How to Set Up and Configure the HTTP Proxy

To set up and configure the HTTP Proxy, follow the steps that are provided in this article. After setting up the HTTP Proxy, you can configure log settings for the service. Because the integrated proxy service of the Barracuda NextGen Firewall F-Series is based on Squid, you can also add generic `squid.conf` entries for configurations such as client IP forwarding, closing redundant client sessions, and customized HTTP and HTTPS ports. From the command line, you can verify the HTTP Proxy server configuration.

In this article:

Step 1. Enable the HTTP Proxy Service

To enable the HTTP Proxy:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > HTTP-Proxy > Service Properties**.
2. Click **Lock**.
3. From the **Enable Service** list, select ***Yes***.

   The remaining settings on the page were configured when the HTTP Proxy service was created. For more details on these general service IP address settings, see Service Settings.
4. Click **Send Changes** and **Activate**.

Step 2. Configure the Connection Settings

Specify the settings for connecting your system to the Internet.

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. From the **Configuration** menu in the left navigation pane, select **HTTP Proxy**.
3. Click **Lock**.
4. From the **Connection Type** list, select how your system is connected to the Internet. You can select one of these options:
   - **Direct Access** – Your Barracuda NextGen Firewall F-Series is directly connected to Internet.
   - **HTTP/S Proxy** – Your Barracuda NextGen Firewall F-Series is connected through an HTTP or HTTPS proxy.
5. Specify the rest of the settings in the **System HTTP Proxy Settings** section.
6. Click **Send Changes** and **Activate**.

Step 3. Specify the Operation and Network Settings

Select the operation mode for the HTTP Proxy and specify its network settings.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. In the **Basic Settings** section, specify the following settings:

   - **Contact Mail** – The admin proxy email address. This address is the contact that will be displayed within upcoming error messages.

- **Visible Hostname –** The hostname that will be displayed within error messages. The visible hostname must be formatted as: "*host.domain.tld*". Special characters are not allowed. If you are running a forwarding/caching DNS server, the hostname MUST NOT be identical to the system hostname.

- **Proxy Mode –** The mode that specifies how the proxy service handles requests. You can select one of the following modes:

Mode	Description
ForwardProxy	If requests received from a client must be directed to another server, select this mode. The HTTP proxy then acts as a client and generates further requests to the server.
TransparentProxy	All requests sent by clients are directed to the proxy server. With this mode, proxy authentication is only possible with the Barracuda DC Agent. With a transparent proxy, you must also create a forwarding firewall rule (App Redirect) or unblock the preconfigured TRANSPARENT-PROXY firewall rule to allow Internet access for your trusted LANs. For more details on configuring firewall rules, see Firewall Access Rules.
ReverseProxy	The reverse proxy directs incoming requests from other servers to clients without providing the origin details. With this mode, you must also configure additional settings for the reverse proxy. For more details, see How to Set Up a Reverse Proxy.

With the **Transparent Proxy** and **Reverse Proxy** modes, the proxy modes and access control lists for the *proxyauthentication* type are deleted.

4. From the **Configuration** menu in the left navigation pane, select **IP Configuration**.
5. In the **Network Settings** section, specify the IP addresses and ports that you want to use. You can also configure SNMP monitoring. For more details on these settings, see HTTP Proxy Settings.
6. Click **Send Changes** and **Activate**.

(Optional) Step 4. Enable SSL Interception

To apply web filter policies or to use virus scanning for HTTPS traffic enable SSL Interception.

You must deploy the root certificate to the clients browsers to avoid SSL errors.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > HTTP-Proxy > SSL Settings**.
2. Click **Lock**.
3. Select **Enable SSL Interception**.
4. Import your root CA Certificate in PKCS12 format:
    1. Click on **Ex/Import** for the **Root CA Certificate.**
    2. Select **Import from PKCS12 File** and select your root CA certificate file on your computer.
5. (optional) In the **SSL Interception** section enter the **Excluded Domains**
6. (optional) In the **SSL Interception** section enter domains which should always be trusted to the **Whitelist.**
7. Click **Send Changes.**
8. Click **Activate**.

