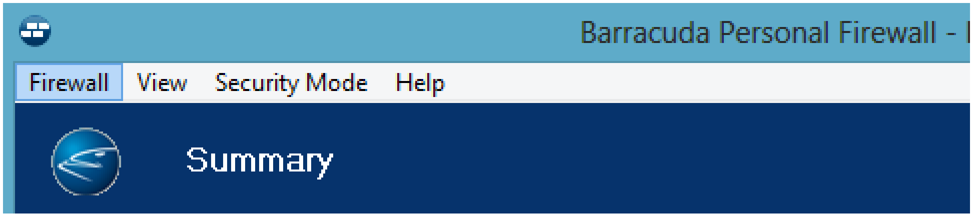
How to Use the Barracuda Personal Firewall

https://campus.barracuda.com/doc/46895469/

The Barracuda Personal Firewall is a centrally managed host firewall that can handle up to four different rulesets at once, depending on the policy applicable to user, machine, date, and time. In the Barracuda Personal Firewall interface, you can edit the **Local Machine** ruleset, adjust the security level, and monitor activities and events in live and history mode.

Selecting the Firewall Mode

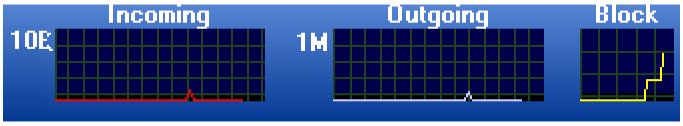
1. Open the configuration screen of the Barracuda Personal Firewall.
2. Click the **ALT** key to display the menu bar on top of the configuration window (use the **ALT** key to open or close the menu bar):



3. To open the functional firewall mode selection, expand the **Security Mode** menu.
   You can select one of the following functional firewall modes in the context menu of the system tray icon:
   - **Block All**
   - **Secure Mode**
   - **Disable Firewall (Allow all Traffic)**

> Do not directly switch from **Disable Firewall (Allow all Traffic)** to **Block All**. Always select **Secure Mode** as the intermediate step.

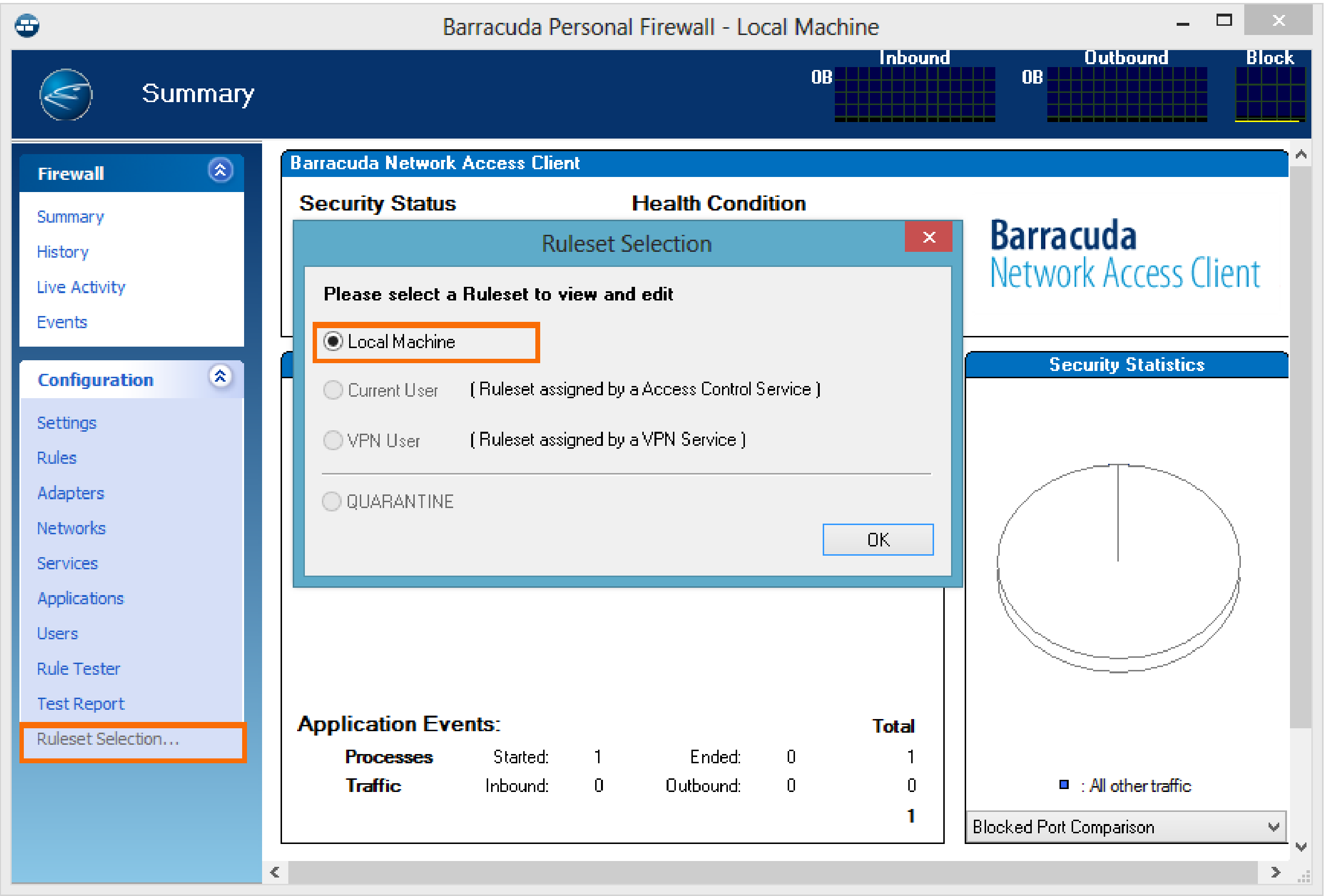
The load display on the top right of the **Summary** window shows the overall traffic load processed by the Barracuda Personal Firewall.



