How to Set Up a Reverse Proxy

https://campus.barracuda.com/doc/79463102/

In **Reverse Proxy** mode, the proxy directs incoming requests from other servers to the client without providing the origin details. To set up a reverse proxy using the Barracuda CloudGen Firewall, configure the listening port and reverse proxy settings.

Before You Begin

Verify that you activated the HTTP Proxy service in reverse proxy mode. For instructions, see How to Set Up and Configure the HTTP Proxy.

Configure the Listening Port

In the settings for the HTTP Proxy, use TCP listening port 80.

1. Go to **CONFIGURATION** > **Configuration Tr ee** > **Box > Assigned Services** > **HTTP Proxy > HTTP Proxy Settings**.
2. In the left menu, select **IP Configuration**.
3. Click **Lock**.
4. In the **TCP Listening Port** field, enter `80`. Verify that you have port 80 available for your reverse proxy.
5. When you change the listening port, you must also change the port used in host firewall rule **OP-SRV-PX**. By default, the rule uses TCP 3128. If you want to use HTTP, change **TCP 3128** to **HTTP**. If you want to use HTTP and HTTPS, change **TCP 3128** to **HTTP+S**. For more information on configuring Host Firewall rules, see Host Firewall.
6. Click **Send Changes** and **Activate**.

Configure Reverse Proxy Settings

To configure the reverse proxy settings:

1. Go to **CONFIGURATION** > **Configuration Tr ee** > **Box > Assigned Services** > **HTTP Proxy > HTTP Proxy Settings** .
2. In the left menu, select **Reverse Proxy Settings**.
3. Click **Lock**.
4. Specify your **Reverse Proxy Settings**. For more information on these settings, see the

following Reverse Proxy Settings section.

5. Click **Send Changes** and **Activate**.

Reverse Proxy Settings

The following table provides more detailed descriptions of the **Reverse Proxy Settings**:

Setting	Description
Backend Web Site	Enter the IP address of the internal webserver behind the reverse proxy. If there is no host header, enter your primary domain (for example, `mydomain.com`).
ACL Mode	Select the ACL mode: • **Default** – Access to the backend website is allowed automatically. • **Advanced** – Access is allowed according to the configured access policy configured in the **HTTP Proxy Settings > Access Control** section.
Use SSL	Select **yes** from the **Use SSL** list to provide HTTPS and HTTP support for the reverse proxy. Import your certificate and key by clicking **Ex/Import** for **SSL Certificate** and **SSL Private Key**. **Switch to Advanced View** and click on **SSL Settings** in the left menu to configure SSL cipher settings. When set to **Disallow Weak Ciphers** (default), the following cipher string is used: !aNULL:ALL:!EXPORT:!LOW:!MEDIUM:!RC2:!3DES:!DSS:!SEED:!RC4:!PSK:@STRENGTH
SSL Listening port	The SSL listening port (default: 443).
SSL Certificate	When using SSL , import a certificate for securing the connection. This should be the certificate of the backend website.
SSL Private Key Type	Select the type of private key that belongs to the certificate. • When selecting **RSA**, import the private RSA key. • When selecting **ECDSA**, import the private ECDSA key.
SSL/TLS Version for Backend	Select the SSL or TLS version to be used for the backend. To let the proxy determine the version, select **Auto** .
Custom Cipher String for Backend	Enter a custom colon-separated string of ciphers. This setting is only valid for reverse proxy mode.
Front-End HTTPS Header	Set to **On** to enable the front-end HTTPS header. Set to **Auto** to add this header if the forwarded request is using HTTPS. The front-end HTTPS header is required when using the reverse proxy for SSL offloading in front of Microsoft OWA.
MS Authentication Forwarding	Microsoft connection-oriented authentication forwarding (NTLM, Negotiate, and Kerberos)
Backend IP Addresses	In this table, add the IP addresses of your backend servers. You must add the IP address of at least one backend server.
Round Robin	Unless you want to use domain or URL-based mapping, you can enable round robin load balancing between multiple backend servers by selecting *yes* from the **Round Robin** list. Load balancing is not available if traffic shaping is enabled on the device to which the web server is attached. For more information, see Traffic Shaping.
Pass Login to Backend	Set to **Yes** if you want the proxy to pass on all authentication headers to the backend servers.
Additional Backend Domains	In this table, you can add additional domains for domain-based virtual hosts.

Domain to Backend Mapping	Note that the **Name** field of entries in this table must not exceed 21 characters. If you have not installed Barracuda CloudGen Firewall hotfix 521, the **ACL-based reverse mapping** table is provided. In this table, you can add ACLs for the backend server that should be used. To map either a domain or a specific URL to a backend server, click **+**, enter a descriptive name for the map (for example, `DOMA04`), and click **OK**. • In the **Backend Mappings** configuration window, map either a domain or a specific URL to a backend server. • From the **Mapping Type** list, select **Domain** for domain to backend mapping. If you are using url-regex to backend mapping, select **Url-Regex**. • From the **Domain** list, select a domain that is specified in the **Additional Backend Domains** table. If you are using url-regex to back-end mapping, enter the regular expression to match a URL against (for example, `http://example.com/foo/.*`). • From the **Backend** list, select the back-end server that should handle the requests that match the above configuration. This list includes the backend servers that you entered in the **Backend IP Addresses** table.