

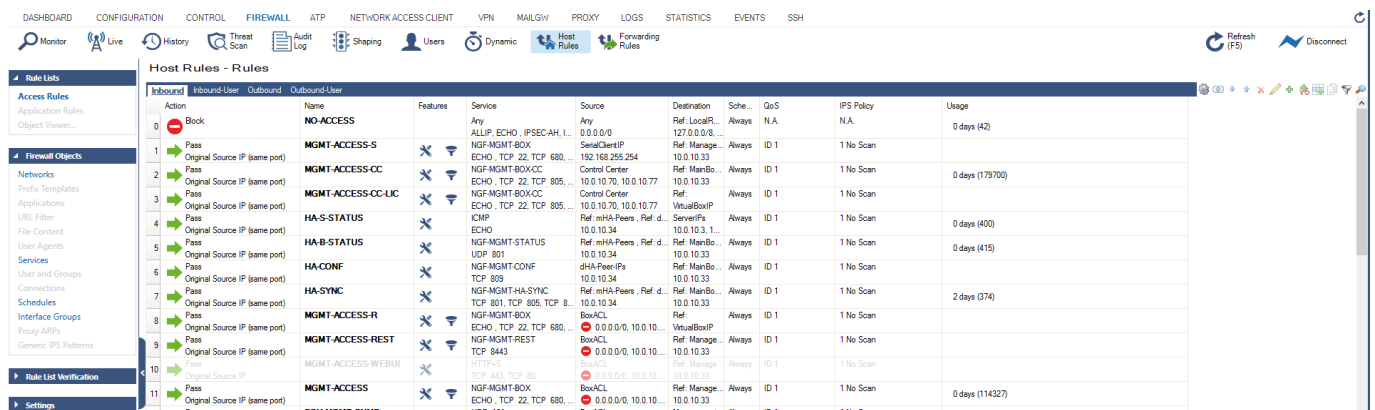
Host and Forwarding Rules Page

<https://campus.barracuda.com/doc/53248623/>

The **Host / Forwarding Rules** pages give you a read-only view of the ruleset. Host and forwarding rules are used to manage traffic going through the Barracuda NextGen Firewall F-Series. To access the **Host / Forwarding Rules** pages, go to the **FIREWALL** tab in the ribbon bar and click **Host Rules** or **Forwarding Rules**.

Host Rules Page

The **FIREWALL > Host Rules** page provides a read-only view of the Host Firewall ruleset together with the configuration menu that is available for Host Firewall rules. Note that all information displayed in this tab is purely informational.



Action	Name	Features	Service	Source	Destination	Sch.	QoS	IPS Policy	Usage
Block	NO-ACCESS		Any	Any	Any	Always	N.A.	N.A.	0 days (42)
Pass	MGMT-ACCESS-S		NGF-MGMT-BOX	SerialClientIP	Ref. Manage...	Always	ID 1	1 No Scan	
Pass	MGMT-ACCESS-CC		NGF-MGMT-BOX	Control Center	Ref. MainBo...	Always	ID 1	1 No Scan	0 days (179700)
Pass	MGMT-ACCESS-CC-LIC		NGF-MGMT-BOX	Control Center	Ref. MainBo...	Always	ID 1	1 No Scan	
Pass	HA-S-STATUS		ICMP	Ref. mHA-Peers...	Ref. d...	Always	ID 1	1 No Scan	0 days (400)
Pass	HA-B-STATUS		NGF-MGMT-STATUS	ECHO	Ref. MainBo...	Always	ID 1	1 No Scan	0 days (415)
Pass	HA-CONF		UDP 801	10.0.10.70, 10.0.10.77	10.0.10.33	Always	ID 1	1 No Scan	
Pass	HA-SYNC		NGF-MGMT-CONF	10.0.10.70, 10.0.10.77	10.0.10.33	Always	ID 1	1 No Scan	2 days (374)
Pass	MGMT-ACCESS-R		NGF-MGMT-CONF	TCP 809	Ref. MainBo...	Always	ID 1	1 No Scan	
Pass	MGMT-ACCESS-REST		NGF-MGMT-REST	BoxACL	Ref. Manage...	Always	ID 1	1 No Scan	
Pass	MGMT-ACCESS-WEBUI		HTTP	BoxACL	Ref. Manage...	Always	ID 1	1 No Scan	
Pass	MGMT-ACCESS		NGF-MGMT-BOX	BoxACL	Ref. Manage...	Always	ID 1	1 No Scan	0 days (114327)
Pass	RDY-MGMT-CONP		HTTP 161	10.0.10.70, 10.0.10.77	10.0.10.33	Always	ID 1	1 No Scan	

To edit and create rules, you must access the **Host Firewall Rules** configuration page. For more information, see [Firewall Rule List Interface and Icons](#).

