

## Firewall Rule List Interface and Icons

<https://campus.barracuda.com/doc/73719541/>

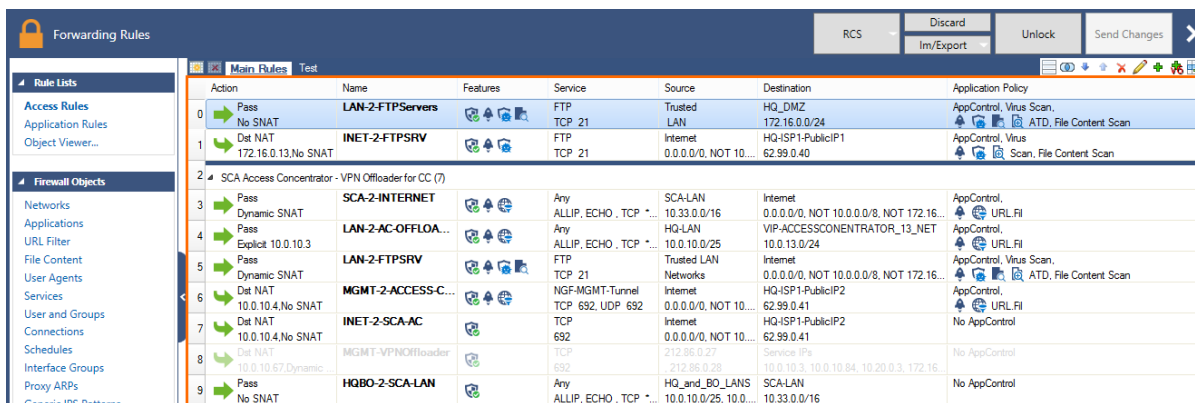
The features and controls of the configuration pages for the Host and Forwarding Firewall rulesets have a similar interface structure. The main rules section in these pages displays the access or application rules depending on the selected ruleset in the left menu. You can view, create, copy, paste,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

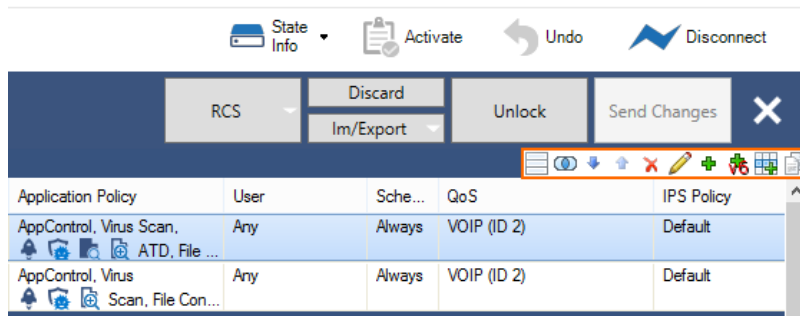


Action	Name	Features	Service	Source	Destination	Application Policy
Pass No SNAT	LAN-2-FTPServers		FTP	Trusted LAN	HQ_DMZ 172.16.0.0/24	AppControl, Virus Scan, ATD, File Content Scan
Dist NAT 172.16.0.13, No SNAT	INET-2-FTPSRV		TCP 21	Internet 0.0.0.0/0, NOT 10...	HQ-ISP1-PublicIP1 62.99.0.40	AppControl, Virus Scan, File Content Scan
Pass Dynamic SNAT	SCA-2-INTERNET		Any	SCA-LAN 10.33.0.0/16	Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16...	AppControl, URL Fil
Pass Explicit 10.0.10.3	LAN-2-AC-OFFLOA...		Any	HQ-LAN 10.0.10.0/25	VIP-ACCESSCONCENTRATOR_13_NET 10.0.13.0/24	AppControl, URL Fil
Pass Dynamic SNAT	LAN-2-FTPSRV		FTP	Trusted LAN	Internet	AppControl, Virus Scan, ATD, File Content Scan
Dist NAT 10.0.10.4, No SNAT	MGMT-2-ACCESS-C...		NGF-MGMT-Tunnel	Internet	HQ-ISP1-PublicIP2 62.99.0.41	AppControl, URL Fil
Dist NAT 10.0.10.4, No SNAT	INET-2-SCA-AC		TCP	Internet 0.0.0.0/0, NOT 10...	HQ-ISP1-PublicIP2 62.99.0.41	No AppControl
Dist NAT 10.0.10.67, Dynamic	MGMT-VPNOffloader		TCP	212.85.0.23 692	Service-IPs 10.0.10.3, 10.0.10.84, 10.20.0.3, 172.16...	No AppControl
Pass No SNAT	HQBO-2-SCA-LAN		Any	HQ_and_BO_LANS 10.0.10.0/25, 10.0...	SCA-LAN 10.33.0.0/16	No AppControl

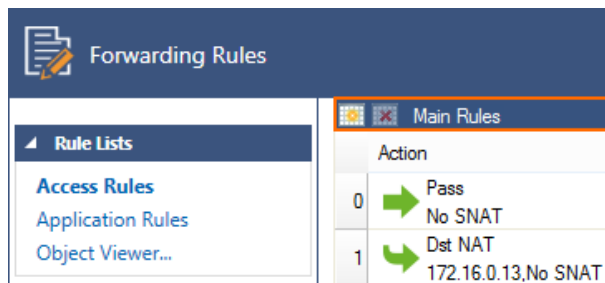
In the main rules table, you can view and edit the settings for your access or application rules. See below for icon descriptions.

