How to Configure Personal Firewall Rules on the CloudGen Firewall

https://campus.barracuda.com/doc/75696500/

To configure personal firewall rules if no Personal Firewall ruleset is present on the Bararcuda CloudGen Firewall, you must first create a new ruleset or import one that has previously been exported from a Barracuda Network Acess Client. Usually, the configuration of the Barracuda Personal Firewall is made directly at the server. Each rule in a Personal Firewall ruleset is constructed from a variety of configuration entities (**Adapters, Networks, Services, Applications, Users**), which can be created and maintained independently of the ruleset itself. They are then pieced together to build a logical formation.

> Personal Firewall rulesets do not support Revision Control System (RCS).

Create a Ruleset on the Bararcuda CloudGen Firewall

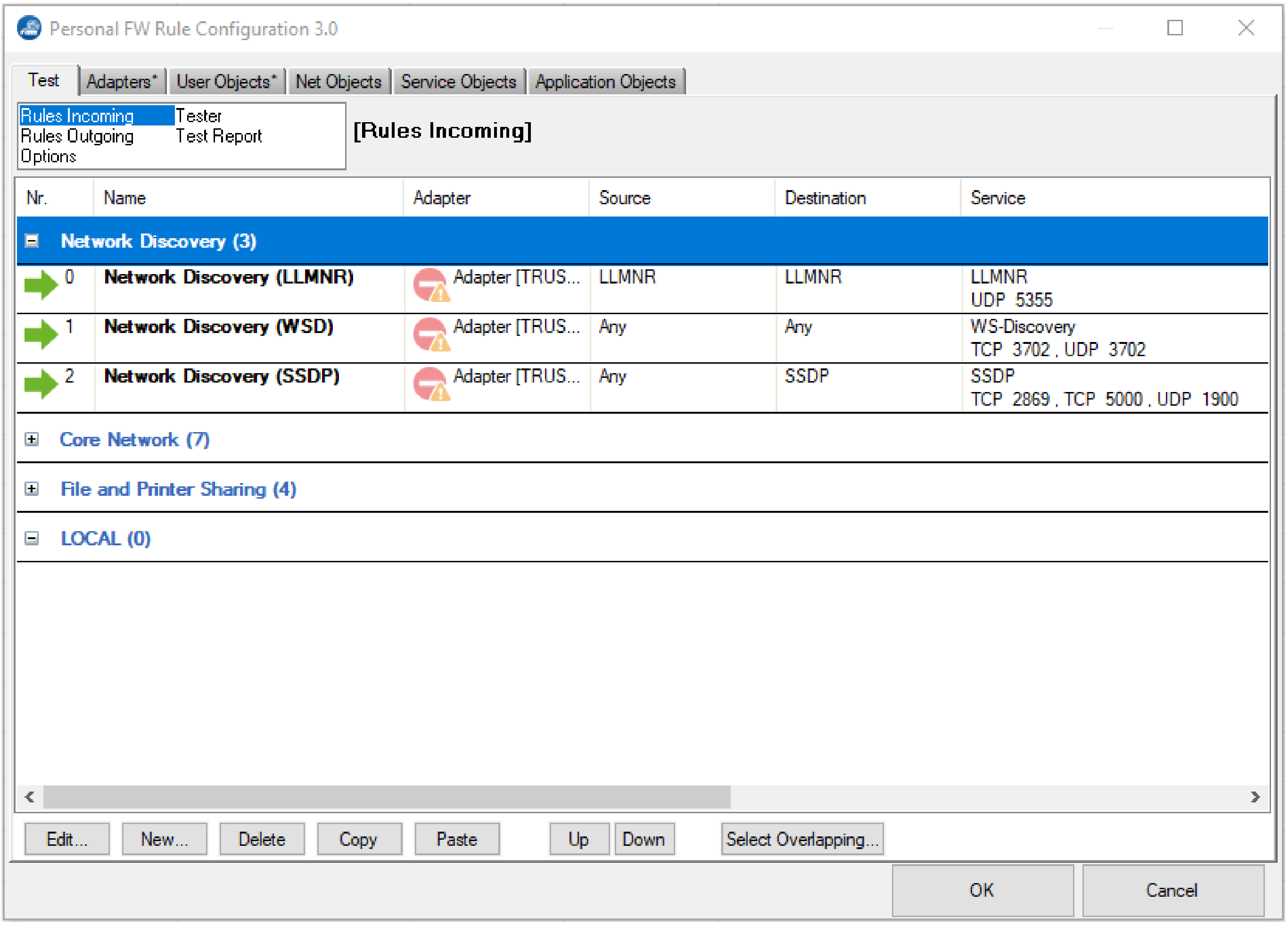
1. In Barracuda Firewall Admin, navigate to **CONFIGURATION > Configuration Tree > Box > Virtual Servers >** ***your virtual server*** **> Assigned Services > VPN-Service > Client to Site**.
2. Open the **VPN FW** tab.
3. Click **Lock**.
4. To create a new ruleset:
    1. Right-click in the empty table space, and select **New VPN Firewall Rule Set**.
    2. Enter a descriptive name for the ruleset, select the **Client Release**, and click **OK**.

