Firewall Rule List Interface and Icons

https://campus.barracuda.com/doc/48202891/

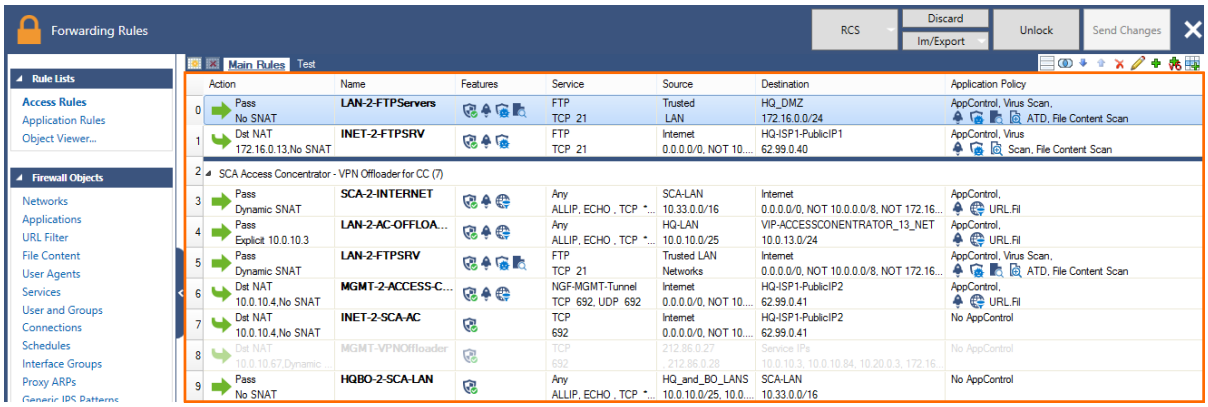
The features and controls of the configuration pages for the Host and Forwarding Firewall rulesets have a similar interface structure. The main rules section in these pages displays the access or application rules, depending on the selected ruleset in the left menu. You can view, create, copy, paste,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

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:

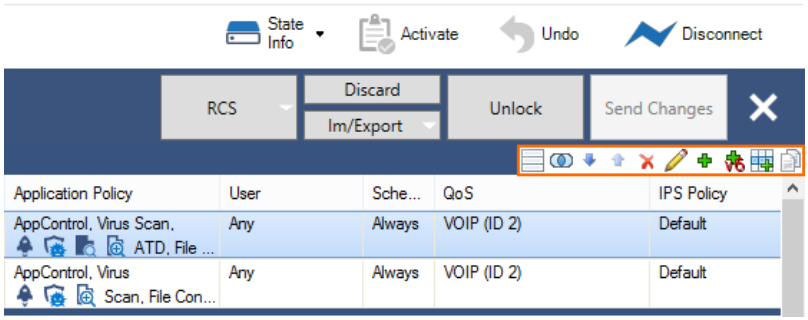
Main rules table



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="30">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 allows you to create additional rule lists.

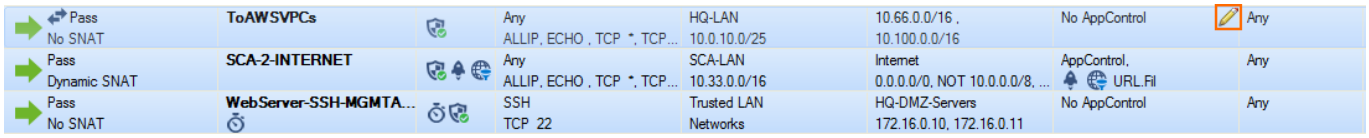
Editing features and icons

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

Shortcuts	Description
	Modify view
	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

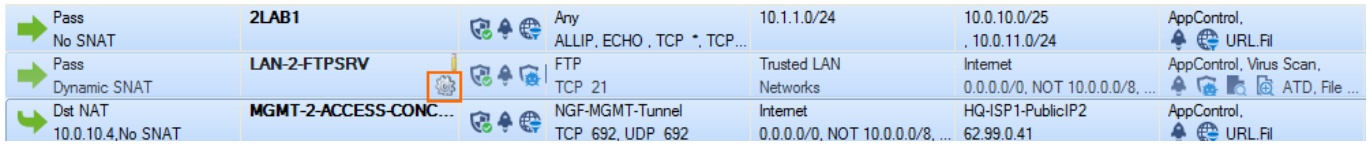
Editing multiple access rules

If you need to change the Application Control, IPS, or QoS settings for multiple access rules, you can use inline edit multiple access rules. Hold down the CTRL key and click the rules you want to edit. The following settings can be changed for all selected access rules by clicking the mouse-over edit icon ():



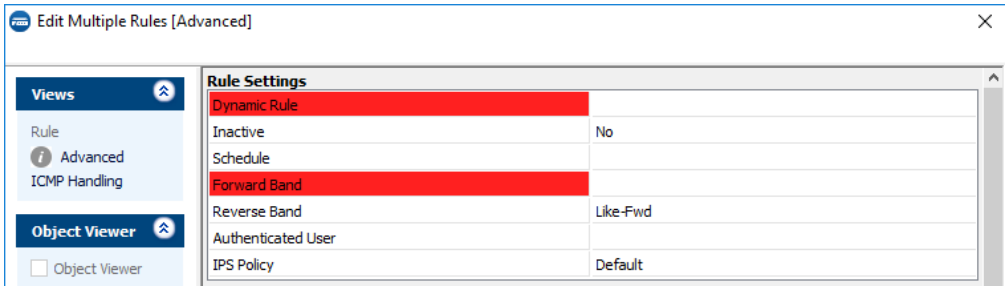
- **Application Control**
- **IPS Policy**
- **QoS**

To change the following properties via multi-edit, click the mouse-over ( ) settings icon in the **Name** column:



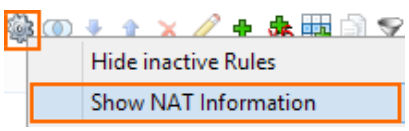
- **Set color**
- **Deactivate or activate rules**
- **Dynamic rule**

To change **Advanced** settings for multiple rules, right-click the selected rules and click **Edit**. Entries highlighted in red differ between the selected rules.



