

How to Configure the Barracuda Personal Firewall

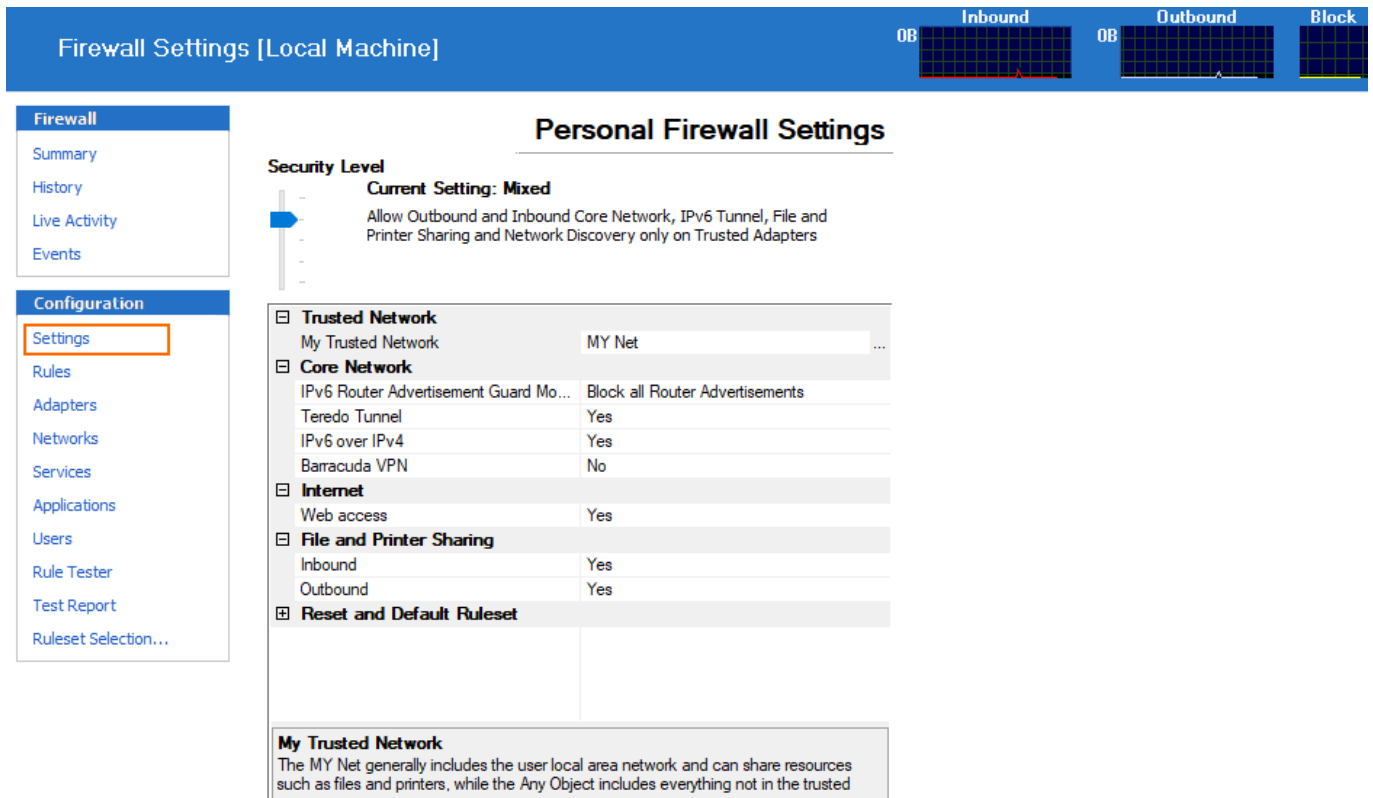
<https://campus.barracuda.com/doc/75696499/>

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 CloudGen 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 parameters 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**.



Firewall Settings [Local Machine]

Personal Firewall Settings

Security Level

Current Setting: Mixed
 Allow Outbound and Inbound Core Network, IPv6 Tunnel, File and Printer Sharing and Network Discovery only on Trusted Adapters

Trusted Network	
My Trusted Network	MY Net
Core Network	
IPv6 Router Advertisement Guard Mo...	Block all Router Advertisements
Teredo Tunnel	Yes
IPv6 over IPv4	Yes
Barracuda VPN	No
Internet	
Web access	Yes
File and Printer Sharing	
Inbound	Yes
Outbound	Yes
Reset and Default Ruleset	

My Trusted Network
 The MY Net generally includes the user local area network and can share resources such as files and printers, while the Any Object includes everything not in the trusted

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.](#)

- **Teredo 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 inbound / outbound** – Can only be enabled when a network object has been configured as **Trusted Network**. When set to **Yes**, connections to local printer(s) and files are allowed.
- **Reset Ruleset to default** – Resets the ruleset to default.
- **Default IPv6 Objects** – Defaults IPv6 network objects.

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.

Barracuda Personal Firewall - Local Machine

Rules [Local Machine]

OB Inbound OB Outbound Block

Firewall

- Summary
- History
- Live Activity
- Events

Configuration

- Settings
- Rules
- Adapters
- Networks
- Services
- Applications
- Users
- Rule Tester
- Test Report
- Ruleset Selection...

Nr.	Name	Adapter	Source	Destin...	Service	Application	User	Comment
Barracuda VPN (2)								
0	Barracuda VPN - Tunnel		localIP	Any	BARRACU... TCP 3128 ...	BARRACUDA VPN cudanacsvc.exe		Outbound
1	Barracuda VPN - Payload	Adapter [VPN]		Any	Any	Any		Outbound
Network Discovery (3)								
2	Network Discovery (WSD)	Adapter [TRUST...]	Any	Any	WS-Discover... TCP 3702 ...	SVCHOST SVCHOST.EXE		Outbound
3	Network Discovery (LLMNR)	Adapter [TRUST...]	localIP	LLMNR	LLMNR UDP 5355	SVCHOST SVCHOST.EXE		Outbound
4	Network Discovery (SSDP)	Adapter [TRUST...]	Any	SSDP	SSDP TCP 2869 ...	SVCHOST.EXE, WMPNETW...		Outbound
Core Network (14)								
Core IPv6 Tunnel (2)								
File and Printer Sharing (5)								
LOCAL (1)								
26	Internet		localIP	Any	WEB TCP 3128 ...	Any		

Edit... New... Delete Copy Paste Up Down Select Overlapping...

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 avoid configuration 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 CloudGen 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 File menu, and select **Save Configuration**.

Figures

1. pfw_settings_50.png
2. fw_rule_list_50.png

© Barracuda Networks Inc., 2024 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.