

How to Configure User Authentication and Access Control

<https://campus.barracuda.com/doc/43847101/>

For user authentication with the HTTP Proxy, the external authentication scheme that you can use depends on the proxy mode. With a transparent or reverse proxy, you can only use the Barracuda DC Agent. With the forward proxy, you can use either MS-CHAP or Kerberos.

To configure access control, you have the following options:

- **Access Control Policy** – An access control policy is composed of ACL entries that define the connections to be restricted or allowed. An ACL entry can define IP addresses, domains, users, groups, browsers, MIME types, URLs, protocols, ports, connections, and times. Access control policies are processed one by one, according to their priority numbers. You can specify the priority of a policy when you create it.
- **Access Control File List** – In addition to ACL entries and policies, you can also configure ACL file lists. ACL file lists are processed before ACL entries and policies.
- **Legacy ACL Settings** – With this option, you can configure ACL files using the squid.conf syntax. From the command line, you can check the syntax of the squid.conf file.

In this article:

Configure User Authentication

To configure user authentication, follow the instructions for the HTTP Proxy mode that you are using:

Transparent and Reverse Proxy Authentication

With a transparent or reverse proxy, you can only configure user authentication with the Barracuda DC Agent. For instructions on how to set up the Barracuda DC Agent with the Barracuda NG Firewall, see [How to Configure MSAD DC Client Authentication](#).

For general information about the Barracuda DC Agent, see [Barracuda DC Agent for User Authentication](#).

Forward Proxy Authentication

With the forward proxy, you can use either MS-CHAP or Kerberos for user authentication. If you want your users to authenticate themselves on a Windows domain controller or a RADIUS server, activate and configure Kerberos.

To configure user authentication for the forward proxy:

1. Verify that you have properly configured the external authentication scheme for the forward proxy:
 - **MS-CHAP** – For instructions, see [How to Configure MS-CHAP Authentication](#).
 - **Kerberos** – For instructions, see [How to Configure Kerberos Authentication](#).
2. Open the **HTTP Proxy Settings** page (**Configuration > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > HTTP-Proxy**).
3. Click **Lock**.
4. From the **Configuration** menu in the left navigation pane, select **User Authentication**.
5. Next to **Authentication Settings**, click **Set**.
 - To use MS-CHAPv2, edit the settings in the **MS-CHAPv2 Settings** section.
 - To use Kerberos, edit the settings in the **Kerberos Settings** section.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Configure Access Control

To configure access control, you have the following options:

Access Control Policy

First create the ACL entries that are required by the policy. Then create the access control policy by adding the ACL entries and selecting an action to handle them.

To configure an access control policy:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. In the left menu, select **Access Control**.
3. Click **Lock**.
4. From the **Default Access Control Policy** list, select *Allow*.
5. In the **ACL Entries** table, add all of the entries that are required for the access control policy.
For each entry:
 1. In the **Enter Name** window, enter a name for the entry, specify the entry type, and then click **OK**.
 2. In the **ACL Entries** window, configure the entry settings and then click **OK**.

If you choose to later delete an ACL entry, you must also delete it from any ACL policies that it has been added to. When you delete an ACL entry, it is not automatically deleted from ACL policies. Actions with broken links to its parent will cause the proxy to fail.
6. In the **Access Control Policies** table, add the policy.
 1. Enter a name for the policy and click **OK**.

2. In the **Access Control Policies** configuration window, specify the priority, required ACL entries, and action for the policy. Then click **OK**.
7. For more details on the settings that you can configure for the ACL entries or access control policies, see [Access Control Settings](#).
8. Click **Send Changes** and **Activate**.

For examples and explanations to help you understand access control policies, see [Access Control Policy Example](#).

Access Control File List

To configure an ACL file list:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. In the left menu, select **Access Control**.
3. From the **Configuration Mode** menu in the left navigation pane, click **Switch to Advanced View**.
4. Click **Lock**.
5. From the **Default Access Control Policy** list, select **Allow**.
6. In the **ACL FileList** table, add the ACL file list.
 1. Enter a name for the list and then click **OK**. The name must be numerical. It determines the priority of the ACL file list. To assign higher priority to the ACL file list, enter a lower number.
 2. In the **ACL FileList** window, configure the file list. Specify the following settings:
 - **Filename** - The name of the ACL file. By default, the file is saved to the `/var/phion/preserve/proxy/<servername>_<servicename>/root/` directory.
You can save the file to a different location, but this is not recommended. First verify that the destination directory has been properly created. When you specify the file name, add the absolute path to the destination directory.

