How to Configure the Barracuda Personal Firewall

https://campus.barracuda.com/doc/46206573/

When connected to an Access Control Service or via VPN, the Barracuda Personal Firewall can accept rulesets sent from the Barracuda CloudGen Firewall (depending on the client license used). The Barracuda Personal Firewall supports multiple rulesets, dynamic adapter handling, RPC handling, and client-side policy enforcement. Usually, the configuration of the firewall is made directly at the server. See How to Configure Personal Firewall Rules on the NextGen Firewall. The Barracuda Personal Firewall integrates with the Windows intrusion control system. If configured to do so, it will properly replace the built-in Windows firewall as long as it is enabled. Disabling the Barracuda Personal Firewall will automatically re-enable the Windows firewall. You can view the current protection status in your Windows Control Panel.

Configure Personal Firewall Settings

The **Settings** view of the Barracuda Personal Firewall allows you to adjust the preconfigured local ruleset of the Barracuda Personal Firewall. Changing these paramaters either triggers rule creation, deletion, or traffic policy changes. Use this configuration area to customize the preconfigured ruleset. Some settings defined in this window are triggered by specifications defined during the installation process by default. See also: Installing the Barracuda Network Access/VPN Client for Windows.

1. Open the configuration screen of the Barracuda Personal Firewall in one of two ways:
   - by right-clicking the **VPN Status** icon in the system tray, then by selecting **Personal Firewall** from the context menu
   - by browsing to **Start > All Programs > Barracuda Network Access Client > Personal Firewall** in the Windows start menu
2. In the **Configuration** menu on the left, select **Settings**.

The **Personal Firewall Settings** window allows overall definition of the Barracuda Personal Firewall **Security Level**:

- **User mode** – Allows and blocks access as customized in the ruleset.
- **Domain** – Allows outbound and inbound core network, IPv6 tunnel, file and printer sharing, and network discovery.
- **WLAN** – Allows outbound and inbound core network, IPv6 tunnel, outbound file and printer sharing. Blocks outbound and inbound network discovery and inbound file and printer sharing.
- **Mixed** – Allows outbound and inbound core network, IPv6 tunnel, file and printer sharing, and network discovery only on trusted adapters.
- **Lockdown** – Locks the Barracuda Personal Firewall and blocks all outbound and inbound traffic.

The following customizable settings are available:

- **My Trusted Network** – By default, this option points to the preconfigured **MyNet** object. Network assignments and references in the network object that have been defined as trustworthy are updated dynamically as soon as network adapters are added to the system with a trust assignment level of **trusted**, or as soon as the IP address configuration of a trusted adapter changes. For more information, see Network Objects and Adapter Objects. You may change this setting to use another available network object. Be aware of possible implications. **Block Trusted Network** disables the feature.
- **IPv6 Router Advertisement Guard Mode** – When using IPv6 router advertisement, select the behavior of the IPv6 router advertisement guard. For more information, see The IPv6 Router Advertisement Guard.
- **Toredo Tunnel** – Enables tunneling IPv6 over UDP through Network Address Translations (NATs).
- **IPv6 over IPv4** – Allows tunneling of IPv6 in IPv4 packets.
- **Barracuda VPN** – Enables standard Barracuda VPN.
- **Web access** – Enables/disables access to the Internet.
- **File and Printer Sharing** – Can only be enabled when a network object has been configured as **Trusted Network**. When set to **yes**, incoming connections to local printer(s) and files are allowed.
- **Ask for unknown outbound / inbound –** Enforces a manual confirmation for all outgoing / incoming connection attempts. Confirmation for the connection establishment grant is then requested by a notification window.
- **Ask for adapter update confirmation** – Triggers a modal dialog as soon as settings assigned to a network adapter change. For more information, see **Automatic Adapter Configuration** below.
- **Reset Ruleset to Default** – Resets the ruleset to default.
- **Default IPv6 Objects** – Defaults IPv6 network objects.

Automatic Adapter Configuration

Enable the **Ask for adapter update confirmation** option in the firewall settings if you want to be notified of adapter configurations changes. A security alert window will then pop up asking you to confirm each configuration change. Generally, the security alert window will pop up if:

- an adapter is used for the first time (for example, if it is added to the system).
- the IP configuration of an adapter changes (for example, if an IP address is added or deleted).

