

Default Host Firewall Rules

<https://campus.barracuda.com/doc/96026327/>

The Host Firewall rule set contains default rules that fit most applications and services that are handled by the Barracuda CloudGen Firewall. The following tables list all Host Firewall rules that are preconfigured.

Default Host Rules of the Barracuda CloudGen Firewall

The default Host Firewall rule set of the Barracuda CloudGen Firewall is divided into the following tabs:

- **Inbound** – Displays all inbound Host Firewall rules.
- **Inbound-User** – (Bound to the **Inbound** set) Shows a subset of inbound Host Firewall rules.
- **Outbound** – Displays all outbound Host Firewall rules.
- **Outbound-User** tab – (Bound to the **Outbound** set) Shows an subset of outbound Host Firewall rules.

Host Firewall Rules - Inbound

#	Default State	Name	Comment
0	Enabled	NO-ACCESS	Blocks external access to local IP used for local redirection in forwarding ruleset.
1	Enabled	MGMT-ACCESS-S	Allows management access via serial line, i.e., device=ppp0
2	Enabled	MGMT-ACCESS-CC	Allows management access from the CC IPs.
3	Enabled	MGMT-ACCESS-CC-LIC	Allows management access from the CC IPs.
4	Enabled	HA-S-STATUS	Allows ICMP based HA-probing of server IPs.
5	Enabled	HA-B-STATUS	Allows control-control HA status check communication.
6	Enabled	HA-CONF	Allows configuration sync between HA partners (dedicated HA).
7	Enabled	HA-SYNC	Allows sync of optional services between HA partners.
8	Enabled	MGMT-ACCESS-R	Allows exclusive management access for addresses within the ACL.
9	Enabled	MGMT-ACCESS-REST	Allows exclusive management access for addresses within the ACL.

10	Enabled	MGMT-ACCESS-WEBUI	Allows exclusive management access for addresses within the ACL.
11	Enabled	MGMT-ACCESS	Allows exclusive management access for addresses within the ACL.
12	Enabled	BOX-MGMT-SNMP	Allows exclusive SNMP access for addresses within the ACL.
13	Enabled	LL-IP-TUNNELS	Allows low level IPIP and GRE tunnels between tunnel endpoints.
14	Enabled	OP-SRV-L2TP	Blocks direct external access to the L2TP daemon. L2TP/IPSEC is not affected.
15	Enabled	OP-SRV-VIRSCAN	Allows global access to optional Virus Scanner Service.
16	Enabled	OP-SRV-VPN	Allows global access to optional VPN service incl. PPTP variant.
17	Enabled	OP-SRV-DHCP	Allows global access to optional DHCP server service.
18	Enabled	OP-SRV-DNS	Allows global TCP/UDP access to optional DNS service.
19	Enabled	OP-SRV-OSPF	Allows global access to OSPF for the optional OSPF-RIP-BGP service.
20	Enabled	OP-SRV-RIP	Allows global access to RIP for the optional OSPF-RIP-BGP service.
21	Enabled	OP-SRV-BGP	Allows global access to BGP for the optional OSPF-RIP-BGP service.
22	Enabled	OP-SRV-SIP	Allows global access to optional SIP proxy service.
23	Enabled	OP-SRV-SAPRT	Allows global access to optional SAP-Router gateway service.
24	Enabled	OP-SRV-SNMP	Allows global access to optional SNMP gateway service.
25	Enabled	OP-SRV-PX	Allows global access to optional HTTP/S proxy service.
26	Enabled	OP-SRV-NTP	Allows exclusive access to optional local NTP service from local networks.
27	Enabled	OP-SRV-ICMP	Allows ICMP ECHO requests to Server IPs.
28	Enabled	BOX-ICMP-PING	Allows ICMP ECHO requests local box addresses.
29	Enabled	BOX-PPTP-IN	Allows box communication with ADSL/PPTP modem.
30	Enabled	BOX-DHCP-IN	Allows exclusive access to optional DHCP client service (device=dhcp).
31	Enabled	BOX-AUTH-MSAD-SYNC-IN	Allows access to configured MSAD user authentication sync type servers. Requires installation of DCAgent on specified MSAD servers.

32	Enabled	BOX-AUTH-TSAGENT-SYNC-IN	Allows access to configured TSAGENT sync type servers. Requires installation of TSAGENT on specified terminal servers.
33	Enabled	BOX-AUTH-WIFIAP-SYNC-IN	Allows access to configured Wi-Fi Access Point authentication sync type servers.

The Barracuda Firewall Control Center box provides the following additional default rules:

#	Name	Comment
2	HA-CONF-CC	Allows configuration sync between HA partners (dedicated HA)
6	CC-ACCESS	Allows access to CC services hosted by this box.
10	OP-SRV-CC	Allows for event and status delivery by managed boxes to CC services.
11	OP-SRV-AUDIT	Allows for audit data delivery by managed boxes to CC Audit service.
12	OP-SRV-PKI	Allows access to PKI service hosted by this box.
13	OP-SRV-VPN	Management tunnel (transport) access to CC VPN server.
14	OP-SRV-DNS	Allows for queries of optional local DNS service.
15	OP-SRV-SYSLOG-SSL	Allows for secure and authenticated delivery of syslog from managed boxes via VPN tunnel.
16	OP-SRV-SYSLOG	Allows for secure and authenticated delivery of syslog from managed boxes via VPN tunnel.

