transactions per second) were a critical bottleneck for the performance and sizing of a load balancer, and required custom hardware for crypto acceleration. However, with new crypto algorithms, advances in x86 CPU performance, and next-generation software architectures such as Avi, SSL performance on commodity x86 servers is no longer an issue.

Crypto Performance

SSL Performance on x86 Platform (2x 8core CPUs)	
RSA 2K certificates	8,000 SSL TPS
ECC certificates	32,000 SSL TPS

Table 1: ECC Performance on x86 Servers is 4x Better

Commodity x86 platform provides better performance for ECC certificates than for RSA certificates (Table 1). A single server can support up to 10Gbps of SSL throughput.

x86 and Moore's Law

Avi Networks ADC leverages instructions within current generation CPUs for AES-NI (New Instructions), which provide better performance using instruction sets native in the CPUs. Following Moore's Law, with dramatic increases in CPU capabilities, new servers introduced into a server farm will continue to dramatically improve the SSL TPS numbers.

Avi Vantage Platform Architecture

Built on software-defined principles, the Avi Vantage Platform is able to scale its micro load balancers (Service Engines or SEs) by distributing workloads across multiple SEs. Think of it as automatically load balancing the load-balancing infrastructure. This allows compute-intensive workloads, such as SSL, processing to be distributed across multiple SEs and their CPU resources.

Today, the Avi Networks ADC system can process 5 million SSL TPS with ECC certificates. Avi Networks expects that number to double within a year, and, with advances in CPU technology, to continue to double again every few years. Compare that to a legacy hardware load balancer, which is statically capped at speeds that are punitively tied to acquisition costs.

RECOMMENDATIONS

SSL Everywhere

SSL should be mandatory for any HTTP application. SSL is easy to enable, and the costs of SSL certificates are negligible for the security they bring. In a system such as Avi Vantage, this represents a few clicks to security.

Third-Party Validation

Enabling SSL is the first task. The next is to ensure correct configuration. This can be daunting, which is why a remarkable number of sites are poorly secured. Third-party tools exist to help by scanning the SSL-enabled site and providing recommendations for better security. These include browser plug-ins or SSL testing services. Or if you are using Avi Networks ADC, it will automatically rate your SSL score based on security, performance, and client compatibility, and provide suggestions for improving your configuration.

Try Avi

Naturally, the best way to simplify the task of improving SSL security for your applications is to deploy them behind Avi Networks ADC. The software is quick to download and easy to deploy. Check it out at https://avinetworks.com/try-avi.

RECOMMENDED READING

SNI

- http://en.wikipedia.org/wiki/POODLE
- https://groups.google.com/a/chromium.org/forum/#!msg/security-dev/Vnhy9aKM_l4/E0G5VPlb9B4J

HSTS

- https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

ECC

- https://arstechnica.com/information-technology/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

PFS

- https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy
- https://vincent.bernat.im/en/blog/2011-ssl-perfect-forward-secrecy

HTTP/2

- http://arstechnica.com/information-technology/2015/02/http2-finished-coming-to-browsers-within-weeks/

SSL Performance

- https://istlsfastyet.com/

Third-Party Validation

- https://www.ssllabs.com/ssltest/
- https://addons.mozilla.org/en-US/firefox/addon/calomel-ssl-validation/reviews/