It will not pop up if:

- an IP address is reintroduced (for example, on a DHCP renew).
- an adapter's IP configuration is reset to **0.0.0.0.**

Click **Untrust** to add the adapter to the **Adapter Objects** list and assign it as **Untrusted** adapter. This will create an incoming adapter block rule in the **Incoming** tab of the firewall ruleset configuration area (see Rules). Click **Trust** to add the adapter to the **Adapter Objects** list and assign it as trusted adapter. This will add a reference to the trusted adapter in the **TrustedNet** object and delete a possibly existing incoming adapter block rule in the **Incoming** tab of the firewall ruleset

configuration area. For a detailed description of adapter configuration options, see Adapter Objects.

Automatic Rule Configuration

If **Ask for unknown outbound / inbound** is active in the firewall settings, an unknown application or service requesting network connection will trigger a security alert pop-up window requesting authorization. The following information is included in the security alert window:

- **Date / Time** – Time of the connection request.
- **Local Server / Program** – Application requesting the connection.
- **Path** – Full path to the application requesting the connection.
- **User** – User responsible for the connection request.
- **Source / Destination** – Connection source and target destination and port.
- **Service** – Service requesting the connection.
- **Message Counter** – Number of security alerts to be considered. Click the arrows to scroll through the alert windows.
- **More Info** – Click this link to open the online help.

Select **Remember this answer** (default) to permanently allow or deny a connection request. Selecting this check box automatically creates a corresponding rule in the **Configuration** area of the Barracuda Personal Firewall, including required **Network**, **Service**, **Application** and **User Objects**. If cleared, one-time access is granted for this specific connection request when clicking **Allow**. Selecting the check box also makes the **Advanced Policy** link available. Click the link in order to customize further connection details:

- **Only this Destination/Source** – Binds the outgoing or incoming connection to a specific IP address.
- **All Destinations/Sources** – If selected, this detaches the connection binding from a specific IP address (default).
- **Only Port** – Binds the outgoing or incoming connection to a specific port. This option is selected by default to allow a restrictive ruleset only.
- **All activities for this application** – Allows connection initiation on arbitrary ports if selected.
- **Port Range** – Select this and insert a port range in order to allow connection initiation on the specified ports only.

Click **Allow** to grant the connection request with regards to the conditions defined above. Or, click **Block** to deny the connection request with regards to the conditions defined above.

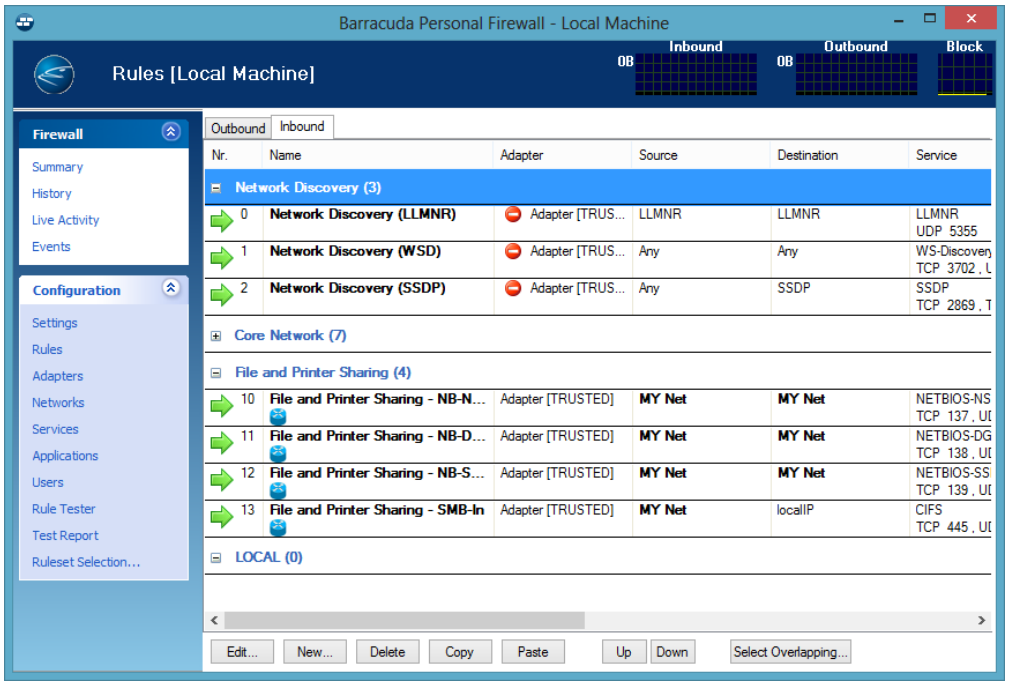
A connection request related to browsing the Internet with a web browser should be treated differently than other more specific connection requests. For connections initiated by the browser, select **All Destinations**. With **All Destinations** selected, the ruleset will be created referencing the global **InterNet** object. However, with **Only this Destination** selected, the ruleset will be created to reference only the specific web server's address.

