How to Configure User Authentication and Access Control

https://campus.barracuda.com/doc/79463099/

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 forwarding proxy, you can use either MS-CHAP or Kerberos for transparent authentication. In case these authentication methods fail, you can configure one of several other authentication schemes, such as NGF-Local, MS-AD, LDAP, or Radius, to serve as a fallback.

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.

Depending on the HTTP Proxy mode, different authentication schemes are supported:

- **Forward Proxy Mode** – MS-CHAP or Kerberos. For more information, see How to Configure MS-CHAP Authentication or How to Configure Kerberos Authentication.
- **Forward Proxy Mode without transparent authentication** – In case MS-CHAPv2 or Kerberos are not available, you can configure an authentication fallback.
- **Transparent Proxy Authentication** – DC Client. For more information, see How to Configure MSAD DC Client Authentication and Barracuda DC Agent for User Authentication.

Configure User Authentication

Step 1. Enable User Authentication

For the forward proxy, you can use either MS-CHAP or Kerberos. For the transparent or reverse proxy, only DC Client for authentication is supported.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP Proxy Settings**.
2. Click **Lock**.
3. In the left menu, select **User Authentication**.
4. 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.

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

Step 2. (optional) Configure User Authentication for Forwarding Proxy Without Transparent Authentication

In case MS-CHAPv2 or Kerberos is not available, you can configure an authentication fallback, e.g., NGF Local.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP Proxy Settings**.
2. Click **Lock**.
3. In the left menu, select **User Authentication**.
4. In the **Authentication Service Settings**, configure:Click **OK**.
   - **Authentication Text** – Enter a welcome message that is displayed when a user is prompted by the fallback authentication scheme.
   - **Authentication Scheme** – Select your fallback authentication scheme, e.g., **NGF Local**.
   - **Use FW Login as Authentication** – Select **Yes**. The HTTP Proxy service queries the firewall login status of the client. If the client is already authenticated, no further HTTP Proxy authentication is needed.
   - **User List Policy** – In case there are users that are not allowed to use the proxy service, select **deny-explicit**. In case only domain users listed in the User List are allowed to use the proxy service, select **allow-only**.
   - **User List** – Click **+** to add users to the list that must fulfill the User List policy.
   - **User names case sensitive** – Select **yes** if every single letter in the user name must match lower-case or capital letters; otherwise, select **no**.
5. Click **Send Changes** and **Activate**.

Step 3. Configure Access Control Policy

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

1. Go to **CONFIGURATION > Configuration Tree > Box > 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**.
   If no **ACL Entries** are configured and user authentication is used, the **Default Access Control Policy** is not applied and access control allows every authenticated user.
5. For each ACL, click **+** to add entries to the **ACL Entries** table:
   1. Enter a **Name** and click **OK**.
      Configure the **Access Control Policy**:
      - **ACL Priority** – Enter a number. Highest numbers are processed first.
      - **Action** – Select the action:

- **Allow**
- **Deny**
- **Deny and redirect** – Enter an external **Redirection** address.
- **Limit-Size** – Enter the **Overall Maximum File Size (MB)**.
- **Outgoing Address** – Set the **Outgoing IP Address** for the connection.
- **Include** – Select additional **ACL Files** to include into the configuration.

- **ACL Entries for this Action** – Select the **ACL Entries** this ACL is applied to.

Before deleting an ACL entry, remove it from the ACL policies. ACL policies with broken links to non-existent ACL entries cause the HTTP proxy to fail.

When configuring **User Authentication** ACL entries in combination with NTLM or MS-CHAP authentication, the username must be entered in the following format: `DOMAIN\username`.

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 on control policies, see Access Control Policy Example.

Step 4. (optional) Configure Access Control File List

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. In the left menu, select **Access Control**.
3. In the left menu, expand the **Configuration Mode** section, and 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 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**.

Step 5. (optional) Legacy ACL Settings

If you must configure squid settings in legacy ACL in squid.conf syntax, enable the legacy ACL settings mode.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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.
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.

Access Control Policy Example

On the Barracuda CloudGen 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.

