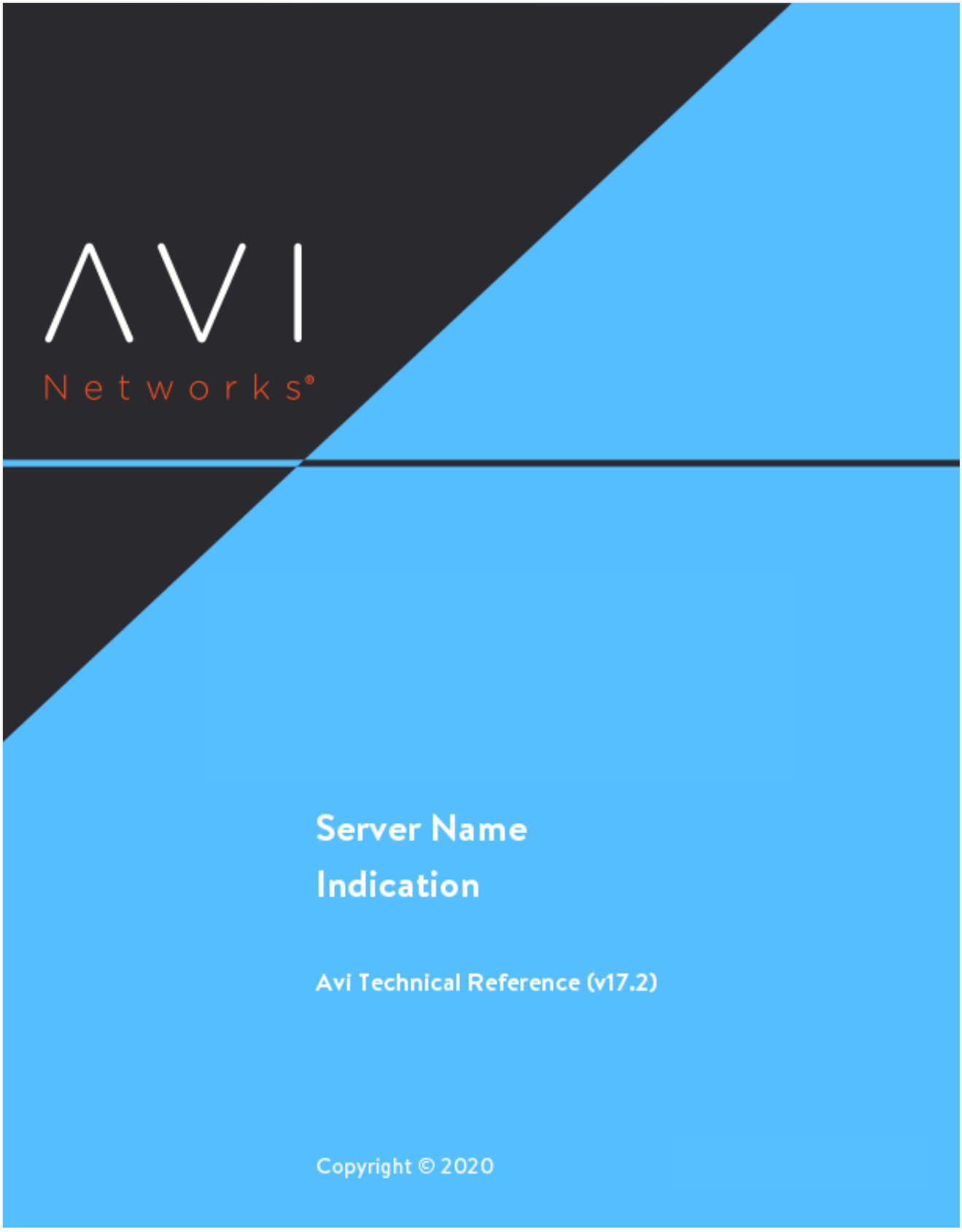


Server Name Indication

Avi Technical Reference (v17.2)

Server Name Indication

view online

Overview

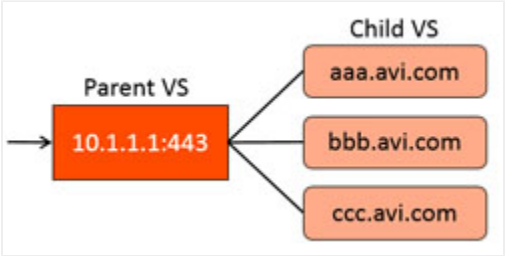
Server Name Indication, or SNI, is a method of virtual hosting multiple domain names for an SSL enabled virtual IP. A single VIP is advertised for multiple virtual services. When a client connects to the VIP, Avi Vantage begins the SSL/TLS negotiation, but does not choose a virtual service, or an SSL certificate, until the client has requested the site by name via the TLS hello packet's domain field. If the requested domain name is configured on the virtual IP, the appropriate certificate is returned to the client and the connection is bound to the proper virtual service.