Selecting the Ruleset

Click **Ruleset Selection** in the bottom left menu to select one of the available rulesets for viewing.

The **Local Machine** ruleset is selected by default. Only the **Local Machine** ruleset may be edited in the Barracuda Personal Firewall.



Ruleset Selection

Please select a Ruleset to view and edit

● Local Machine

○ Current User (Ruleset assigned by a Access Control Service)

○ VPN User (Ruleset assigned by a VPN Service)

○ QUARANTINE

OK

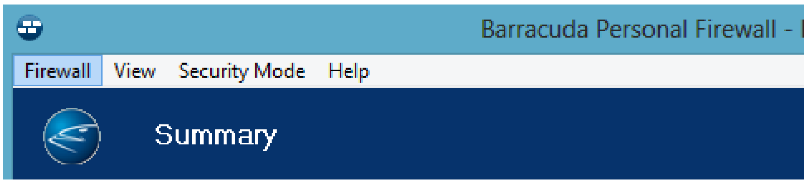
Application Events:

					Total
Processes	Started:	1	Ended:	0	1
Traffic	Inbound:	0	Outbound:	0	0
					1

To learn how to configure centrally managed Personal Firewall rulesets on the Barracuda CloudGen Firewall, see How to Configure Personal Firewall Rules on the CloudGen Firewall.

The Personal Firewall Menu Bar

Clicking the **ALT** key makes the following options available (use the **ALT** key to open or close the menu bar):