Do not use file names such as `squid.conf` and `ftpsquid.conf`; otherwise, you may lose configuration information. To avoid such situations, it is recommended that you use the default location and `.acl` as the file name extension. For example, `aclfile.acl`.
 - **ACL Entries** - The entries that are written to the file. ACL entries are processed line by line. If a line must exceed 1012 characters, use the forward slash (/) to section lines.

ACL entries must match the `squid.conf` syntax. They are not checked against `squid.conf` for compatibility. Do NOT use Inverted CIDR Notation. Access control policies will only apply if *all* ACL entries are met. For example, if you add three ACL entries to one policy, the policy only applies if all three ACL entries match.
 3. Click **OK**.
7. Click **Send Changes** and **Activate**.

Legacy ACL Settings

To configure legacy ACL settings:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. In the left menu, select **Access Control**.
3. From the **Configuration Mode** menu in the left navigation pane, click **Switch to Advanced View**.
4. Click **Lock**.
5. From the **Default Access Control Policy** list, select *Allow*.
6. From the **Access Configuration** list, select *legacy*.
7. Next to **Legacy**, click **Set**.
8. In the **Access Control Entries** field, enter your ACL entries. These entries must use the `squid.conf` syntax. You can enter complete ACLs, as well as entries from the ACL file list.
Because your ACL entries are not checked against `squid.conf` for compatibility, make sure that you use the exact syntax. Do NOT use [inverted CIDR notation](#).
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

The `squid.conf` file can be located at
`/var/phion/preserve/proxy/<servername_servicename>/root/`.

