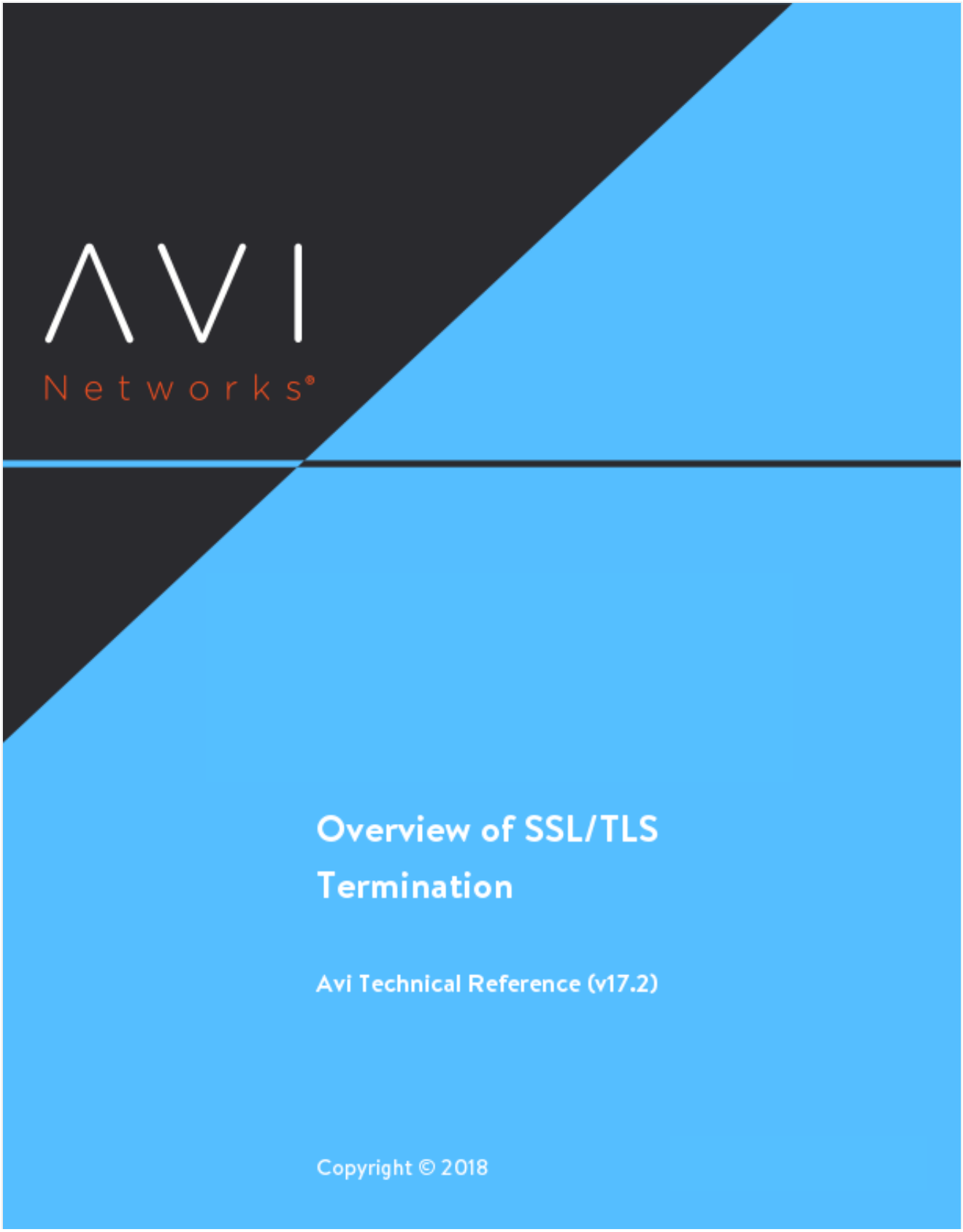

Overview of SSL/TLS Termination

Avi Technical Reference (v17.2)

Overview of SSL/TLS Termination

view online

Avi Vantage fully supports termination of SSL- and TLS-encrypted HTTPS traffic. The SSL and TLS names are used interchangeably throughout the documentation unless otherwise noted.

Using Avi Vantage as the endpoint for SSL enables it to maintain full visibility into the traffic and also to apply advanced traffic steering, security, and acceleration features. The following deployment architectures are supported for SSL:

- None: SSL traffic is handled as pass-through (layer 4), flowing through Avi Vantage without terminating the encrypted traffic.
- Client-side: Traffic from the client to Avi Vantage is encrypted, with unencrypted HTTP to the back-end servers.
- Server-side: Traffic from the client to Avi Vantage is unencrypted HTTP, with encrypted HTTPS to the back-end servers.
- Both: Traffic from the client to Avi Vantage is encrypted and terminated at Avi Vantage, which then re-encrypts traffic to the back-end server.
- Intercept: Terminate client SSL traffic, send it unencrypted over the wire for taps to intercept, then encrypt to the destination server.

Configuring SSL/TLS Termination

Avi Vantage supports multiple architectures for terminating SSL traffic. For client-to-Avi-Vantage SSL, the configuration is done on the virtual service page. For Avi-Vantage-to-server SSL encryption, the configuration is performed by editing the pool. For either, a virtual service or pool must be configured with an SSL profile and an SSL certificate, described below.

Virtual Service Configuration

- Pool Configuration
- Server Name Indication (SNI)

SSL Profile

The profile contains the settings for the SSL-terminated connections. This includes the list of supported ciphers and their priority, the supported versions of SSL/TLS, and a few other options.

- SSL Profile
- App Transport Security
- SSL Version Support
- Configure Strong SSL Cipher Strength

SSL Certificate

An SSL certificate is presented to a client to authenticate the application. A virtual service may be configured with two certificates at the same time, one each of RSA and elliptic curve cryptography (ECC). A certificate may also be used for authenticating Avi Vantage to back-end servers.

- SSL Certificates
- EC versus RSA Certificate Priority
- Notification of Certificate Expiration
- Client Certificate Validation / PKI Profile
- Physical Security for SSL Certificates

- Thales nShield Integration

SSL Performance

The performance of SSL-terminated traffic is dependent on the underlying hardware allocated to the Avi Service Engine, the number of SEs available to handle the virtual service, and the certificate and ciphers settings negotiated. As a general rule of thumb, each vCPU core can handle about 1000 RSA 2K transactions per second (TPS) or 2500 ECC SSL TPS. A vCPU core can push about 1 Gb/s SSL throughput. SSL-terminated concurrent connections are more expensive than straight HTTP or layer 4 connections, and may necessitate additional memory to sustain high concurrency.

- SSL Performance
- SE Memory Consumption

Additional Topics

SSL is a complicated subject, occasionally requiring redirects, rewrites, and other manipulation of HTTP to ensure proper traffic flow. Avi Vantage includes a number of useful tools for troubleshooting and correcting SSL-related issues. They are described in the articles below.

- SSL Everywhere
- HTTP to HTTPS Redirect
- SSL Visibility and Troubleshooting