Additional References

- Wildcard SNI Matching for Virtual Hosting
- Support for SNI Extension in TLS Handshakes to Pool Servers

Configuration

Avi Vantage uses the concept of parent and child virtual services for SNI virtual hosting. When the option for virtual hosting virtual service is selected on the create (via advanced mode) or edit, the virtual service participates in the virtual hosting. The virtual hosting virtual service must be configured as either a parent or a child virtual service.



Parent Virtual Service

The parent virtual service governs the networking properties used to negotiate TCP and SSL with the client. It may also be a catch-all if a client's requested domain name does not exist or does not match one of the configured child virtual services.

Configure the following properties on the parent virtual service:

- Network: The listener IP address, service port, network profile, and SSL profile. No networking properties are configured on the child virtual services.
- Pool: Optionally specify a pool for the parent virtual service. The pool will only be used if no child virtual service matches a client's requested domain name.
- SSL Certificate: An SSL certificate may be configured which could either be a wildcard certificate or a specific domain name. The parent's SSL certificate will only be used if the client's request does not match a child virtual service domain. If an SSL certificate with specific domain name is returned to the client, as in the case of sending a friendly error message, the client will receive an SSL name mismatch message. So, it is advisable to use a wildcard on the parent.

The parent virtual service will receive all new client TCP connection handshakes, which will be reflected in the statistics. Once a child virtual service is selected, the connection is internally handed off to a child virtual service, so subsequent metrics such as packets, concurrent connections, throughput, requests, logs and other statistics will only be recorded on the child virtual

service. Similarly the child virtual service will not have logs for the initial TCP or SSL handshakes, such as the SSL version mismatch errors, which are recorded at the parent virtual service.

The parent delegates to the child during the SNI phase of the TLS handshake.

If there is an SNI message received from the client and the SNI hostname matches the configured hostnames for any of the child virtual services, then the connection switches to the child virtual service at that point. Also, all the SSL (certificate etc.) and L7 state (policies, DataScripts etc.) of the child virtual service is applied to the HTTP request. Subsequently, the log ends up on the child virtual service.

If switch to child virtual service did not happen, then the connection/request is handled on the parent virtual service, and hence the SSL and L7 state of the parent gets applied. The default certificate on the parent is presented to the client. Once the request is received and parsed, you can close the client-side TCP connection through no pool, or pool with close action, or security policy. If you have a wildcard certificate on the parent that covers all the subdomains of the child virtual services, then you can serve that from the parent and then close the connection as mentioned above.

Selection of a child virtual service is solely based on the FQDNs (Fully Qualified Domain Name) configured on the SNI child. Ensure that there are no duplicates or overlaps among the child FQDNs. Common Name/ Subject Alternate Name in the virtual service certificate has no role to play in selection of children for SNI traffic.

Once a child is selected (using client hello?s server name TLS extension), its certificate will be served on the connection and further HTTP request?s host header should match one of that child?s FQDNs. Else this connection would fail with virtual host error on the applog.

If connection fails to select a child, it will be served by the parent virtual service.

Child Virtual Service

The child virtual service does not have an IP address or service port. Instead, it points to a parent virtual service, which must be created first. The domain name field is a fully qualified name requested by the SNI-enabled client within the SSL handshake. The parent matches the client request with the child's configured domain name. It does not match against the configured SSL certificate. The child may use a wildcard or domain specific certificate.

If no child matches the client request, the parent's SSL certificate and pool are used.

However, when you have a TLS SNI parent with a TLS/SSL profile that supports TLS versions 1, 1.1, and 1.2, and a TLS child which has only TLS 1.2 configured, the child will continue to use TLS 1.2.

In such a setup where the parent and child virtual services use different SSL profiles, the flow for SSL handshake is as follows:

1. TCP handshake -> Parent virtual service
2. Client Hello -> Parent virtual service The client Hello contains the SNI and so Avi Vantage will select the child virtual service.
3. SSL profile of the child is used Child virtual service SSL profile is used to allow or deny based on the SSL/TLS version and select a cipher.
4. Child virtual service responds with a server Hello that includes the cipher and the child certificate.

Logs

Starting with Avi Vantage version 17.2.5, the application logs option on the user interface displays SNI hostname information along with other SSL related information. The SNI information in the application logs provide more insight about the incoming requests and also help in troubleshooting various issues. When the child virtual service sees an SSL connection with SNI

header, the hostname in the SNI header is recorded in the application log along with the SSL version, PFS, and cipher related information. To check for SNI-enabled virtual service related logs, navigate to Applications > Virtual Service, select the desired virtual service, and navigate to Logs.