Check the squid.conf Syntax

To check the syntax of the `squid.conf` file from the command line, enter:

```
squid -X -N -f  
/phion0/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.

On the Barracuda NG Firewall, Perl-compatible regular expressions (PCRE) can be used (for example in the HTTP Proxy server ACL configuration section). You can use PCRE when you want to substitute hard coded character strings against expressions that match in multiple cases. For an overview of meta characters in regular expressions, see [Regular Expressions](#).

Access Control Policy Example

These sections provide steps to configure two example access control policies and an explanation of how the the policies are processed:

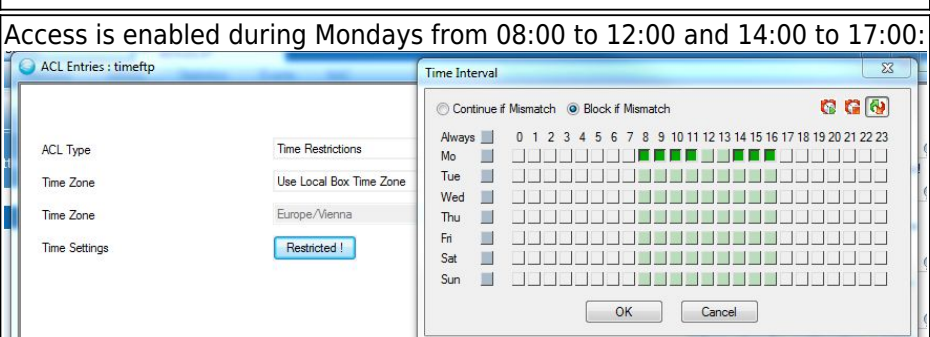
Creating the Example Access Control Policies

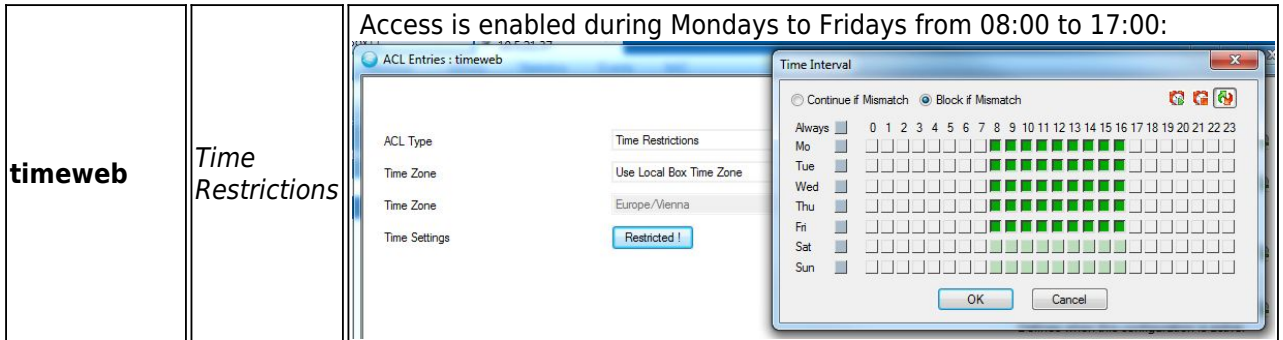
This example procedure configures two access control policies that limit FTP and HTTP access for a client at 10.0.8.1 to the following days and times:

Access Control Policy	Access Times
FTP Access	Mondays, 08:00 - 12:00 and 14:00 - 17:00
HTTP Access	Mondays to Fridays, 08:00 - 17:00

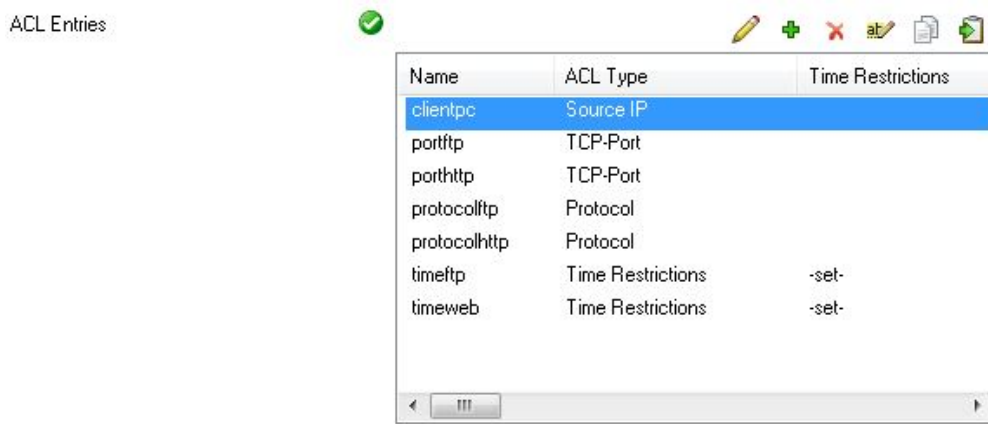
First create all of the required ACL entries. Then add these entries to the policies.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > HTTP-Proxy > HTTP Proxy Settings.**
2. In the left menu, select **Access Control.**
3. Click **Lock.**
4. From the **Default Access Control Policy** list, select *Allow*.
5. In the **ACL Entries** table, create these ACL entries:

ACL Entry Name	ACL Entry Type	Settings
clientpc	Source IP	<ul style="list-style-type: none"> IP Configuration: Singlemode Set IPs: 10.0.81
portftp	TCP-Port	Specify Destination Port Address: 21
porthttp	TCP-Port	Specify Destination Port Address: 80
protocolftp	Protocol	Define Transfer Protocol: FTP
protocolhttp	Protocol	Define Transfer Protocol: HTTP
timeftp	Time Restrictions	<p>Access is enabled during Mondays from 08:00 to 12:00 and 14:00 to 17:00:</p> 



After all of the required ACL entries are created, they are displayed in the **ACL Entries** table as follows:



In the squid.conf file, the days of the week are stated as follows:

- o **M** - Monday
- o **T** - Tuesday
- o **W** - Wednesday
- o **H** - Thursday
- o **F** - Friday
- o **A** - Saturday
- o **S** - Sunday

For the example timeftp and timehttp settings, the following ACL entries are generated in squid.conf for all of the times when access is enabled:

timeftp	timehttp
<pre>acl mytime time M 08:00-12:00 acl mytime time M 14:00-17:00 There are two entries for Monday because access is enabled from 8:00 to 12:00, restricted from 12:00 to 14:00, and then re-enabled from 14:00 to 17:00.</pre>	<pre>acl mytime time M 08:00-17:00 acl mytime time T 08:00-17:00 acl mytime time W 08:00-17:00 acl mytime time H 08:00-17:00 acl mytime time F 08:00-17:00</pre>

6. In the **Access Control Policies** table, create these access control policies:

Access Control Policy Name	Settings
----------------------------	----------

webaccess	<ul style="list-style-type: none"> ◦ ACL Priority: 1 ◦ Action: Allow ◦ ACL Entries for this Action: <ul style="list-style-type: none"> ■ <i>clientpc</i> ■ <i>porthttp</i> ■ <i>protocolhttp</i> ■ <i>timeweb</i>
ftpassess	<ul style="list-style-type: none"> ◦ ACL Priority: 2 ◦ Action: Allow ◦ ACL Entries for this Action: <ul style="list-style-type: none"> ■ <i>clientpc</i> ■ <i>portftp</i> ■ <i>protocolftp</i> ■ <i>timeftp</i>

After the access control policies are created, they are displayed in the **Access Control Policies** as follows:

Access Control Policies



Name	ACL Priority	Action
webaccess	1	Allow
ftpassess	2	Allow

In `squid.conf`, the following lines are generated for the example `webaccess` and `ftpassess` policies:

