Configuring SSL for Services and Servers

https://campus.barracuda.com/doc/4259877/

Configuring SSL for SSL Enabled Services

You can configure SSL encryption for data transmitted between the client and the service. In the **BASIC > Services** page, click **Edit** next to a listed service and configure the following fields:

- **Status** – Set to *On* to enable SSL on your service. **Status** defaults to *On* for a newly created SSL enabled service.
- **Certificate** – Select a certificate presented to the browser when accessing the service. Note that only RSA certificates are listed here.
  - If you have not created the certificate, select **Generate Certificate** from the drop-down list to generate a self-signed certificate. For more information on how to create self-signed certificates, see Creating a Client Certificate.
  - If you want to upload a self-signed certificate, select **Upload Certificate** from the drop-down list. Provide the details about the certificate in the **Upload Certificate** dialog box. For information on how to upload a certificate, see Adding an SSL Certificate.
- **Select ECDSA Certificate** – Select an ECDSA certificate presented to the browser when accessing the service.
- **SSL/TLS Quick Settings** - Select an option to automatically configure the SSL/TLS protocols and ciphers.
  - **Use Configured Values** - This option allows you to use the previously saved values. If the values are not saved, the **Factory Preset** option can be used.
  - **Factory Preset** - This option allows you to enable **TLS 1.1, TLS 1.2** and **TLS 1.3** protocols without configuring override ciphers.
  - **Mozilla Intermediate Compatibility (Default, Recommended)** - This configuration is a recommended configuration when you want to enable **TLS 1.2** and **TLS 1.3** and configure override ciphers for the same.
  - **Mozilla Modern Compatibility** - This configuration is compatible when you want to enable **TLS 1.2** and configure override ciphers for the same.
  - **Mozilla Old Compatibility(Not Recommended, special purpose only)** - This is not recommended because it turns on older, less secure protocols such as SSLv3, TLS1.0 and TLS1.1. It is meant for use as a last resort when the incoming clients are older and do not support the latest protocols.

    For more information on the Mozilla presets, see this article.
- **Enable OCSP Stapling** - Select **Yes** if the certificate that is bound to this service supports OCSP Stapling.
- **SSL Protocols** – Select the SSL protocol(s) used by the clients to establish a connection to the service. You can also configure an override list for each protocol by using the **Override Ciphers** section. For more information, see Creating an HTTPS Service.
- **Enable SNI** – Set to *Yes* to enable Server Name Indication (SNI).

- **Enable Strict SNI Check** – Set to *Yes* to block access for non-SNI clients. If set to *No*, the certificate selected in the certificate drop-down list will be used for non-SNI clients.
- **Domain** – Enter the domain name and the certificate that needs to be associated with the domain. The Barracuda Web Application Firewall supports two types of certificates: RSA and ECDSA. If you want to associate the ECDSA certificate to the domain, select the certificate from the ECDSA certificate drop-down list.
  You can enter multiple domain names and associate a certificate with each one. Client requests for domains that are not associated with any certificate will get the default certificate (i.e. the certificate selected in the certificate drop-down list). The **Configured Domains** parameter displays the configured domains and associated certificates.
- **Enable Perfect Forward Secrecy** – If set to *Yes* and DHE/ECDHE key-exchange is chosen during a SSL/TLS handshake, a new ephemeral public-private key pair is generated for every SSL/TLS session. Enabling Perfect Forward Secrecy (PFS) ensures that if the private key is compromised in the future, the encrypted communication cannot be decrypted. Configure the cipher suites by selecting *Custom* in the **Ciphers** field, and delete the non-DHE/ECDHE cipher suites if you want to prevent non-PFS traffic from passing through the Barracuda Web Application Firewall. If set to *No* and DHE/ECDHE key-exchange is chosen during a SSL/TLS handshake, a public-private key pair generated during the service creation is used for all SSL/TLS communications.
- **Ciphers** – Select *Custom* to choose the ciphers for the service from the *Available Ciphers* list. *Default* includes all ciphers listed in *Available Ciphers*.
  The cipher suite selection is done by the Barracuda Web Application Firewall. The strongest cipher suite is selected from the *Default* or *Custom* cipher suites which is mutually supported by the client.
  Cipher names on the Barracuda Web Application Firewall use the OpenSSL names. To find the corresponding IANA names, see https://wiki.mozilla.org/Security/Server_Side_TLS#Cipher_names_correspondence_table.
- **Enable Client Authentication** – If set to *Yes*, the Barracuda Web Application Firewall authenticates the client with a presented certificate or authenticates the client using an authorization policy configured through **ACCESS CONTROL > Authorization**. **Note**: Certificate validation is performed only when both **Enable Client Authentication** and **Enforce Client Certificate** are set to *Yes*.
- **Enforce Client Certificate** – Set to *Yes* if you want the client to present the certificate while connecting to the service. If the client fails to present the certificate, the SSL handshake is immediately terminated.
- **Trusted Certificates** – Select one or more trusted certificates used to validate the certificates presented by the client connecting to the service. Only those client certificates that are signed by one of these trusted certificates will be allowed access. For information on how to upload a trusted certificate, see Adding an SSL Certificate.