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

Creating the Example Access Control Policies

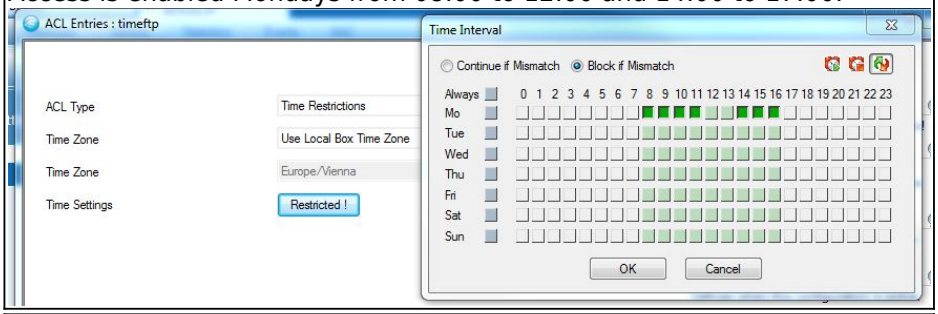
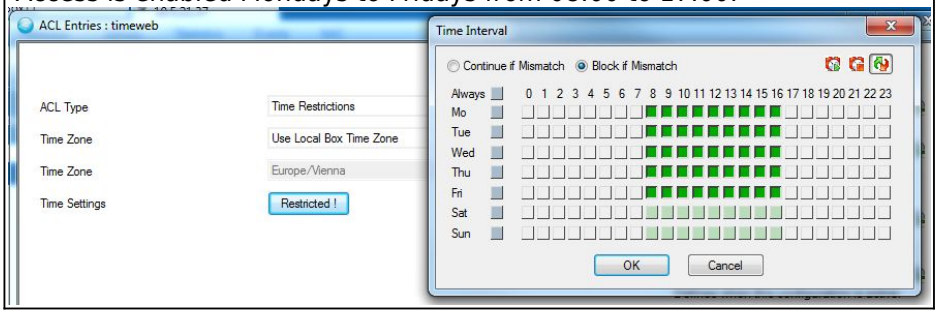
This example procedure configures two access control policies that limit FTP and HTTP access for a client at 10.0.8.1 to the following days and times:

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

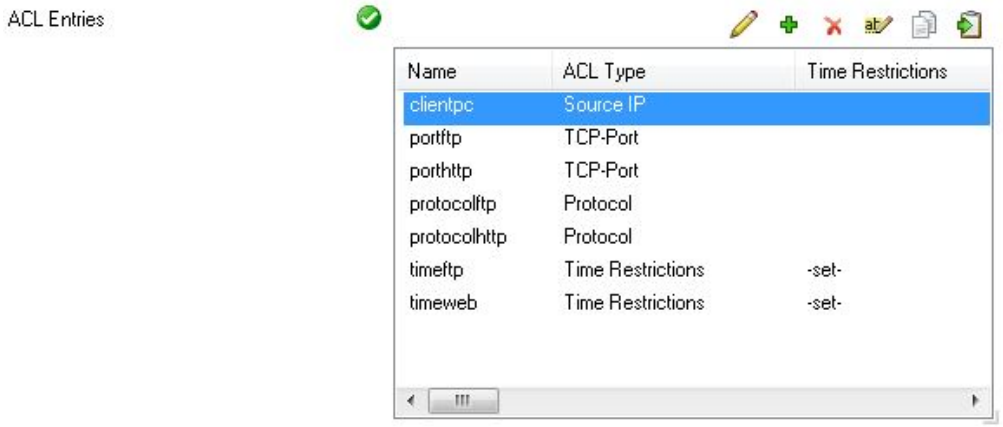
First create all of the required ACL entries. Then add these entries to the policies.

1. Go to **CONFIGURATION > Configuration Tree > Box > 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*	◦ **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*	Access is enabled Mondays from 08:00 to 12:00 and 14:00 to 17:00: 
timeweb	*Time Restrictions*	Access is enabled Mondays to Fridays from 08:00 to 17:00: 

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:

- **M** – Monday
- **T** – Tuesday
- **W** – Wednesday
- **H** – Thursday
- **F** – Friday
- **A** – Saturday
- **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:

