Step 2: Configuring a Service

The Barracuda Web Application Firewall can be configured to secure web servers from incoming traffic threats. To do this, create a Service which can receive the incoming traffic type (for example: an HTTP service can receive HTTP data), then associate security settings with that service to address the security risks of that traffic type. The Service also receives responses from the servers and applies security before returning responses to the client.

Using any Service, the Barracuda Web Application Firewall acts as a server to which the client connects on the front-end. On the back-end, the Service acts as a client to the real servers. The Barracuda Web Application Firewall fulfills each of these roles using the Service and its associated configuration settings.

What is a Service?

A Service is configured with a Virtual IP (VIP) address and a TCP port. Traffic arriving at the designated VIP and port is validated, subjected to security checks configured for the service, and then passed to one of the Real Servers associated with that Service.

Configuring Your First Service

The BASIC > Services page allows you to add a new service(s) and server(s) to be protected by the Barracuda Web Application Firewall. The type of Service you choose should correlate to the type of traffic coming into the application you are protecting, so the service can terminate and validate the requests before applying security. For example, you should select an HTTP Service for unsecured traffic, versus an HTTPS Service for secured traffic.

The types of Services you can configure with the Barracuda Web Application Firewall depend on the deployment mode you choose.

In Bridge Mode (Bridge Path) you can configure:

- **HTTP or HTTPS Services**: Validate and apply security to unencrypted or encrypted HTTP traffic.

In Proxy Mode, you can configure:

- **HTTP and HTTPS Services**: Validate and apply security to unencrypted or encrypted HTTP traffic;
- **FTP and FTPS Services**: Validate and apply security to unencrypted and encrypted FTP traffic;
- **Instant SSL** and **Redirect Services**: Implement off-loaded SSL validation and encryption for unencrypted traffic;
- **Custom** and **Custom SSL Services**: Allow the Barracuda Web Application Firewall to process any application layer traffic over TCP. Traffic sent by the client to a Custom or Custom SSL Service is forwarded to the back-end servers without analysis. The Barracuda Web Application Firewall does not validate the incoming requests or outgoing responses.

**Steps to Configure a Service**

For detailed instructions on configuring a service, go to the **BASIC > Services** page and click **Help**.

Once successfully created, a Service appears in the **Services** section with a green, orange, or red health indicator next to it. See **Health Indicators for Services and Servers** for more information. Newly configured Services, by default, use the ‘default security policy’, and have a Passive enforcement mode, so at first, all URLs and Parameters are compared to the ‘default security policy’ settings. The Service page allows you to edit Services so you can change the settings or enforcement mode. For instructions on editing a Service, see **Step 3: Configuring Basic Service Settings**.

**Example Video**

Watch the "Creating Services in the Barracuda Web Application Firewall" video to know how to create and modify a service in the Barracuda Web Application Firewall.

**Creating SSL Enabled Services**

To use SSL you need to select a Certificate which the service presents to authenticate itself to a client. Certificates are created or uploaded using the **BASIC > Certificates** page, where you can add a certificate to the available Certificate list. You choose your Service certificate from this list before using **Add** to create the service. You can change the certificate to any available certificate by clicking **Edit** for the service in the **Services** list.
Configuring SSL for SSL Enabled Services

By clicking Edit next to the service on the Services section of the BASIC > Services page, you can configure the SSL supported protocols. SSL status defaults to On for a newly created SSL enabled service. If you set Enforce Client Certificate to Yes, any request from a client without a certificate immediately terminates. If you set Enable Client Authentication to Yes, the Barracuda Web Application Firewall authenticates the client with the presented certificate, or authenticates the client using an authorization policy configured through ACCESS CONTROL > Authorization. Authentication of certificates uses selected trusted certificates.

SSL enabled services allow configuration of encryption between the requesting client and the Barracuda Web Application Firewall. To encrypt transactions between the appliance and the back-end servers, refer to Back-end SSL Server Configuration.

Health Indicators for Services and Servers

The following are the health indicators displayed for each Service and server:

- ✓ - Service is up; Server is responding.
- ▲ - If multiple servers are configured for a Service, the orange dot indicates that more than 50% of Servers are down and the Service is running.
- ✗ - Service is down; Server is not responding.

Continue with Step 3: Configuring Basic Service Settings.
Figures

1. green.png
2. orange.png
3. red.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.