   To import an existing new ruleset:
    1. Right-click in the empty table space, and select **Import from Personal Firewall**.
    2. Select the ruleset file and finalize the importing.
    3. Double-click the appropriate VPN firewall ruleset to open the **Personal FW Rule Configuration** window.
5. In the **Personal FW Rule Configuration** window, use the tabs to configure your rules as described in the sections below.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

The Personal FW Rule Configuration Window

The **Personal FW Rule Configuration** window provides all functionalities for creating and testing Personal Firewall rules and for configuring Personal Firewall settings. The configuration area is divided into the following tabs:

- The **Test** tab allows for manual rule configuration, testing, and configuring. All currently present Personal Firewall rules are listed here.
  - The **Rules Incoming** view shows the rules controlling incoming traffic.
  - The **Rules Outgoing** view shows the rules controlling outgoing traffic.
  - The **Options** view contains settings to control the overall behavior of the Personal Firewall if this ruleset is active.
  - The **Tester** and **Test Report** views allow testing rulesets for consistency. For more information, see How to Test Personal Firewall Rules.
- The **Objects** tabs show all available firewall objects that can be used in Personal Firewall rules and allow you to create new firewall objects. For more information, see Network Objects, Adapter Objects, Service Objects, Application Objects, User Objects.



Nr.	Name	Adapter	Source	Destination	Service
⊟	**Network Discovery (3)**				
0	**Network Discovery (LLMNR)**	Adapter [TRUS...	LLMNR	LLMNR	LLMNR UDP 5355
1	**Network Discovery (WSD)**	Adapter [TRUS...	Any	Any	WS-Discovery TCP 3702 , UDP 3702
2	**Network Discovery (SSDP)**	Adapter [TRUS...	Any	SSDP	SSDP TCP 2869 , TCP 5000 , UDP 1900
⊞	Core Network (7)				
⊞	File and Printer Sharing (4)				
⊟	LOCAL (0)				

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

- **Edit / New** – Opens the rule configuration dialog for the selected rule / allows you to create a new rule.
- **Rule Action** – Allows to select an action for the selected rule(s).

- **Activate / Deactivate Rule** – Activates /Deactivates the selected rule(s).
- **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 incorrect 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 an entry and select **Show** to display the following context menu:

- **Show Source / Destination Addresses** – Displays all source / destination addresses affected by the selected rule.
- **Show Services / Applications / Adapters / Users** – Displays 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.

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.

Configure Personal Firewall Rules

When creating a new personal firewall rule, a minimum specification of the following connection details is mandatory in the following sections:

- **Source / Destination / Service** or
- **Adapter / Source / Service** or
- **Adapter / Destination / Service**

Step 1. Create a New Rule Object

1. Double-click the appropriate VPN firewall ruleset.
2. Select the option that applies to the rules you want to configure. For example: **Rules Outgoing**.