Firewall Menu

- **Save Configuration** – Saves configuration changes immediately. To save configuration changes after prior confirmation inquiry, click the **Save Configuration** link within the configuration item bar.
- **Settings** – Select this item to adjust general behavior of the Barracuda Barracuda Personal Firewall.
  You can configure the following parameters:
    - **Firewall Settings Tab** – Configure various firewall settings here.
        - **Log dropped packets / Log successful connections** – Select these check boxes to activate logging for dropped packets and / or successful connections.
        - **File name** – Path and name of the VPN client log file. By default, the file is saved to: `C:\Program Files\BarracudaNG\phlog.txt`
        - **Size limit** Maximum size in KByte for the log file.
        - **IP Monitor** Selecting this check box (default) activates the dynamic updating of network objects (see Network Objects).
        - **Automatic Adapter Assignment** – Selecting this check box (default) activates the dynamic updating of network interface adapters. If active, network adapters are automatically added to the **Adapter Objects** configuration area as soon as they are used for the first time (see Adapter Objects).
        - **Disable Windows Firewall** Selecting this check box (default) disables the Windows firewall if it is installed.
        - **Block all IP Fragments** – By default, IP fragments are generally allowed to pass the firewall notwithstanding the configured ruleset. Select this check box to block IP fragments.
    - **ICMP Parameters Tab** – Configure the blocking of ICMP packets here.
    - **ICMPv6 Error Messages Tab** – By default, IPv6 packets are generally allowed to pass the firewall notwithstanding the configured ruleset. Select these check boxes to block IPv6 packets.
- **Export Firewall Ruleset** – This item allows you to export the ruleset from the Barracuda Personal Firewall to a text file.
- **Import Firewall Ruleset** – This item allows you to import a ruleset into the VPN client. The ruleset may either originate from another Barracuda Personal Firewall or from a firewall configured on a Barracuda CloudGen Firewall.
- **Close Firewall Window** – Selecting this item closes the Barracuda Personal Firewall configuration window.

View Menu

- **DCERPC List** – Status of each DCERPC communication slot. For detailed information concerning DCERPC, see the Barracuda CloudGen Firewall documentation.
- **Access Control Server IPs** – Displays every Access Control Server the client knows of.
- **Activated Application Time Frame Rules** – Displays rules with a configured time frame.
- **Route Advertise List** – Displays route advertising information.

Security Mode Menu

The items in the **Security Mode** menu allow you to adjust the security level of the Barracuda Personal Firewall.

- **Block All** – Prohibit all traffic.
- **Secure Mode** – Activate customized firewall rulesets.
- **Disable Firewall (Allow All Traffic)** – Turn the firewall off and allow all traffic.
- **Process Monitor** – Generate an entry in the **Events** monitor for every process initiation. The load display is a graphical view of current incoming and outgoing connections. The dimensions of the graphs depend on the current peak load. The last graph (**Block**) depicts the amount of blocked connections.
- **Adapter Reset** – Resets adapters to initial state.
- **Increase permissions** – Change administrative firewall permissions.

Help Menu

This section offers online help and displays product information.

Monitoring Personal Firewall Activities

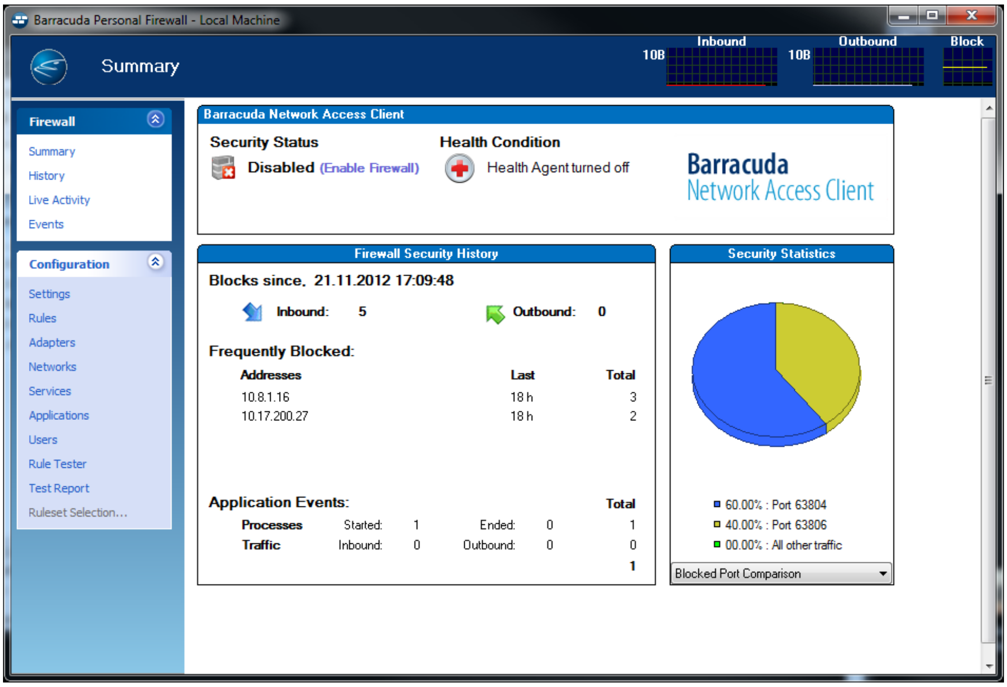
The **Firewall** menu in the left navigation bar provides access to the **Life Activity** view. Items arranged in the **Life Activity** view give a review of application activities in the Barracuda Personal Firewall. The **Life Activity** view is divided into the following sub-items:

