Step 2: Configuring a Service

https://campus.barracuda.com/doc/4259899/

You can configure the Barracuda Web Application Firewall to secure web servers from incoming traffic threats. To do this, create a service to receive the incoming traffic type (for example: an HTTP service can receive HTTP data), and 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.

The Barracuda Web Application Firewall acts as a server for the client connection on the front end, and the service acts as a client to the real servers on the back end. 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 that the service can terminate and validate the requests before applying security. For example, you should select an HTTP service for unsecured traffic and 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** - Validate and apply security to unencrypted or encrypted HTTP traffic.

In Proxy Mode, you can configure:

- **HTTP and HTTPS** - Validate and apply security to unencrypted or encrypted HTTP traffic.
- **FTP** and **FTPSSL** - Validate and apply security to unencrypted and encrypted FTP traffic.
- **Instant SSL** and **Redirect Service** - Implement off-loaded SSL validation and encryption for unencrypted traffic.
- **Custom** and **Custom SSL** - 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**.

After you successfully create a service, it 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 use the **default** security policy and have a passive enforcement mode. Initially, all URLs and parameters are compared to the default security policy settings. The service page allows you to edit the service options so that 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 create and modify a service in the Barracuda Web Application Firewall.

Creating SSL Enabled Services

To use SSL, you need to select a certificate that the service uses 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. Before you create a service, you must choose your service certificate from this list. You can change the certificate to any available certificate by going to the **BASIC > Services** page and clicking **Edit** in the **Services > Actions** section.

Configuring SSL for SSL Enabled Services

You can configure the SSL supported protocols by going to the **BASIC > Services** page and clicking **Edit** next to the service in the **Services > Actions** section. 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 selected certificate or 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, see 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