```
http_access allow clientpc
porthttp protocolhttp timeweb
http_access allow clientpc portftp
protocolftp timeftp
```

Processing of the Example Policies

When the HTTP proxy URL filter is configured with the example `webaccess` and `ftpassess` policies, it grants access to connections that match the ACL entries that are included in the policies. To determine if access should be granted, the HTTP proxy URL filter first processes the `webaccess` policy (which has higher priority) for a match. If the connection does not match the `webaccess` policy, then the `ftpassess` policy is processed. The policies are processed as follows:

1. If *clientpc* **AND** *porthttp* **AND** *protocolhttp* **AND** *timeweb* are **TRUE**, grant access and stop processing rules.
Otherwise, proceed to the next rule.

2. If *clientpc* **AND** *portftp* **AND** *protocolftp* **AND** *timeftp* are **TRUE**, grant access.

Example Scenarios

It is Monday at 9:00. If a user at 10.0.81 tries to access the Internet on port 80, the first rule is processed. The connection is allowed by the *http_access* rule because *clientpc* **AND** *porthttp* **AND** *protocolhttp* **AND** *timeweb* are **TRUE**. No other rules are processed.

It is Monday at 18:00. If a user at 10.0.81 tries to access an FTP server on port 21, the the first rule is processed and determined to be FALSE because the connection does not match any criteria except for *clientpc*. Subsequently the second rule is processed, but it is determined that the connection does not match *timeftp*. The connection attempt is then rejected because it does not match both rules.

Access Control Settings

These sections provide more detailed descriptions of the settings that you configure for ACL entries and access control policies:

ACL Entries Settings

This table provides descriptions of the setting that you can configure for each ACL entry type:

ACL Type	Description
Time Restrictions	<p>Defines times and days. For this ACL entry type, you can configure the following settings:</p> <ul style="list-style-type: none"> • Time Zone - Select one of the following options to specify which time zone to use: <ul style="list-style-type: none"> ◦ <i>Use Local Box Time Zone</i> - Uses the local time zone of the system. ◦ <i>explicit</i> - Uses the time zone that is selected from the following Time Zone list. • Time Settings - Click Always and then select the required days and times in the Time Interval window. If specific days and times have already been selected for the time restriction, Always is changed to Restricted. By default, the configuration is always active. • Use Extended Time List - Enables the days and times that are listed in the Extended Time List table instead of those that are configured in the Time Settings section. (This setting is only available if Advanced View is selected from the Configuration Mode menu on the left.) • Extended Time List - In this table, add an entry for each day of the week. For each day, specify the times to include. <p>If time restriction applies, the label of the button changes to Restricted!.</p>

Source IP Destination IP Source IPv6 Destination IPv6	<p>Defines the source or destination IP address of a connection. For these ACL entry types, you can configure the following settings:</p> <ul style="list-style-type: none"> • IP Configuration - From this list, select one of the following options to specify if you are adding specific IP addresses or a range of IP addresses: <ul style="list-style-type: none"> ◦ <i>Singlemode</i> - Select to add specific IP addresses. ◦ <i>Rangemode</i> - Select to add a range of IP addresses. <p>NG Admin Settings applies if activated.</p> <ul style="list-style-type: none"> • IP Ranges From To - In these fields, enter the first and last IP addresses in the IP range. • Single IPs - In this section, add specific IP addresses to the Set IPs table.
Source Domain Destination Domain	<p>Defines client domains. Add the domains to the Domains table. Include a dot before the domain names. Example: <i>.barracuda.com</i>. Processing delays may be caused when using domain names. Squid needs to reverse DNS lookups (from client IP address to client domain name) before it can interpret the ACL.</p>
User Authentication	<p>Defines users who must authenticate themselves in an external authentication program. For this ACL entry type, you can configure the following settings:</p> <ul style="list-style-type: none"> • Required for All Users - Specifies if all users or only select users using the proxy must authenticate themselves. From this list, you can select: <ul style="list-style-type: none"> ◦ <i>yes</i> - All users must be authenticated. ◦ <i>no</i> - Only certain users must be authenticated. Add these users to the following Users table. • Users - If only certain users must be authentication, add their usernames to this table.