3. Select **New** from the context menu or in the bottom bar.
4. Select **Pass** to enable a connection request, or select **Block** to prevent it.
5. Enter a descriptive name for the rule.
6. For easier identification, insert a rule description (optional).
7. In the **Adapter** section, select an adapter for the connection request. To create a new Adapter object, right-click the **Adapter** window below the list and select **New**. For more information, see Adapter Objects.
8. In the **Source** / **Destination** sections, select a source and destination for the connection request. In the list, all Network objects as defined in the **Networks** window are available. For more information, see Network Objects.
9. In the **Service** section, select a service for the connection request. For more information, see Service Objects.
10. If applicable, select an **Application** and a **User** or group for the connection request. For more information, see Application Objects and User Objects.

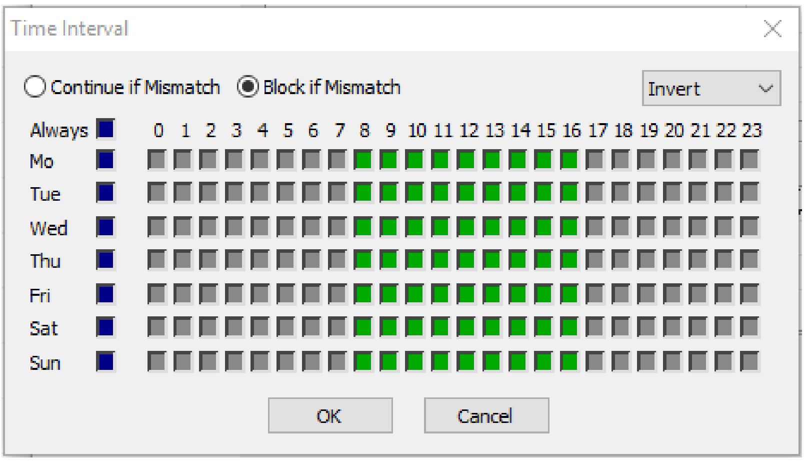
Selecting the check box **IPv6 Company Prefix Match** activates the IPv6 Router Advertisement Guard.

> Modifying an object is a global action. For example, any other rule using the specific object will be affected by the modification. This applies only for referenced objects, not for **explicit** objects. Explicit objects are only available for the current rule.

Step 2. Configure Advanced Rule Settings

Configure the connection details in the **Advanced** view of the **Rule Object** window:

1. In the left menu, expand the **Common** section, and select **Advanced**.
2. In the **Rule Mismatch Policy** section, select one of the following options for each rule part:
   - **Continue on Mismatch** (default) – Process the rule even if the corresponding object does not match the configured setting.
   - **BLOCK on Mismatch** – Do not process the rule if the corresponding object does not match the configured setting.
3. In the **Miscellaneous** section, you can assign a **Time Restriction** for the rule. The granularity is one hour on a weekly base. A rule is allowed at all times by default; for example, all check boxes in the **Time Interval** window are cleared.
   Selecting a check box denies a rule for the given time.
   - Select **Invert** to configure allowed and disallowed time intervals simultaneously.
   - Select **set allow** to clear selected check boxes.
   - Select **set deny** to configure disallowed time intervals.
   - Select **Continue if Mismatch** to process the rule even if the time restriction denies it.
   - Select **Block if Mismatch** (default) to prevent rule processing if the time restriction denies it.



○ Continue if Mismatch ● Block if Mismatch

Invert

Always	■	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mo	■	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨	▨	▨
Tue	■	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨	▨	▨
Wed	■	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨	▨	▨
Thu	■	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨	▨	▨
Fri	■	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨	▨	▨
Sat	■	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨	▨	▨
Sun	■	▨	▨	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨	▨	▨	▨	▨	▨	▨

- Click **OK**.

4. In the **Monitor Connections** field, select whether or not connections should be monitored.
5. Click **OK**.

Configure Personal Firewall Options

The **Options** view contains the same setting as the **Settings** window of the Personal Firewall. To specify the overall behavior of the Personal Firewall when a ruleset is active:

1. Double-click the appropriate VPN firewall ruleset to open the **Personal FW Rule Configuration** window.
2. Select **Options**.
3. Configure the settings as described in **Configure Personal Firewall Settings** in How to Configure the Barracuda Personal Firewall.

To save configuration changes made on the Barracuda CloudGen Firewall, click **Send Changes** and **Activate**. 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