

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:

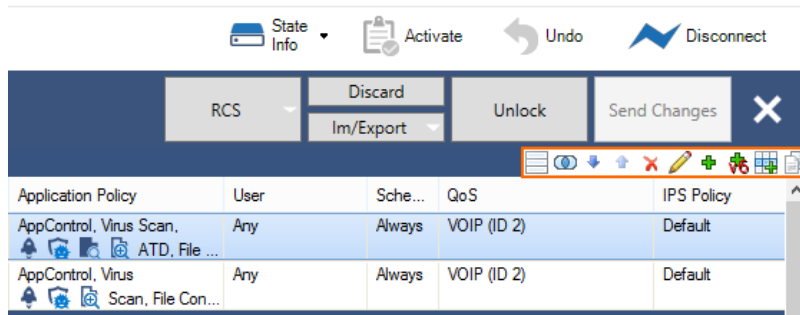
Main Rule Table

Action	Name	Features	Service	Source	Destination	Application Policy
0 Pass No SNAT	LAN-2-FTPServers		FTP TCP 21	Trusted LAN	HQ_DMZ 172.16.0.0/24	AppControl, Virus Scan, ATD, File Content Scan
1 Det NAT 172.16.0.13.No SNAT	INET-2-FTPSRV		FTP TCP 21	Internet 0.0.0.0/0, NOT 10...	HQ-ISP1-PublicIP1 62.99.0.40	AppControl, Virus Scan, File Content Scan
2 SCA Access Concentrator - VPN Offloader for CC (7)						
3 Pass Dynamic SNAT	SCA-2-INTERNET		Any ALLIP, ECHO, TCP ...	SCA-LAN 10.33.0.0/16	Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16...	AppControl, URL_Fi
4 Pass Explicit 10.0.10.3	LAN-2-AC-OFFLOA...		Any ALLIP, ECHO, TCP ...	HQ-LAN 10.0.10.0/25	VIP-ACCESSCONCENTRATOR_13_NET 10.0.13.0/24	AppControl, URL_Fi
5 Pass Dynamic SNAT	LAN-2-FTPSRV		FTP TCP 21	Trusted LAN Networks	Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16...	AppControl, Virus Scan, ATD, File Content Scan
6 Det NAT 10.0.10.4.No SNAT	MGMT-2-ACCESS-C...		NGF-MGMT-Tunnel TCP 692, UDP 692	Internet 0.0.0.0/0, NOT 10...	HQ-ISP1-PublicIP2 62.99.0.41	AppControl, URL_Fi
7 Det NAT 10.0.10.4.No SNAT	INET-2-SCA-AC		TCP 692	Internet 0.0.0.0/0, NOT 10...	HQ-ISP1-PublicIP2 62.99.0.41	No AppControl
8 Det NAT 10.0.10.67.Dynamic	MGMT-VPNOFFloader		TCP 692	212.86.0.27 .212.86.0.28	Service IPs 10.0.10.3, 10.0.10.84, 10.20.0.3, 172.16...	No AppControl
9 Pass No SNAT	HQBO-2-SCA-LAN		Any ALLIP, ECHO, TCP ...	HQ_and_BO_LANS 10.0.10.0/25, 10.0...	SCA-LAN 10.33.0.0/16	No AppControl

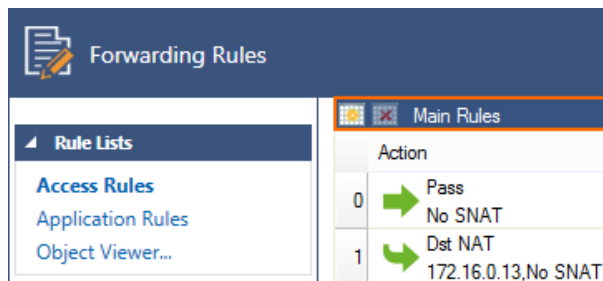
In the main rules table, you can view and edit the settings for your access or application rules. See below for icon descriptions.

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
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	Feature
		Dynamic Rule
		Advanced rule parameter changed
		Rule matches for swapped source and destination
		Scheduled Rule
		Generic TCP Proxy
		No Source NAT
		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 Interception
		Application Control Scan with SSL Interception
		AV scan
	The following icons apply to application rules only:	
	Icon	Feature
		Application Filter Object
		Application Object
	Custom Application	
	Overridden Application	
	Native Application	
Service	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.	
Source	The source addresses selected for the access rule.	
Destination	The destination addresses selected for the access rule.	
Application Policy	The application policies applied to the access rule. For more information, see Application Control .	
User	The users affected by the access rule.	
Schedule	Displays the times when the rule is applied.	











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:

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:								
	<table border="1"> <thead> <tr> <th>Icon</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>	Icon	Description		No IPS		No Source NAT		Legacy Layer 7 Application Control
	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](#).

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

© 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.