Summary

In the **Summary** window, the current security state is indicated as following:

- **Disabled** – By default (after a fresh installation), the firewall is in disabled state. Click the link to enable the secure mode.
- **Secure** – The secure firewall mode is active. Click the link to deactivate any impacts of the configured ruleset.

The **Summary** view gives a quick comparative overview of the 5 most used **Ports**, **Active Internet**, and **Blocked Applications**.



Barracuda Network Access Client

Security Status: Disabled (Enable Firewall)

Health Condition: Health Agent turned off

Firewall Security History

Blocks since. 21.11.2012 17:09:48

Inbound: 5 Outbound: 0

Frequently Blocked:

Addresses	Last	Total
10.8.1.16	18 h	3
10.17.200.27	18 h	2

Application Events:

					Total
Processes	Started:	1	Ended:	0	1
Traffic	Inbound:	0	Outbound:	0	0
					1

Security Statistics

- ■ 60.00% : Port 63804
- ■ 40.00% : Port 63806
- ■ 00.00% : All other traffic

History

The **History** view details the entire network traffic (established connections and connection attempts) that appeared since the last system boot. The listing is divided into the following columns:

- **Direction** – Flags the connection direction (**Incoming** icon, **Outgoing** icon).
- **Connection State** – Flags the connection state (**Granted connections** icon, **Blocked connection attempts** icon, **Failed connection attempts** icon).
- **Date/Time** – Date and time of traffic initiation.
- **Application** – Name of the application.
- **Protocol** – Protocol assigned to the application.
- **Source** – Source IP of the connection.
- **Destination** – Destination IP of the connection.
- **Port** – Connection port.
- **User** – Name of the user who initiated the connection attempt.
- **Traffic Policy** – Name of the effective firewall rule.
- **Info** – Connection status (**passed**, **blocked**, **failed**).
- **Count** – Total number of connections processed over this slot.
- **Last** – Time passed since the last traffic activity over this slot.
- **Service** – Affected service object or UUID (Universal Unique IDentifier).
- **Adapter** – NIC that was used for connection.
- **AID** – Unique Access ID of the connection.

Select and then right-click a list entry to display the following context menu:

- **Show Details** – Select **Show Details** or double-click a list entry to view a summary of

connection details.
- **Show Rule** – Displays rule information if applicable.
- **Expand/Collapse all** – Expands/collapses the entry list.
- **Resolve Source/Destination IP** – Tries to resolve the source and destination IP adresses and summarizes the results (port, IP address, hostname, and description) in a separate window.
- **Send to Rule Tester** – Inserts the connection details into the rule tester and opens the rule tester window.
- **Add Pass Rule** – Inserts the connection details into a new rule with default action **Pass** and opens the rule object window for editing.
- **Add Block Rule** – Inserts the connection details into a new rule with default action **Block** and opens the rule object window for editing.
- **Flush History** – Clears all entries from the history listing.
- **Details View** – Displays rule information if applicable.
- **Group by** – Groups list entries by the selected item.
- **Ungroup** – Undoes the **Group by** command and sorts the connection entries into a successive listing.
- **Tools** – Offers the standard **Tools** context menu.

In the **History Selection** tab, the following check boxes are available for fast and easy filtering.

- **Access** – Only displays connections that have been granted (marked with a green dot).
- **Rule Block** – Only displays connection attempts that have been blocked (marked with a red square).
- **Fail** – Only displays connection attempts that have failed (marked with an exclamation mark).
- **Show all Ethernet protocols** Additionally displays connection attempts over protocols other than TCP, UDP, or ICMP.
- **Show Hostnames** Translates IP addresses into hostnames, if possible.