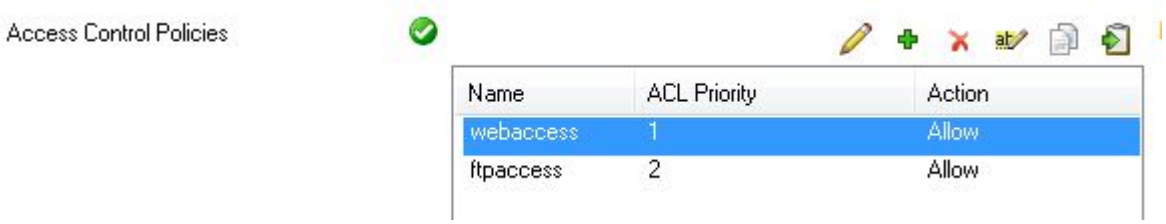
timeftp	**timehttp**

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.	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

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

Access Control Policy Name	Settings
webaccess	◦ **ACL Priority**: *1* ◦ **Action**: *Allow* ◦ **ACL Entries for this Action**: ■ *clientpc* ■ *porthttp* ■ *protocolhttp* ■ *timeweb*
ftpaccess	◦ **ACL Priority**: *2* ◦ **Action**: *Allow* ◦ **ACL Entries for this Action**: ■ *clientpc* ■ *portftp* ■ *protocolftp* ■ *timeftp*

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



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

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

Processing the Example Policies

When the HTTP proxy URL filter is configured with the example webaccess and ftpaccess 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, the ftpaccess policy is then 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	Defines times and days. For this ACL entry type, you can configure the following settings: • **Time Zone** – Select one of the following options to specify which time zone to use: ◦ *Use Local Box Time Zone* – Uses the local time zone of the system. ◦ *explicit* – 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. If time restriction applies, the label of the button changes to **Restricted!**.
Source IP | **Destination IP** | **Source IPv6** | **Destination IPv6**	Defines the source or destination IP address of a connection. For these ACL entry types, you can configure the following settings: • **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: ◦ *Singlemode* – Select to add specific IP addresses. ◦ *Rangemode* – Select to add a range of IP addresses. Inverted CIDR notation applies if activated. • **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**	Defines client domains. Add the domains to the **Domains** table. Include a dot before the domain names. Example: *.barracuda.com.* 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.
User Authentication	Defines users who must authenticate themselves in an external authentication program. For this ACL entry type, you can configure the following settings: • **Required for All Users** – Specifies if all users or only select users using the proxy must authenticate themselves. From this list, you can select: ◦ *yes* – All users must be authenticated. ◦ *no* – Only certain users must be authenticated. Add these users to the following **Users** table. • **Users** – If only certain users must be authenticated, add their usernames to this table.

Groups	Defines groups. In case you want to access MSAD-groups with NTLM via MSCHAP, you must configure the MSAD authentication service to provide this information. For more information, see How to Configure MSAD Authentication. For this ACL entry type, you can configure the following settings: • **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 metadirectory group patterns. Group names are the distinguished names of metadirectories. Example for LDAP: *CN=myname, OU=myOU, DC=com*
URL Path	Defines URL path regular expressions (urlpath_regex) 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 urlpath_regex looks for the specified value in the URL path following the hostname. For example, with *http://www.exampledomain.com/example/domain/index.htm*, the word "example" will only be looked for within the path "/example/domain/index.htm".
URL	Defines URL extensions (url_regex) considering protocol and hostname (ACL Type = urlextension). 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.
Maximum Connections	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 *TRUE* if the limit is exceeded.
Protocol	Defines a list of protocols. In the **Define Transfer Protocol** table, add transfer protocols such as *HTTP*.
Requestmethod	Defines a list of request methods. In the **Define Request Method** table, add request methods such as *GET*, *POST*, or *UPDATE*.
TCP Port	Defines a destination's port address. In the **Specify Destination Port Address** field, enter the destination server's port number.
Browser	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 *Firefox*, it will be searched for in the user-agent header of an incoming request.
Mime Types	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 .

URL Filter Categories	Defines an ACL consisting of URL filter categories. For this ACL entry type, you can configure the following settings: • **URL Filter Categories** – In this table, add the URL filter categories. • **Num Categorize Helpers** – The number of helpers for URL Filter categorization.
External	Defines an ACL by using external helper programs. For this ACL entry type, you can configure the following settings: • **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 a pre-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 *Allow*, *Deny* or, *Limit-Size*.
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 *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. 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 *Limit-Size*, enter the maximum size of files that can be downloaded. To disable this setting, enter *0*. This setting may be configured more granularly 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