Configuring SSL for Services and Servers

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

Configuring SSL for SSL Enabled Services

By clicking **Edit** next to a listed Service on the **BASIC > Services** page, in the SSL section you can configure SSL Encryption of data transmitted between the client and the Service. 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 which should be presented to the browser 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 wish 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.
- **Enable ECDSA Ciphers** – Set to ***On*** to enable ECDSA cipher suites for the Service.
- **Select ECDSA Certificate** – Select an ECDSA certificate which should be presented to the browser accessing the Service.
- **SSL Protocols** – Select the SSL protocol(s) to be used by the clients to establish the connection to the Service from the table. Also, you can configure an override list for each protocol by using the **Override Ciphers** section. For more information, see the Creating a HTTPS Service article.
- **Enable SNI** – Select *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 should select the RSA certificate along with the ECDSA certificate for the domain. ECDSA certificate is used ONLY when **Enable ECDSA Ciphers** is set to *On*.

  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, please refer to this link.
- **Enable Client Authentication** – When 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 clients to present their certificate while connecting to the Service. If the clients fail to present their certificate, the SSL handshake is immediately terminated.
- **Trusted Certificates** – Select one or more trusted certificates, which should be used to validate the certificates presented by the clients 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 you desire. 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, refer to SSL (Server). Certificates are authenticated using the **Trusted Certificates** you select. Upload Trusted Certificates on 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 any type of

certificates (single, wildcard or SAN) to a single Barracuda Web Application Firewall Service. SNI support applies only to Services with type HTTPS.

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) to be used by the clients to establish the connection to the Server from the table.
- **Validate Server Certificate** – Set to *Yes* to validate the server certificate using an internal bundle of certificates belonging 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*.
- **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 (Barracuda Web Application Firewall authenticates itself to the Server).