After each selection change, click the **refresh arrows icon** to refresh the view. Click the **Group History by** link to sort listing entries by topic.

In the **History Filter** tab, filter conditions can be set to confine the view to the minimum desired number of entries. If filters apply, the **History Filter** tab is highlighted in yellow. Select the check box on the right side of an available filter to activate it and insert the condition to apply.

- **Policy** – Filter the connection’s traffic policy.
- **Source** – Filter the source IP address of the connection.
- **Application** – Filter the application that has attempted to connect.
- **In/Out**– Filter incoming or outgoing connections.
- **Protocol** – Filter a connection protocol.
- **Destination** Filter the destination IP address of the connection.
- **Port** – Filter a connection port.
- **Show matching entries / Hide matching entries** Toggle between displaying and hiding the matching entries.

Live Activity

The **Live Activity** view details all currently active connections. The listing is divided into the following columns:

- **Direction** Flags the connection direction (**Outgoing connections** icon, **Incoming connections** icon).
- **Load** – Displays the current connection load using a bar graph.
- **Date/Time** – Date and time of traffic initiation.
- **Application** – Application name and its PID (Process ID).
- **Protocol** Protocol assigned to the application.
- **Source** – Source IP address of the connection.
- **Destination** – Destination IP address of the connection.
- **Port** – Connection port.
- **User** – Name of the user who has initiated the connection attempt.
- **Policy** – Name of the effective firewall rule.
- **bps** – Connection load in bits per second.
- **Idle** – Idle time of the connection.
- **Total** – Total amount of traffic summarized from incoming (**In** column) and outgoing (**Out** column).
- **Start** – Time that has passed since the connection's initiation.
- **Action** – Action affecting the connection.
- **Service** – Affected service object or UUID (universal unique identifier).
- **ID** – Internal slot ID.
- **Session Timeout** – Effective connection state or current session timeout value.

Select and right-click a list entry to display the following context menu:

- **Show Details** – Select **Show Details** or double-click a list entry in order to view a summary of the connection details.
- **Show Rule** – Shows the effective firewall rule.
- **Disconnect** – Terminates the selected connection.
- **Resolve Source/Destination IP** – Tries to resolve the source and destination IP addresses and summarizes the results (port, IP address, hostname, and description) in a separate window.

Entries displayed in *italics* indicate closed connections waiting for RST-ACK (reset acknowledgement). The closed connections must wait for RST-ACK so they are not blocked by the firewall.

Click the **Filter** button on the top right to open the **Filter Condition** window. This allows you to specify filter conditions in order to confine the view to the minimum desired number of entries. Click **Activate** to activate the filter settings. Click **Disable** to deactivate the filter settings. After specifying a filter, click the **Refresh** icon to refresh the view.

Click **Capture** to record traffic processed over the network interface. Administrator rights are required to use the **Capture** option. The data acquired is saved as a `.cap` file in the local folder of the VPN client (usually **C:\Program Files\BarracudaNG**).

> A special viewer is needed for viewing network traffic recorded in `.cap` files. You may use, e.g., *wireshark* for this purpose; it's downloadable at www.wireshark.org.

Events

The **Events** view details all applications that are currently or have been executed on the system. Double-click a list entry to view event details. Select **Reload Logs** from the context menu to reload the display of logged entries. The listing is divided into the following columns:

- **Date** – Date and time the connection has been initiated.
- **Action** – Type of recorded action: System Information, Monitored connection, or Informational message.
- **Application** – The application that initiated the connection and assigned the port over which the connection is processed.
- **Parent** – Parent process that initiated the application.
- **Access** – Status and direction assigned to the connection. An application can either be in **Process started** or **Process ended** state, and the connection direction can either be **Outbound** or **Inbound**.
- **User** – The user object assigned to the connection (see also: User Objects).
- **Object** – Full path to the application responsible for the connection.

The **Filter** section allows you to define filters in order to narrow down the view in the event listing. Select the check box assigned to an item to activate filter effectiveness, and select or insert the desired filter value. Click **Refresh** to apply the filter settings.

Figures