(Optional) Step 5. Configure Misc. Settings

If required, you can configure these miscellaneous settings for the HTTP Proxy:

- Use of extended passive FTP
- Number of CPU cores
- Use of the X-Forwarded-For header for requests
- Cache settings
- Size limit for files that will be processed

To configure these settings:

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **HTTP-Proxy** > **HTTP Proxy Settings**.
2. In the left navigation menu, expand **Configuration Mode** and click **Switch to Advanced View**.
3. In the left navigation menu, click **Basic**.
4. Click **Lock**.
5. In the **Misc. Settings** section, configure the miscellaneous settings. For more details on these settings, see HTTP Proxy Settings.
6. Click **Send Changes** and **Activate**.

Configure Log Settings

To specify the log settings for the HTTP Proxy:

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **HTTP-Proxy** > **HTTP Proxy Settings**.
2. In the left navigation menu, expand **Configuration Mode** and click **Switch to Advanced View**.
3. In the left navigation menu, click **Basic**.
4. Click **Lock**.
5. In the **Log Settings** section, specify the log settings for the service. For more details on these settings, see HTTP Proxy Settings.
6. Click **Send Changes** and then click **Activate**.

Add Squid Configurations

To configure client IP forwarding, closing redundant client sessions, and customized HTTP and HTTPS ports, add `squid.conf` entries in the advanced settings for the HTTP Proxy.

For more information about Squid proxy configuration, see the official Squid documentation at www.squid-cache.org. Note that changing advanced configuration parameters should only be done by an expert administrator. If you have any questions, contact Barracuda Networks Technical Support for assistance.

To add `squid.conf` entries:

First, enable legacy settings for the Barracuda NextGen Firewall F-Series:

1. Click the Barracuda icon in the top left of Barracuda NextGen Admin and select **Settings**.
2. Expand **Admin and CC Settings** and select the **Show legacy configuration elements** check box in the **Legacy Configuration** section.
3. To activate the settings, restart Barracuda NextGen Admin.

The `squid.conf` settings are visible in Barracuda NextGen Admin now. Continue with the following steps:

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **HTTP-Proxy** > **HTTP Proxy Settings**.
2. In the left navigation pane, expand **Configuration Mode** and click **Switch to Advanced View**.

3. Click **Lock**.
4. From the **Configuration** menu in the left navigation pane, click **Advanced**.
5. In the **Generic squid.conf Entries** field, add the required `squid.conf` entries.
6. Click **Send Changes** and **Activate**.

More information on how to configure the required `squid.conf` entries is provided in these sections:

Client IP Forwarding

To grant access to web servers that do not accept anonymous HTTP requests from proxies, you can add a `squid.conf` entry. The Barracuda NextGen Firewall F-Series HTTP proxy uses the `forwarded_for` option to add the `X-Forwarded-For` option in the HTTP header for such requests. If the option is set to `unknown`, the web server may block the request. To grant access to this web server, you must enable client IP address forwarding or delete the entire `X-Forwarded-For` entry from the HTTP header.

To configure client IP forwarding, enter one of the following options:

Forwarding Option	Description
`forwarded_for on`	Adds the actual client IP address to the HTTP header.
`forwarded_for off`	Adds `unknown` as a value in the HTTP header. To maintain anonymity, Barracuda Networks recommends that you use the `delete` option.
`forwarded_for delete`	Deletes the entire `X-Forwarded-For` entry from the HTTP header.
`forwarded_for transparent`	Does not alter the `X-Forwarded-For` entry in the HTTP header in any way.
`forwarded_for truncate`	Removes all existing `X-Forwarded-For` entries and adds itself as the sole entry.