Host Firewall Rules - Inbound-User

#	Name	Comment
0	PASSALL	A catch-all rule to warrant free traffic flow. Adapt this to your needs.

Host Firewall Rules - Outbound

#	Default State	Name	Comment
0	Enabled	OP-SRV-CLOUD-NTP	Allows NTP queries for cloud-based boxes.
1	Enabled	BOX-MGMT-CLOUD-CC	Allows traffic from cloud-based boxes to CC.
2	Enabled	NO-ACCESS	Block direct outbound access from unrouted loopback networks.
3	Enabled	HA-B-STATUS	Allows control-control HA status check communication.
4	Enabled	HA-S-STATUS	Allows ICMP based HA-probing of server IPs.
5	Enabled	HA-CONF	Allows configuration sync between HA partners (dedicated HA).

6	Enabled	HA-SYNC	Allows sync of optional services between HA partners.
7	Enabled	LL-IP-TUNNELS	Allows low level IPIP and GRE tunnels between tunnel endpoints.
8	Disabled	BOX-DNS-MGMT-NAT	Routes connections to the static configured DNS-servers via management tunnel. The explicit connection via interface tap3 routes DNS-requests to the static configured DNS-servers through the management tunnel. It is only useful if the box is using remote management to the MC.
9	Enabled	BOX-DNSFWD-OUT	Allows local DNS queries to configured DNS servers and root DNS servers.
10	Enabled	BOX-DNSSLV-OUT	Allows zone transfers initiated by local box DNS secondary server.
11	Enabled	BOX-DNSREC-OUT	Allows recursive local DNS queries.
12	Enabled	BOX-NTP-OUT-T	Allows NTP queries via box management tunnel to CC.
13	Enabled	BOX-NTP-OUT	Allows NTP queries to configured NTP servers.
14	Enabled	OP-SRV-VPN	Allows global access for optional VPN service.
15	Enabled	OP-SRV-DNS	Allows global access for optional DNS service.
16	Enabled	OP-SRV-OSPF	Allows outgoing access for OSPF in an optional dyn. routing service.
17	Enabled	OP-SRV-RIP	Allows outgoing access for RIP in an optional dyn. routing service.
18	Enabled	OP-SRV-BGP	Allows outgoing access for BGP in an optional dyn. routing service.
19	Enabled	BOX-SYSLOG-AUDIT-OUT	Allows delivery of logfiles or audit data to CC.
20	Enabled	BOX-EVENT-OUT	Allows event notification delivery to CC.
21	Enabled	BOX-STATUS-CC	Allows status notification delivery to CC.
22	Enabled	BOX-CONFIG-CC	Allows config update delivery to CC.
23	Enabled	BOX-SYNC-CC	Allows sync to CC.
24	Enabled	BOX-GW-TEST	Allows ICMP gateway probing.
25	Enabled	BOX-MONIP-TEST	Allows ICMP monitoring IP probing.
26	Enabled	BOX-UMTS-TEST	Allows ICMP probing of Wireless WAN gateway and monitoring IPs.

27	Enabled	BOX-xDSL-TEST	Allows ICMP probing of ADSL link gateway and monitoring IPs.
28	Enabled	BOX-ISDN-TEST	Allows ICMP probing of ISDN link gateway and monitoring IPs.
29	Enabled	BOX-DHCP-OUT	Allows broadcasts from local DHCP client service.
30	Enabled	BOX-DHCP-TEST	Allows ICMP probing of DHCP link gateway and monitoring IPs.
31	Enabled	BOX-RAM-TEST	Allows ICMP probing of box management tunnel monitoring IPs incl.
32	Enabled	BOX-RAM-OUT	Allows ICMP probing of box management tunnel gateways (points of entry).
33	Enabled	BOX-PPTP-OUT	Allows box communication with ADSL/PPTP modem.
34	Disabled	BOX-AUTH-MGMT-NAT	Routes connections to the authentication servers via management tunnel. The explicit connection via interface tap3 routes authentication requests to the backend servers through the management tunnel. It is only useful if the box is using remote management to the MC.
35	Enabled	BOX-AUTH-MSAD	Allows access to configured MSAD type authentication servers.
36	Enabled	BOX-AUTH-MSNT	Allows access to configured MSNT type authentication servers.
37	Enabled	BOX-AUTH-RADIUS	Allows access to configured RADIUS type authentication servers.
38	Enabled	BOX-AUTH-LDAP	Allows access to configured LDAP, MSADIR type authentication servers.
39	Enabled	BOX-AUTH-MSAD-SYNC	Allows access to configured MSAD user authentication sync type servers. Requires installation of DCagent on specified MSAD servers.
40	Enabled	BOX-AUTH-RSA	Allows access to configured RSA-SecurID type authentication servers.
41	Enabled	BOX-AUTH-TACACS	Allows access to configured TACACS+ type authentication servers.
42	Enabled	BOX-AUTH-WSG	Allows access to configured Web Security Gateway type authentication servers.
43	Enabled	BOX-BRS-REPORTINGSERVER-MGMT-NAT	Allows access to configured Web Security Gateway type authentication servers.

44	Enabled	BOX-BRS-REPORTINGSERVER	Log streaming to the Barracuda Reporting Server.
----	---------	-------------------------	--

The Barracuda Firewall Control Center box provides the following additional default rules:

#	Name	Comment
5	HA-SYSLOG	Allows for HA sync of optional central syslog service.
7	BOX-DNS-OUT	Allows for DNS requests from local box.
17	OP-SRV-DNS	Allows global access for optional DNS service.
18	OP-SRV-CC	Allows for autonomous CC services access to managed boxes.
19	OP-SRV-CC-R	Allows for autonomous CC services access (license) to managed boxes.

Host Firewall Rules - Inbound/Outbound-User

#	Name	Comment
0	PASSALL	A catch-all rule to warrant free traffic flow. Adapt this to your needs.

© Barracuda Networks Inc., 2024 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.