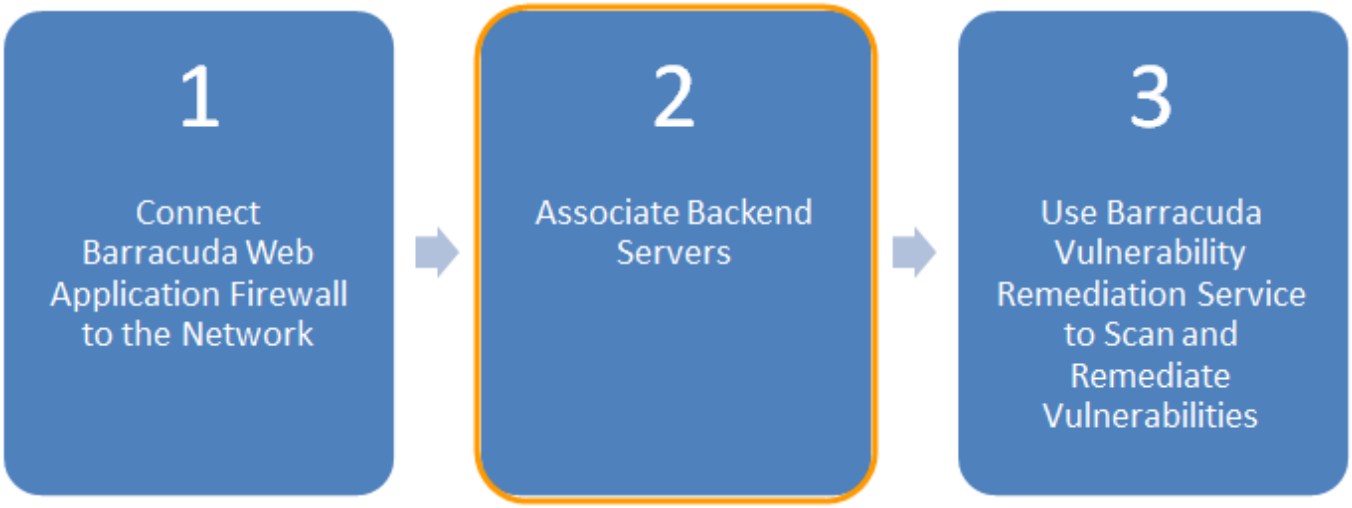
Step 2: Associate Backend Servers

https://campus.barracuda.com/doc/67174864/

Step 2: Associate Backend Servers



The Barracuda Web Application Firewall acts as a reverse proxy for your backend servers. That is, it listens for traffic on the (typically public) IPs that your users access, and forwards traffic to the application servers actually serving the requests. In this step, tell the Barracuda Web Application Firewall on which IPs to listen for traffic, and to which servers to forward legitimate traffic.

For detailed instructions on how to create services on your Web Application Firewall, refer to Step 2: Configuring a Service in the Barracuda Web Application Firewall section of Barracuda Campus.

You may *initially* configure the service you created in Passive Mode, but you **must** switch it to Active Mode after verifying that the application runs properly. Passive Mode is intended for testing only; in Passive Mode, the Web Application Firewall *does not* secure your application.

Continue to Step 3: Scan and Remediate Vulnerabilities.

Figures