Select a certificate to present to requesting clients for authentication. You can select an already uploaded certificate, or use the **BASIC > Certificates** page to upload a certificate. SSL enabled services allow you to handle encrypted traffic passing between the requesting client and the Barracuda Web Application Firewall. To encrypt transactions between the unit and the back-end servers, see SSL (Server). Certificates are authenticated using the selected trusted certificates. You

can upload trusted certificates in the **BASIC > Certificates** page.

Server Name Indication (SNI)

SNI extends the SSL/TLS protocol to solve the issue of hosting multiple domains on the same IP address. If each domain has a distinct SSL certificate, there needs to be a way for the real server to select the proper certificate for a particular domain. The virtual domain information is sent as part of the SSL/TLS negotiation between the client and server. Clients supporting this extension send the domain name when initializing a secure SSL session. The server side component will look at the domain name and send the corresponding certificate to the client.

For SNI to work properly, both the client browser and the web servers must support the SNI extension. SNI is already supported on most major browser platforms and on both Apache and IIS.

With SNI, you can use the Barracuda Web Application Firewall to assign any number and type of certificates (single, wildcard, or SAN) to a single Barracuda Web Application Firewall service. SNI support applies only to HTTPS services.

The SNI extension supported browsers are:

- Firefox 2.0 and higher
- IE 7 and higher on Windows Vista and higher
- Safari 5.17 on Windows 7
- Google Chrome 6 or higher on Windows 7

SSL (Server)

To encrypt data transmitted between the Barracuda Web Application Firewall and the server, configure the following fields:

- **Server uses SSL** – Set to *Yes* to enable SSL for communication with the back-end servers.
- **SSL Protocols** – Select the SSL protocol(s) used by the clients to establish the connection to the server.
- **Validate Server Certificate** – Set to *Yes* to validate the server certificate using an internal bundle of certificates that belong to well-known certificate authorities. If set to *No*, any certificate from the server is accepted. If your servers provide self-signed or test certificates, you should set this to *No*.
- **Enable SSL Compatibility Mode** - When set to **Yes**, the Barracuda Web Application Firewall restricts the list of cipher suites to be used to connect with legacy servers. Set this to **Yes** only when you need compatibility with legacy servers.
- **Enable HTTP2** - When set to **Yes**, it will enable HTTP2 protocol per server.
    - Before enabling HTTP2 for the server, make sure you disable the Connection Pooling

option.
    - Make sure you always select the server as SSL for HTTP2 backend connections to work.
    - Make sure that all the servers have HTTP2 enabled for backend connections to work.
    - When the server is added to an HTTP2-enabled service, make sure it supports the HTTP2 protocol.
- **Enable SNI** - (HTTPS services only) - Server Name Indication (SNI) is an extension of SSL and TLS protocols. When **Enable SNI** is set to **Yes**, the Barracuda Web Application Firewall allows a client to request a certificate for a specific domain from a web server. It can be used if multiple virtual HTTP domains with different certificates are hosted on one server.
- **Send TLS Extensions** – Set to *Yes* to use TLS extensions (as defined in RFC 4366) to negotiate SSL connection with the back-end server.
- **Client Certificate** – Select a certificate from the drop-down list to be used when the server requires client authentication (The Barracuda Web Application Firewall authenticates itself to the server).