
Firewall Rule List Interface and Icons

<https://campus.barracuda.com/doc/41116359/>

The features and controls of the configuration pages for the Host and Forwarding Firewall rule sets have a similar interface structure. The main rules section in these pages displays access and application rules that are configured for use in your network. You can view, create, and edit your access rules on this page.

In this article:

The Forwarding Firewall Rule Set

The Forwarding Firewall rule set contains all forwarding access and application rules and provides access to the rules configuration. To open the Forwarding Firewall rule set, go to **Config > Full Config > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.

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

- **Main Rules Section** - In the main rules table, you can view and edit the settings for your access or application rules.
- **Configuration Menu** - The left navigation pane on the page provides you with menu sections to configure your access rules.
- **Main Rules Tab** - This section lets you create additional rule lists.
- **Editing Features** - Use these features to edit the rule set.

Editing Features

Main Rules tab - allows creating Rule Lists

State Info | Activate | Undo | Disconnect

Forwarding Firewall - Rules | RCS | Discard | Lock | Send Changes | Im/Export

Action	Name	Features	Service	Source	Destination	Application
3 Access rule required to allow traffic to flow across the firewall during an eval in bridge mode (used by setup wizard) (9)						
4	Pass No SNAT	BO1-2-BO2	Any ALLIP, ECHO, TCP, TCP...	BO1-LAN 10.0.80.0/24	BO2-LAN 10.0.81.0/24	AppContn
5	Pass No SNAT	HQ-2-BO2-VLANS	Any ALLIP, ECHO, TCP, TCP...	HQ-LAN 10.0.10.0/25	192.168.100.0/24 . 192.168.200.0/24	AppContn
6	Pass No SNAT	HQ-2-BO1-2	Any ALLIP, ECHO, TCP, TCP...	HQ-LAN 10.0.10.0/25	Ref: BO1-LAN, Ref: BO2-L...	AppContn
7	Pass Dynamic SNAT	LAN-2-VIPs	Any ALLIP, ECHO, TCP, TCP...	HQ-LAN 10.0.10.0/25	VIP Network 10.0.11.0/25	AppContn
8	Pass No SNAT	HQ-BO2	Any ALLIP, ECHO, TCP, TCP...	HQ-LAN 10.0.10.0/25	BO2-LAN 10.0.81.0/24	AppContn
9	Pass Dynamic SNAT	SSH-HQ-2-SRV	SSH TCP 22	HQ-LAN 10.0.10.0/25	InternetSRV 214.51.2.80	AppContn
10	Pass Dynamic SNAT	HQ-2-SRV-NFS	NFS UDP	Trusted LAN Networks	214.51.2.80	AppContn
11	Pass Dynamic SNAT	HQ-LAN-2-SRV-RPC	PORTMAPPER TCP 111, UDP 111	Trusted LAN Networks	214.51.2.80	AppContn
12	Pass No SNAT	EVAL-MODE-BRIDGE	Any ALLIP, ECHO, TCP, TCP...	Eval Mode Bridged Ports 0.0.0.0/0 dev MGMT, 0.0.0...	Eval Mode Bridged Ports 0.0.0.0/0 dev MGMT, 0.0.0...	AppContn
13 Access rule required to enable access to preconfigured Management IP via a dynamically assigned DHCP-IP (3)						
17 Access Rules that redirect web traffic to the transparent Web Proxy (3)						
21 Access Rules that control traffic flows between the LAN (Trusted LAN), Internet, VPN Clients and remote Sites (8)						
22	Pass Dynamic SNAT	LAN-2-INTERNET	Any ALLIP, ECHO, TCP, TCP...	HQ-LAN 10.0.10.0/25	Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...	AppContn
23	Pass Dynamic SNAT	WIFI-2-INTERNET	Any ALLIP, ECHO, TCP, TCP...	WIFI Network	Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...	AppContn
24	Pass No SNAT	LAN-2-LAN	Any ALLIP, ECHO, TCP, TCP...	Trusted LAN LAN	Trusted LAN	AppContn

Main Rules section - allows creating and editing Rules























Configuration Menu

- Rule Lists
 - Access Rules
 - Application Rules
 - Object Viewer...
- Firewall Objects
 - Networks
 - Applications
 - URL Filter
 - Services
 - User and Groups
 - Connections
 - Interface Groups
 - Proxy ARPs
 - Generic IPS Patterns
- Rule List Verification
 - Rule Tester
 - Test Report
- Settings
 - Setup...
 - Export...
 - Import...
 - Reload Externals
 - Reload GTI Objects

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 that is 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 Layer7 Application Control
		Continue on Device Mismatch
		Proxy ARP
		No Application Control 2.0 Scan
		Application Control 2.0 Scan without SSL Interception
		Application Control 2.0 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 that have been selected for the access rule.	
Destination	The destination addresses that have been selected for the access rule.	
Application Policy	The application policies that have been applied to the access rule. For more information, see Application Control 2.0 .	
User	The users who are 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) .

Main Rules Tab

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

Editing Features and Icons

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

Hotkey	Description
	Show/hide inactive rules
	Show/select overlapping rules
	Move a rule down in the rule set
	Move a rule up in the rule set
	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 rule set, see [Forwarding Firewall](#).

Host Access Rule Set

The host access rule set contains default rules that fit most applications and services that are handled by the Barracuda NG Firewall. Changing the host access rule set 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 rule set 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 rule sets, 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 that is 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 Layer7 Application Control</td> </tr> </tbody> </table>	Icon	Description		No IPS		No Source NAT		Legacy Layer7 Application Control
	Icon	Description							
		No IPS							
	No Source NAT								
	Legacy Layer7 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 who are 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.								

For more information on the functionalities of the host access rule set, see [Host Firewall](#).

Figures

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