Groups	<p>Defines groups. For this ACL entry type, you can configure the following settings:</p> <ul style="list-style-type: none"> • Interpret as RegEx - If the groups list contains regular expressions and matching should be possible for RegEx meta symbols, select Yes. When this setting is enabled, the Partial Search and Case Insensitive settings are disabled. If there is only one meta symbol * or it is the first one in a RegEx, enter it by a leading . (dot). • Partial Search - To enable partial pattern matching, select Yes. • Case insensitive - If group matching is case insensitive, select Yes. • Groups - In this table, add meta directory group patterns. Group names are the distinguished names of meta directories. Example for LDAP: <i>CN=myname, OU=myOU, DC=com</i>
URL Path	<p>Defines URL path regular expressions (<i>urlpath_regex</i>) that match the URL but not the protocol or hostname. In the URL Path Extensions table, add regular expressions, words, or word patterns. All entries are treated as case-insensitive. The <i>urlpath_regex</i> looks for the specified value in the URL path following the hostname. For example, with <i>http://www.exampledomain.com/example/domain/index.htm</i>, the word "example" will only be looked for within the path <i>"/example/domain/index.htm"</i>.</p>

URL	<p>Defines URL extensions (url_regex) considering protocol and hostname (ACL Type = urlextension).</p> <p>In the URL Path Extensions table, add regular expressions, words, or word patterns. All entries are treated as case-insensitive. The url_regex looks for the specified value in the URL path including the protocol and hostname.</p>
Maximum Connections	<p>Defines the maximum number of connections from a single client IP address. In the Define Maximum Connections field, enter this limit. The value of the ACL is <i>TRUE</i> if the limit is exceeded.</p>
Protocol	<p>Defines a list of protocols. In the Define Transfer Protocol table, add transfer protocols such as <i>HTTP</i>.</p>
Requestmethod	<p>Defines a list of request methods. In the Define Request Method table, add request methods such as <i>GET</i>, <i>POST</i>, or <i>UPDATE</i>.</p>
TCP Port	<p>Defines a destination's port address. In the Specify Destination Port Address field, enter the destination server's port number.</p>
Browser	<p>Defines regular expression patterns or words, matching the user-agent header transmitted during the request. In the Define Browser Access table, add the regular expressions or words. For example, if you add <i>Firefox</i>, it will be searched for in the user-agent header of an incoming request.</p>
Mime Types	<p>Defines a list of MIME types. In the Mime Types table, add mime type expressions. For more information, see http://www.iana.org/assignments/media-types.</p>
URL Filter Categories	<p>Defines an ACL consisting of URL filter categories. For this ACL entry type, you can configure the following settings:</p> <ul style="list-style-type: none"> • URL Filter Categories - In this table, add the URL filter categories. • Num Categorize Helpers - The number of helpers for URL Filter categorization.
External	<p>Defines an ACL by using external helper programs. For this ACL entry type, you can configure the following settings:</p> <ul style="list-style-type: none"> • External Group - Uses an existing external helper or a new one. • External ACL Format - Defines the ACL input format, for example: the external ACL input type. • External ACL Binary - Import dialogue for external ACL binaries/scripts. • External ACL Binary Parameter - Parameter that will be passed to the external ACL helper program/script. • External Group Reference - Select an already defined external group ACL. • External ACL Parameter - Parameter for the defined external ACL.

Access Control Policies Settings

This table provides descriptions of the settings that you can configure for access control policies:

Setting	Description
ACL Priority	Enter a number to specify the priority for this policy. To assign higher priority to a policy, enter a lower number. Access control policies with higher priority are processed first.

Action	Specifies how to handle the ACL entries that are added to this policy. You can select <i>Allow</i> , <i>Deny</i> or, <i>Limit-Size</i> .
ACL Entries for this Action	In this table, add the ACL entries to which the selected action will be applied. Access control policies will only apply if <i>all</i> ACL entries are met. For example, if you add three ACL entries to one policy, the policy only applies if all three ACL entries match. When you delete an ACL entry, you must also delete it from any access control policies that it has been added to.
Overall Maximum File Size	If the selected action for this policy is <i>Limit-Size</i> , enter the maximum size of files that can be downloaded. To disable this setting, enter <i>0</i> . This setting may be configured more granular as ACL.
ACL Policy Description	Brief description of the policy action and the ACL entries that it affects.

Figures

1. Time_FTP.png
2. Time_Web.png
3. ACLEntries.png
4. Access_Control_Policies.png

© Barracuda Networks Inc., 2021 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.