You may use hot keys in the security alert window: holding the **CTRL** key while left-clicking either **Allow** or **Block** confirms all current connection notifications. The number of messages is shown in the message counter. Or, pressing the **Escape** key confirms the current connection notification with **Block**.

The Personal Firewall Ruleset

The **Rules** view in the configuration window of the Barracuda Personal Firewall allows manual rule configuration. To access the **Rules** view, expand **Configuration** and click **Rules** in the left navigation menu. Depending on the selected ruleset (click **Ruleset Selection** in the left navigation menu and chose **Local Machine**, **Current User** or **VPN User**), you can configure rule objects for the different stages.

Rules controlling incoming traffic are arranged in the **Inbound** tab; rules controlling outgoing traffic are arranged in the **Outbound** tab.



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

- **Edit / New** – Opens the rule configuration dialog for the selected rule / allows to create a new rule.
- **Delete** – Deletes the selected rule(s).
- **Copy / Paste** – Copies the selected rule(s) into the clipboard / pastes the selected rule(s) out of the clipboard.

- **Select Overlapping** – Because a connection request can match several conditions, the succession of the rules within a ruleset is very important. If rules are in an erroneous sequence, they might interfere with one another. The **Select Overlapping** function is meant to help avoidconfiguration mistakes. When applied to a selected rule, all rules possibly interfering with it are highlighted. In the majority of cases, the overlap is a harmless outcome of using very openly defined objects, such as the **InterNet** object.

Right-click a list item and select **Show** to display the following context menu:

- **Show Source / Destination Addresses** – Opens a window displaying all source / destination addresses affected by the selected rule.
- **Show Services / Applications / Adapters / Users** – Opens a window displaying all services / applications / adapters / users affected by the selected rule.

The option bar at the bottom of the page offers some of the functionalities of the context menu. The **Up** and **Down** buttons enable you to select a rule followed by clicking one of these buttons in order to shift the rule either up or down within the ruleset. Alternatively, you can drag and drop rules within the ruleset.

> According to a regular Barracuda CloudGen Firewall ruleset, the Barracuda Personal Firewall ruleset is processed in sequence until an applicable rule is available. Therefore, to achieve correct rule processing, rules need to be arranged in the correct order.

Create Personal Firewall Rules

The **Rules** view allows you to create Personal Firewall rules. Usually, the configuration of rules is made directly at the server. See How to Configure Personal Firewall Rules on the NextGen Firewall.

Adapters

The **Adapters** view allows you to view and configure network adapters available on the system. Adapters may be employed in firewall rules in order to restrict rule processing to a specific adapter or a set of adapters only. In the **Adapter Objects** view, several dynamic adapter objects are preconfigured. For more information, see Adapter Objects.

Networks

The **Networks** view facilitates IP address/network management. Use the **Networks** window to assign names to single IP addresses or to combine several IP addresses, networks, or references into

networking objects. For clearly arranged network management, use referencing network objects instead of explicit IP addresses when configuring CloudGen Firewall rulesets. For more information, see Network Objects.

Services

The **Services** window facilitates port and protocol management. Use the **Services** window for assigning ports and protocols to specific services and for merging multiple services to one **Service Object** using references. For more information, see Service Objects.

Applications

Application objects are used to reference lists of applications when creating application-aware firewall access rules. The **Application Objects** window allows you to create predefined applications for employment in rulesets. The preconfigured default application objects are required in Microsoft Windows domains. For more information, see Application Objects.

Users

The **Users** view allows you to create user objects to be employed in rulesets. A user object can contain a list of users that can be used in firewall rule conditions. For more information, see User Objects.

Rule Tester / Test Report

Opens the Personal Firewall rule tester and displays rule testing results. For more information, see How to Test Personal Firewall Rules.

Ruleset Selection

Allows selection of 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.

Saving Configuration Changes

To save configuration changes made on the Barracuda Personal Firewall, use the option provided on the page, or click the **Alt** key, expand the **Firewall** menu, and select **Save Configuration**.

Figures