Close Client Sessions

After a certain number of established sessions, the firewall engine blocks new sessions until the HTTP proxy and the antivirus service are restarted. As a result, the number of antivirus file descriptors increases when using the HTTP Proxy and firewall authentication via HTTPS may not work. To close redundant client sessions, enter the following two parameters:

- `pconn_timeout 10 seconds`
- `half_closed_clients off`

Customized HTTP and HTTPS Ports

If required, you can add customized ports with `squid.conf` entries. Some environments require customized ports for HTTP proxy. For example, *http://www.intranet.com:81* or *https://www.intranet.com:81*. If the ports are not automatically accepted by the proxy, you can allow these ports via an ACL.

By default, the Squid proxy only accepts HTTP and HTTPS requests on the following ports:

Accepted Port	Service
443 / 563	HTTPS
80	HTTP
21	FTP
70	Gopher
210	WAIS
280	HTTP-MGMT
488	GSS-HTTP
591	FileMaker

Add Ports to the ACL

To add ports to the ACL, enable legacy settings for the Barracuda NextGen Firewall F-Series and then add the `squid.conf` entries for the ports.

1. Enable legacy settings for the Barracuda NextGen Firewall F-Series.
   1. Click the Barracuda icon in the top left of Barracuda NextGen Admin and select **Settings**.
   2. Expand **Admin and CC Settings** and select the **Show legacy configuration elements** check box in the **Legacy Configuration** section.
   3. To activate the settings, restart Barracuda NextGen Admin.
2. Log back into the Barracuda NextGen Firewall F-Series and open the **HTTP Proxy Settings - Advanced** page in advanced configuration mode.
3. Add the `squid.conf` entries for the required ports. Depending on the protocol, use the following syntax:

Protocol	Syntax
HTTP	`acl Safe_ports port <portnumber>`
HTTPS	`acl SSL_ports port <portnumber>`

For example, to add port 81:

Protocol	Example
HTTP	`acl Safe_ports port 81 # http customized`
HTTPS	`acl SSL_ports port 81 # https customized`

Verify the HTTP Proxy Configuration

From the command line, you can verify your HTTP proxy server configuration.

1. At the command line, log in as ***root***.
2. Enter the following:
   `squid -N -f /var/phion/preserve/proxy/<servername_servicename>/root/squid.conf`

If there are any errors in your configuration, the number of the row that contains the error is printed.

HTTP Proxy Settings

These sections provide more detailed descriptions of the networking, log, and miscellaneous settings that you can configure for the HTTP Proxy:

Click here to see more

Networking Settings

Settings	Description
TCP Listening Port	The port on which the proxy service listens for incoming HTTP connections. By default, port *3128* is used. Be aware that, if you change the default TCP listening port, you must also change the port number in the service object for the default HTTP proxy local firewall rule (**OP-SRV-PX**). Otherwise, all HTTP traffic is blocked. For more details on configuring service objects, see How to Create Service Objects.

TCP Outgoing Address	The IP address that is used by the proxy server when executing HTTP requests. You can select *First-IP*, *Second-IP*, or *Dynamic*. If you select *Dynamic,* an IP address is automatically selected from the available server address pool. To enter an explicit IP address, select *Other*.
UDP Incoming Address	The IP address that is used by the proxy server when responding to ICP queries. You can select *First-IP*, *Second-IP*, or *None*. To enter an explicit IP address, select *Other*.
UDP Outgoing Address	The IP address that is used by the proxy server when executing ICP and DNS queries. You can select *First-IP* or *Second-IP*. To enter an explicit IP address, select *Other*. If you are accessing the Internet through a dynamically assigned IP address (such as through an xDSL line), enter *255.255.255.255.* If you entered explicit IP addresses in the **TCP Outgoing Address**, **UDP Incoming Address**, or **UDP Outgoing Address** fields, make sure that you also add these IP addresses to the **Additional IP** table on the **Server Properties** page for your virtual server. For more details, see How to Configure Virtual Servers.
ICP Port	The port through which the proxy service handles ICP connections with its neighbor caches. By default, port 3130 is used. To disable this port, enter `0`.
Neighbor Settings	In this table, specify how the proxy server treats neighboring proxies. For information on how to configure this section, see How to Configure Neighbor Proxies.
DNS Server IP addresses	In this table, add the DNS server IP addresses that are exclusively used by the HTTP Proxy service. If one of the defined DNS servers is unreachable, the HTTP proxy will not use the globally defined servers of the Barracuda NextGen Firewall F-Series unit itself. You can only edit this table in the Advanced Configuration Mode. In the left navigation pane, expand **Configuration Mode** and click **Switch to Advanced View**. Note that this setting overwrites system-wide DNS server settings.
SNMP Monitoring	To configure the SNMP monitoring settings, click **Set**. For more details, see SNMP Monitoring.