NAT Information

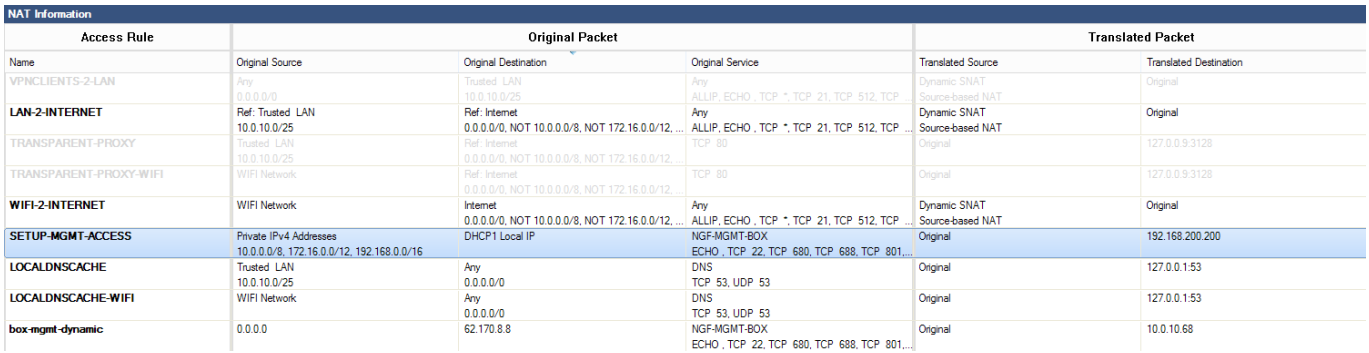
Use the NAT Information view to display the access rules based on translated IP addresses. To access the NAT view, expand the 'modify view' icon and select **Show NAT information**.



The **NAT Information** window displays the following details:

- **Access Rule** – This column lists all access rules with a connection method of source or destination NAT. To display or edit a rule from the NAT view, double-click it.

- **Original Packet** – The columns in this section display the original source, destination, and service object that apply to the access rule.
- **Translated Packet** – The columns in this section display the selected NAT method. This can be source NAT or destination NAT. This section also shows whether source or destination is translated and displays the translated IP address.



NAT Information

Access Rule	Original Packet			Translated Packet	
Name	Original Source	Original Destination	Original Service	Translated Source	Translated Destination
VPNCLIENTS-2-LAN	Any 0.0.0.0/0	Trusted LAN 10.0.10.0/25	Any ALLIP, ECHO , TCP *, TCP 21, TCP 512, TCP ...	Dynamic SNAT Source-based NAT	Original
LAN-2-INTERNET	Ref: Trusted LAN 10.0.10.0/25	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16.0.0/12, ...	Any ALLIP, ECHO , TCP *, TCP 21, TCP 512, TCP ...	Dynamic SNAT Source-based NAT	Original
TRANSPARENT-PROXY	Trusted LAN 10.0.10.0/25	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16.0.0/12,	TCP 80	Original	127.0.0.9:3128
TRANSPARENT-PROXY-WIFI	WIFI Network	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16.0.0/12,	TCP 80	Original	127.0.0.9:3128
WIFI-2-INTERNET	WIFI Network	Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16.0.0/12, ...	Any ALLIP, ECHO , TCP *, TCP 21, TCP 512, TCP ...	Dynamic SNAT Source-based NAT	Original
SETUP-MGMT-ACCESS	Private IPv4 Addresses 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	DHCP1 Local IP	NGF-MGMT-BOX ECHO , TCP 22, TCP 680, TCP 688, TCP 801,...	Original	192.168.200.200
LOCALDNSCACHE	Trusted LAN 10.0.10.0/25	Any 0.0.0.0/0	DNS TCP 53, UDP 53	Original	127.0.0.1:53
LOCALDNSCACHE-WIFI	WIFI Network	Any 0.0.0.0/0	DNS TCP 53, UDP 53	Original	127.0.0.1:53
box-mgmt-dynamic	0.0.0.0	62.170.8.8	NGF-MGMT-BOX ECHO , TCP 22, TCP 680, TCP 688, TCP 801,...	Original	10.0.10.68

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 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:

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

Allowed characters in the firewall ruleset

All text configuration elements in the firewall ruleset are restricted to using only the following characters, number, and symbols:

- **Letters** - a-z, A-Z
- **Numbers** – 0-9
- **Symbols** – # \r \n . _ / : , ; * + -

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. hk0.png
27. hk1.png
28. hk2.png
29. hk3.png
30. hk4.png
31. hk5.png
32. hk6.png
33. hk7.png
34. hk8.png
35. hk9.png
36. hk10.png
37. hk6.png
38. multi-edit-appctrl.png
39. hk0.png
40. multi-edit-name.png
41. multi-edit-advanced.png
42. FW_nat_view01.png
43. FW_nat_view02.png
44. noips.png

45. ico_nsnat.png
46. leg_app.png