Creating a HTTPS Service

Configuring a HTTPS Service requires the configuration of a Certificate. See Configuring SSL for Services and Servers.

A HTTPS service is a controlled entry point for an encrypted HTTPS web application on the server. This service handles encrypted transactions between clients and the Barracuda Web Application Firewall, authenticating itself using a configured certificate, while acting as a server to requesting clients. To create an HTTPS service, select **HTTPS** as the type of service. For additional instructions go to the **BASIC > Services** page and click **Help**.

With HTTPS, HTTP uses SSL/TLS to initiate a secure connection to the application. The SSL/TLS protocols provide an encrypted connection using a set of cipher suites to encrypt the traffic. SSLv3 is the oldest of these protocols, succeeded in turn by TLS1.0, TLS1.1 and TLS1.2. Each of these protocols supports a specific set of cipher suites. Over the last few years, many vulnerabilities have been discovered in the SSL/TLS protocols and the cipher suites that they use. Due to these vulnerabilities, the current recommendations are to disable SSLv3 and use only the TLS protocols; the preferred TLS protocol is TLS1.2, with TLS1.1 offering the best mix of security and compatibility. Cipher suites have also had vulnerabilities; some of these vulnerabilities target a specific protocol/cipher suite combination. The BEAST vulnerability, for instance, targets SSL v3.0 and TLS 1.0 when used with block ciphers.

To help migrate smoothly to more secure protocols and cipher suites, the Barracuda Web Application Firewall now allows administrators to select specific cipher suites for each protocol. Instead of using the same set of cipher suites for all protocols, you can now configure an override list for each of the protocols. Once this is configured, each protocol will only use its own override list to negotiate the configuration.

Steps To Configure Cipher Override:

1. Go to the **BASIC > Services** page.
2. Click **Edit** next to an HTTPS service. The **Edit Service Configuration** window appears.
3. Scroll down to the **SSL** section and click **Show Advanced Settings**.
4. Under **Override Ciphers**:
    1. For each protocol version select the ciphers you want to include from the **Available Ciphers** list and click **Add**.
    2. Click **Save**.

For more information on secure protocol and cipher suite combinations, you can refer to the NIST article or Mozilla wiki:

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
- https://wiki.mozilla.org/Security/Server_Side_TLS