Log Settings

This table provides more detailed descriptions for the log settings that you can configure in Configure Log Settings.

Setting	Description
Write Cache-Log	The cache log file records debug and failure messages generated by squid during operating time. Amongst others, it includes information about service start and termination, and execution of ACLs.
Debug Level	The debug level defines the verbosity of the cache log file. You can select: • **normal** – Minimal logging. Errors will not be listed exhaustively; statistical information will not be generated. • **verbose** – Generates statistical information and logs most errors. • **debug** – Exhaustive logging of errors and statistical information. With the *debug* setting, more disk space is used by the service log.
Log via Syslog	Determines how to handle log files that are generated by the HTTP Proxy service. You can select: • **Auto** – Queries the Syslog-Proxy configuration prior to log data processing. If a streaming profile for HTTP Proxy log files is defined, it will be used to stream log files to a syslog server and generates a local log file as well. • **Yes** – Forwards logging data to the local Syslog proxy, where more data processing can be defined. For more details, see How to Configure Syslog Streaming. • **No** – Generates logs files on the Barracuda NextGen Firewall F-Series. If you are impacted by performance issues with remote logging to busy servers, select *No*.

IPFIX Streaming	To stream HTTP Proxy logs to an external IPFIX collector, select *Yes*. You must also configure the IPFIX streaming settings. For more details, see How to Configure Audit & Reporting With IPFIX.

Misc. Settings

This table provides more detailed descriptions for the log settings that you can configure in (Optional) Step 4. Configure Misc. Settings.

Setting	Description
Disable Extended Passive FTP	Control whether Squid uses EPSV extension for efficient NAT handling and IPv6 protocol support in FTP. You cannot enable FTP on more than one proxy.
Number of Workers	Defines the number of CPU cores used by the HTTP Proxy engine. Auto allocates all available cores to the HTTP Proxy engine.
Follow X-Forwarded-For Header	To use the X-Forwarded-For header of HTTP requests for logging and ACLs, select *yes*.
Cache Settings	To configure the cache settings, click **Set**. • **Cache Type** – Specifies the behavior of the HTTP Proxy cache. You can chose between the following options: ◦ **None** – Disables the local cache (Proxy mode only). ◦ **Minimal** – The system uses minimal disk space for caching. ◦ **Aggressive** – The system uses up to half of the available hard-disk for caching. ◦ **User-Defined** – This option lets you define the cache settings manually and enables the following parameters: • **Size in MB** – The maximum size of the cache directory in MB. It is recommended that you set this limit to at least 100 MB. The cache is located in `/var/phion/squid cache_SERVERNAME_SERVICE NAME`. • **Level1 Directories / Level2 Directories** – These settings define the structural organization of the proxy service's cache directory. The default values (16 / 256) are the recommended minimum values for the Level1 and Level2 directories respectively. Be aware that entering high values will generate a vast number of subdirectories. • **Max Object Size(kB)** – Objects exceeding this limit will not be cached. • **Mem Cache Size (MB)** – The memory size of the lookup cache.
Limit Settings	To specify the maximum size for files that will be processed by the HTTP proxy, click **Set**. In the **Overall Maximum File Size** field, enter the file size limit. Files that exceed this limit are dropped by the HTTP Proxy service. An equal limitation may also be set by using Proxy Access Control Lists.