Firewall Rule List Interface and Icons

https://campus.barracuda.com/doc/46209171/

The features and controls of the configuration pages for the Host and Forwarding Firewall rulesets have a similar interface structure. The main rules section in these pages displays the access or application rules depending on the selected ruleset in the left menu. You can view, create, copy, paste, clone, and edit your access rules on this page.

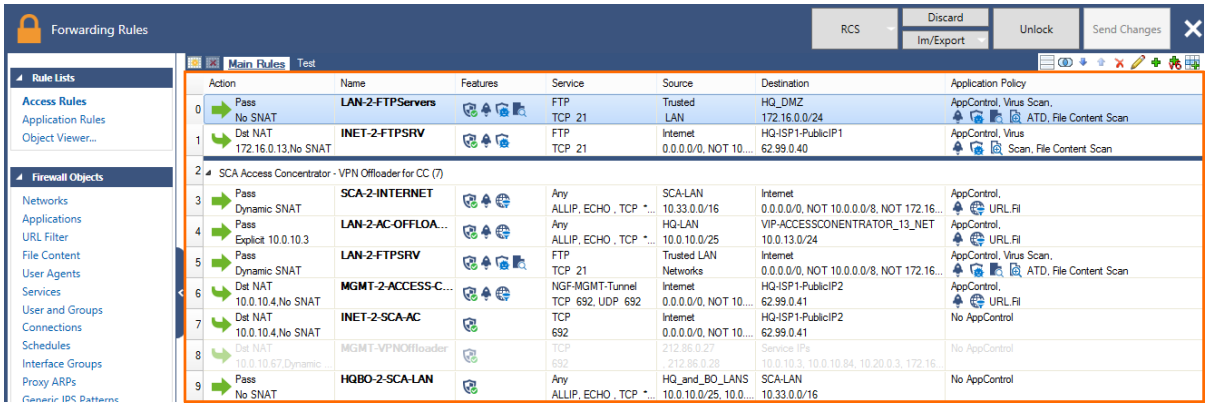
In this article:

The Forwarding Firewall Ruleset

The Forwarding Firewall ruleset contains all forwarding access and application rules and provides access to the access and application rule configuration dialog. To open the Forwarding Firewall ruleset, go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.

The **Forwarding Rules** page is divided into the following sections:

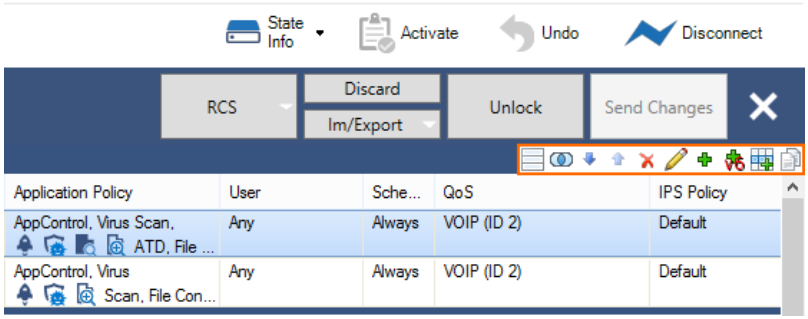
Main Rule Table



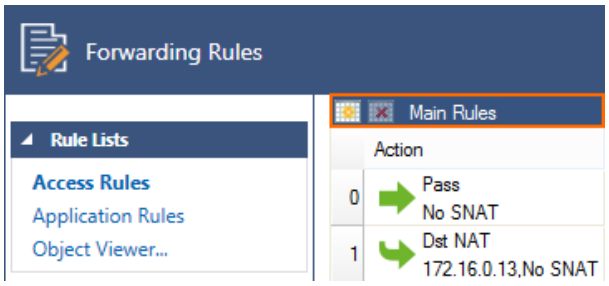
In the main rules table, you can view and edit the settings for your access or application rules. See below for icon descriptions.

Editing Features

Use these icons to create, edit, and otherwise manipulate the access or application rules in the main ruleset. See below for icon descriptions.



Rule Lists



This ruleset cannot be deleted, although additional rulesets can be created. See below for icon descriptions.

Main Rules Section and Icons

In the main rules table, the settings for each access rule are organized in the following columns:

Column	Description
Action	The action performed by the access rule.
Name	The name of the access rule.

<table>
<tr><td rowspan="25">Features</td><td colspan="2">The features that have been applied to the access rule, as indicated by the following icons:</td></tr>
<tr><td>Icon</td><td>Feature</td></tr>
<tr><td></td><td>Dynamic Rule</td></tr>
<tr><td></td><td>Advanced rule parameter changed</td></tr>
<tr><td></td><td>Rule matches for swapped source and destination</td></tr>
<tr><td></td><td>Scheduled Rule</td></tr>
<tr><td></td><td>Generic TCP Proxy</td></tr>
<tr><td></td><td>No Source NAT</td></tr>
<tr><td></td><td>Authenticated User</td></tr>
<tr><td></td><td>No IPS</td></tr>
<tr><td></td><td>Custom IPS Policy</td></tr>
<tr><td></td><td>Default IPS Policy</td></tr>
<tr><td></td><td>Legacy Layer 7 Application Control</td></tr>
<tr><td></td><td>Continue on Device Mismatch</td></tr>
<tr><td></td><td>Proxy ARP</td></tr>
<tr><td></td><td>No Application Control Scan</td></tr>
<tr><td></td><td>Application Control Scan without SSL Interception</td></tr>
<tr><td></td><td>Application Control Scan with SSL Interception</td></tr>
<tr><td></td><td>AV scan</td></tr>
<tr><td colspan="2">The following icons apply to application rules only:</td></tr>
<tr><td>Icon</td><td>Feature</td></tr>
<tr><td></td><td>Application Filter Object</td></tr>
<tr><td></td><td>Application Object</td></tr>
<tr><td></td><td>Custom Application</td></tr>
<tr><td></td><td>Overridden Application</td></tr>
<tr><td></td><td>Native Application</td></tr>
<tr><td>Service</td><td colspan="2">The service that applies to the access rule. For example, the IP protocol used or, with TCP/UDP, the relevant IP protocol and the port for the traffic.</td></tr>
<tr><td>Source</td><td colspan="2">The source addresses selected for the access rule.</td></tr>
<tr><td>Destination</td><td colspan="2">The destination addresses selected for the access rule.</td></tr>
<tr><td>Application Policy</td><td colspan="2">The application policies applied to the access rule. For more information, see Application Control.</td></tr>
<tr><td>User</td><td colspan="2">The users affected by the access rule.</td></tr>
<tr><td>Schedule</td><td colspan="2">Displays the times when the rule is applied.</td></tr>
</table>