Forwarding Rules Page

The **FIREWALL > Forwarding Rules** page provides a read-only view of the Forwarding Firewall ruleset together with the configuration menu that is available for Forwarding Firewall rules. Note that all information displayed in this tab is purely informational.

DASHBOARD CONFIGURATION CONTROL **FIREWALL** ATP NETWORK ACCESS CLIENT VPN MAILGW PROXY LOGS STATISTICS EVENTS SSH

Monitor Live History Threat Scan Audit Log Shaping Users Dynamic Host Rules **Forwarding Rules** Refresh (F5) Disconnect

Forwarding Rules - Rules

Action	Name	Features	Service	Source	Destination	Application Policy	User	Sche...	GoS	IPS Policy	Usage
Block	Block-QUIC		QUIC	Trusted LAN	Internet	N.A	Any	Always	N.A.	N.A.	83 days (...)
Block	Block-DNS-Sinkhole-IPv4		Any	Host LAN	DNS Sinkhole - Fake IPv4 IP	N.A.	Any	Always	N.A.	N.A.	
App Redirect	HQ-Offline/Auth		HTTP-S	Trusted LAN	Internet	No AppControl	Any	Always	ID 2	0 Default Policy	27 days (...)
Pass	GUESTLAN-2-INTERNET		Any	Guest Network	Internet	AppControl, URL Fil...	All Authenticated...	Always	ID 2	0 Default Policy	
Dynamic NAT	LAN-2-TicketingAdminInt...		HTTP-S	Trusted LAN	TicketingAdminInterface	No AppControl	Any	Always	ID 2	0 Default Policy	
App Redirect	HQ-Inline/Auth-2-Internet		HTTP-S	Trusted LAN	Internet	No AppControl	All Authenticated...	Always	ID 2	0 Default Policy	0 days (2...)
Dynamic NAT	HQ-2-FAKEINET		HTTP-S	Trusted LAN	Internet	No AppControl	All Authenticated...	Always	ID 2	0 Default Policy	22 days (...)
Pass	HQ-2-FAKEINET		HTTP-S	Trusted LAN	Internet	No AppControl	All Authenticated...	Always	ID 2	0 Default Policy	
Dynamic NAT	HQ-2-FAKEINET		HTTP-S	Trusted LAN	Internet	No AppControl	All Authenticated...	Always	ID 2	0 Default Policy	
Pass	HQ-2-FAKEINET		HTTP-S	Trusted LAN	Internet	No AppControl	All Authenticated...	Always	ID 2	0 Default Policy	
Dat NAT	INET-2-FTPSRV		FTP	Internet	HQ-ISP1-PublicIP1	AppControl, Virus	Any	Always	ID 2	0 Default Policy	
172.16.0.13.Original Sourc...			FTP	Internet	HQ-ISP1-PublicIP1	AppControl, Virus	Any	Always	ID 2	0 Default Policy	
172.16.0.13.Original Sourc...			FTP	Internet	HQ-ISP1-PublicIP1	AppControl, Virus	Any	Always	ID 2	0 Default Policy	
SCA Access Concentrator - VPN Offloader for CC (10)											
Pass	LAB2AWSVPcs		Any	HQ-LAN	AWS_VPC_Networks	No AppControl	Any	Always	No-Shaping	0 Default Policy	89 days (1)
Original Source IP	SCA-2-INTERNET		ALLIP, ECHO, TCP, TCP...	10.0.10.0/25	10.100.0.0/16...	No AppControl	Any	Always	ID 2	0 Default Policy	
Pass	SCA-2-INTERNET		ALLIP, ECHO, TCP, TCP...	10.0.10.0/25	10.100.0.0/16...	No AppControl	Any	Always	ID 2	0 Default Policy	
Dynamic NAT	WebServer-SSH-MGMTA...		SSH	Trusted LAN Networks	HQ-DMZ Servers	AppControl, URL Fil...	Any	Always	ID 2	0 Default Policy	
Original Source IP	LAN-2-AC-OFFLOADER...		TCP	10.0.10.0/25	172.16.0.10, 172.16.0.11	No AppControl	Any	Always	ID 2	0 Default Policy	
Pass	LAN-2-AC-OFFLOADER...		Any	HQ-LAN	VIP-ACCESSCONTRAT...	AppControl	Any	Always	ID 2	0 Default Policy	

To edit and create rules, you must access the **Forwarding Rules** configuration page. For more information, see [Firewall Rule List Interface and Icons](#).

Figures

1. h_rules.png
2. f_rules.png

© Barracuda Networks Inc., 2021 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.