#### 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
<b>Action</b>	The action performed by the access rule.
<b>Name</b>	The name of the access rule.

<b>Features</b>	The features that have been applied to the access rule, as indicated by the following icons:	
	<b>Icon</b>	<b>Feature</b>
		Dynamic Rule
		Advanced rule parameter changed
		Rule matches for swapped source and destination
		Scheduled Rule
		Generic TCP Proxy
		Original Source IP
		Authenticated User
		No IPS
		Custom IPS Policy
		Default IPS Policy
		Legacy Layer 7 Application Control
		Continue on Device Mismatch
		Proxy ARP
		No Application Control Scan
		Application Control Scan without SSL Inspection
		Application Control Scan with SSL Inspection
		AV scan
	The following icons apply to application rules only:	
	<b>Icon</b>	<b>Feature</b>
	Application Filter Object	
	Application Object	
	Custom Application	
	Overridden Application	
	Native Application	
<b>Service</b>	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.	
<b>Source</b>	The source addresses selected for the access rule.	
<b>Destination</b>	The destination addresses selected for the access rule.	
<b>Application Policy</b>	The application policies applied to the access rule. For more information, see <a href="#">Application Control</a> .	
<b>User</b>	The users affected by the access rule.	
<b>Schedule</b>	Displays the times when the rule is applied.	












<b>QoS</b>	Any <a href="#">traffic shaping</a> settings. For more information, see <a href="#">How to Create and Apply QoS Bands</a> .
<b>IPS Policy</b>	The IPS policy that is applied to the access rule. For more information, see <a href="#">Intrusion Prevention System (IPS)</a> .
<b>Usage</b>	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 <b>Usage</b> field is only filled with information in the read-only version of the ruleset. Go to <b>FIREWALL &gt; Forwarding Rules</b> .

### 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 (



Pass No SNAT	ToAWSVPCs	Any ALLIP, ECHO, TCP *, TCP...	HQ-LAN 10.0.10.0/25	10.66.0.0/16, 10.100.0.0/16	No AppControl	Any
Pass Dynamic SNAT	SCA-2-INTERNET	Any ALLIP, ECHO, TCP *, TCP...	SCA-LAN 10.33.0.0/16	Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...	AppControl, URL Fil	Any
Pass No SNAT	WebServer-SSH-MGMTA...	SSH TCP 22	Trusted LAN Networks	HQ-DMZ-Servers 172.16.0.10, 172.16.0.11	No AppControl	Any

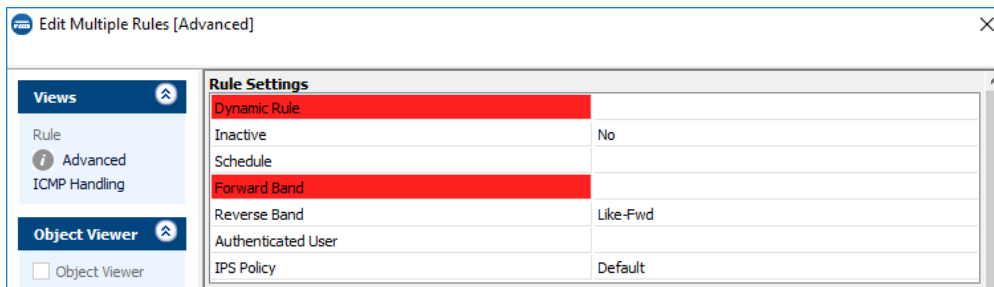
- **Application Control**
- **IPS Policy**
- **QoS**

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

Pass No SNAT	2LAB1	Any ALLIP, ECHO, TCP *, TCP...	10.1.1.0/24	10.0.10.0/25, 10.0.11.0/24	AppControl, URL Fil
Pass Dynamic SNAT	LAN-2-FTPSRV	FTP TCP 21	Trusted LAN Networks	Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...	AppControl, Virus Scan, ATD, File ...
Dest NAT 10.0.10.4.No SNAT	MGMT-2-ACCESS-CONC...	NGF-MGMT-Tunnel TCP 692, UDP 692	Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...	HQ-ISP1-PublicIP2 62.99.0.41	AppControl, URL Fil

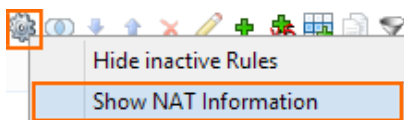
- **Set color**
- **Deactivate or activate rules**
- **dynamic rule**

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 that are handled by the Barracuda CloudGen Firewall. 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	
<b>Action</b>	The action performed by the access rule	
<b>Name</b>	The name of the access rule	
<b>Features</b>	The features that have been applied to the access rule, as indicated by the following icons:	
	<b>Icon</b>	<b>Description</b>
		No IPS
		Original Source IP
		Legacy Layer 7 Application Control
<b>Service</b>	The service that applies to the access rule	
<b>Source</b>	The source selected for the access rule	
<b>Destination</b>	The destination selected for the access rule	
<b>Comment</b>	(Optional) Comment	
<b>User</b>	The users affected by the access rule	
<b>QoS</b>	Any <a href="#">traffic shaping</a> settings. For more information, see <a href="#">How to Create and Apply QoS Bands</a> .	
<b>Schedule</b>	Displays the times when the rule is applied.	
<b>Usage</b>	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 <b>Usage</b> field is only filled with information in the read-only version of the ruleset. Go to <b>FIREWALL &gt; Host Rules</b> .	

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 use 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

© Barracuda Networks Inc., 2019 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.