QoS	Any traffic shaping settings. For more information, see How to Create and Apply QoS Bands.
IPS Policy	The IPS policy that is applied to the access rule. For more information, see Intrusion Prevention System (IPS).
Usage	This column shows when the rule was last used and how often. E.g.: 5 days (1234) – The rule matched certain traffic 5 days ago and matched 1234 times total. The **Usage** field is only filled with information in the read-only version of the ruleset. Go to **FIREWALL > Forwarding Rules**.

Main Rules Tab

The **Main Rules** tab section allows you to create additional rule lists.

Editing Features and Icons

The editing features section on the top right of the page provides the following hot keys that let you perform different actions:

Hot-key	Description
	Show/hide inactive rules
	Show/select overlapping rules
	Move a rule down in the ruleset
	Move a rule up in the ruleset
	Delete a rule
	Edit a rule
	Add a new rule
	Add a new IPv6 rule
	Insert a new rule section
	Clone a rule

For more information on the functionalities of the Forwarding Firewall ruleset, see Forwarding Firewall.

Host Access Ruleset

The host access ruleset contains default rules that fit most applications and services that are handled by the Barracuda NextGen Firewall F-Series. Changing the host access ruleset should only be done by an expert administrator because changes can affect the behavior of your system. For help with changing default host access rules, contact Barracuda Networks Technical

Support.

You can view the host access ruleset on the **Host Firewall - Rules** page. To open this page, go to **Config > Box > Infrastructure Services > Host access rules**.

The **Host Firewall - Rules** page provides an interface very similar to the Forwarding Firewall and is divided into the following sections:

- **Configuration Menu** – The left navigation pane of the page provides you with menu sections to configure your access rules.
- **Inbound and Outbound Table** – In the table, you can view and edit the settings for all inbound and outbound host access rules. To switch between viewing the inbound and outbound rulesets, click the following tabs:
  - **Inbound** – Shows all inbound Host access rules.
  - **Inbound-User** – (Bound to the Inbound set) Shows a subset of inbound Host access rules.
  - **Outbound** – Shows all outbound Host access rules.
  - **Outbound-User** tab – (Bound to the Outbound set) Shows a subset of outbound Host access rules.

Main Rules Section and Icons

Below the **Inbound** and **Outbound** tabs, the settings for each access rule are organized into the following columns:

<table>
<tr><th>Column</th><th colspan="2">Description</th></tr>
<tr><td>Action</td><td colspan="2">The action performed by the access rule</td></tr>
<tr><td>Name</td><td colspan="2">The name of the access rule</td></tr>
<tr><td rowspan="4">Features</td><td colspan="2">The features that have been applied to the access rule, as indicated by the following icons:</td></tr>
<tr><td>Icon</td><td>Description</td></tr>
<tr><td></td><td>No IPS</td></tr>
<tr><td></td><td>No Source NAT</td></tr>
<tr><td></td><td>Legacy Layer 7 Application Control</td></tr>
<tr><td>Service</td><td colspan="2">The service that applies to the access rule</td></tr>
<tr><td>Source</td><td colspan="2">The source selected for the access rule</td></tr>
<tr><td>Destination</td><td colspan="2">The destination selected for the access rule</td></tr>
<tr><td>Comment</td><td colspan="2">(Optional) Comment</td></tr>
<tr><td>User</td><td colspan="2">The users affected by the access rule</td></tr>
<tr><td>QoS</td><td colspan="2">Any traffic shaping settings. For more information, see How to Create and Apply QoS Bands.</td></tr>
</table>

Schedule	Displays the times when the rule is applied.
Usage	This column shows when the rule was last used and how often. E.g.: 5 days (1234) – The rule matched certain traffic 5 days ago and matched 1234 times total. The **Usage** field is only filled with information in the read-only version of the ruleset. Go to **FIREWALL > Host Rules**.

For more information on the functionalities of the host access ruleset, see Host Firewall.

Figures

1. FW_main_rule_area.png
2. FW_edit_icon_bar.png
3. FW_rule_lists.png
4. dyn.png
5. param.png
6. swap.png
7. time.png
8. ico_tcp.png
9. ico_nsnat.png
10. user.png
11. noips.png
12. ips.png
13. defips.png
14. leg_app.png
15. cont.png
16. parp.png
17. noscan.png
18. native.png
19. ssl.png
20. av.png
21. filter.png
22. app.png
23. custom.png
24. over.png
25. native.png
26. hk1.png
27. hk2.png
28. hk3.png
29. hk4.png
30. hk5.png
31. hk6.png
32. hk7.png
33. hk8.png
34. hk9.png
35. hk10.png
36. noips.png
37. ico_nsnat.png
38. leg_app.png