
Live Page

<https://campus.barracuda.com/doc/48203268/>

Under the **Live** tab, you can view and filter real-time information for the traffic that passes through the Barracuda NextGen Firewall F-Series. You can also manage the traffic sessions. To access the **Live** page, open the **FIREWALL** tab and click the **Live** icon in the ribbon bar.

Video

To get a feel for how to use the **FIREWALL > Live** page in NextGen Admin, watch the following video:



Connection Blocked
Troubleshooting
Barracuda NG Firewall

Viewing Session Details

On the **Live** page, the details for all sessions are listed. You can view additional information for a specific session by double-clicking an entry.

DASHBOARD CONFIGURATION CONTROL **FIREWALL** NAC VPN MAILGW LOGS STATISTICS EVENTS SSH

Monitor Live History Threat Scan ATD Audit Log Trace Shaping Users 19 Sessions

Traffic Selection Forward, Local In, Local Out, IPv4, IPv6 Status Selection Closing, Established, Failing, Pending Idle Time [s] 3

ID	State	IP Pr...	Port	Sou...	Interface	User	Dest...	Output-IF	Appli...	Applic...	QoS	Rule	Bit/s	Total	Idle	TI ID
II...	→	TCP	692	100.2...	eth1		62.99...	eth0				MGMT-Tunnela...	6.3 K	584.2 M	0s	-
I...	→	TCP	5049	10.0...	eth0		10.0...	eth0				BOX-AUTH-MS...	0	682.0	0s	-
III...	→	TCP	807	10.1...	eth0		10.0...	eth0				MGMT-ACCESS	8.3 K	786.2 K	0s	-
I...	→	TCP	680	10.0...	eth0		10.0...	eth0				BOX-SYSLOG-A...	2.5 K	42.1 M	0s	-
III...	→	TCP	692	213.4...	eth1		62.99...	eth0				MGMT-Tunnela...	11.6 K	25.4 M	0s	-
I...	→	TCP	692	52.19...	eth1		62.99...	eth0				MGMT-Tunnela...	6.7 K	23.9 M	0s	-
I...	→	ICMP		10.2...	eth4		10.20...	eth4				OP-SRV-VPN	640	229.8 K	1s	-
I...	→	ICMP		10.0...	eth0		10.0...	eth0				BOX-GW-TEST	608	218.2 K	1s	-
I...	→	ICMP		62.99...	eth1		8.8.8.8	eth1				OP-SRV-VPN	752	270.4 K	1s	-
I...	→	TCP	443	10.0...	eth0	mzoller	64.235	eth1	Cud.. api.cuda...			LAN-2-INTERN...	0	5.9 K	1s	-
I...	→	ICMP		62.99...	eth1		62.99...	eth1				OP-SRV-VPN	640	229.8 K	1s	-
I...	→	ICMP		62.99...	eth1		212.86.					OP-SRV-VPN	408	146.7 K	1s	-
I...	→	ICMP		10.0...	eth0		10.0...	eth0				OP-SRV-VPN	608	238.5 K	1s	-
I...	→	ICMP		10.0...	eth0		10.0...	eth0				OP-SRV-VPN	608	253.8 K	1s	-
I...	→	ICMP		10.0...	eth0		10.0...	eth0				BOX-GW-TEST	624	224.0 K	1s	-
I...	→	ICMP		10.0...	eth0		10.0...	eth0				BOX-GW-TEST	608	218.2 K	1s	-
I...	→	ICMP		194.9...	eth2		194.93.	eth2				OP-SRV-VPN	656	235.5 K	1s	-
I...	→	UDP	801	10.0...	eth0	admi...	10.0...	eth0				LAN-2-AC-OFFL...	0	870.0 K	2s	-
I...	→	TCP	692	212.8...	eth1		62.99...	eth0				MGMT-Tunnela...	0	113.4 M	3s	-

Active 0 Kill Selected << Hide Proc Traffic Bits/Sec

PID	Connections	bps	Heart...	PID	Description
199...	0	0	1	19997	Request Handler
200...	0	0	1	20008	State Handler
200...	0	0	1	20013	Sync Handler
200...	0	0	1	20002	Timer Handler
200...	0	0	1	20048	Invalid Handler











The following information is provided for each session:

Info	Description
ID	The icons indicating the amount of traffic (Low to High...). The number provided is the unique access ID for the connection.
State	The connection status (one-way traffic; connection established (TCP); two-way traffic (all other); connection could not be established; closing connection). The icon next to the status symbol indicates the application policy.
IP Protocol	The protocol that is used. For example, TCP, UDP, or ICMP.
Application Context	The context of the affected application.
Application	The name of the affected application.
Content	The content of the affected application.
Rule	The name of the affected firewall rule.

Type	The origin, as specified by the following abbreviations: <ul style="list-style-type: none"> • LIN - Local In. The incoming traffic on the box firewall. • LOUT - Local Out. The outgoing traffic from the box firewall. • LB - Loopback. The traffic via the loopback interface. • FWD - Forwarding. The outbound traffic via the Forwarding Firewall. • IFWD - Inbound Forwarding. The inbound traffic to the firewall. • PXY - Proxy. The outbound traffic via the proxy. • IPXY - Inbound Proxy. The inbound traffic via the proxy. • TAP - Transparent Application Proxying. The traffic via stream forwarding.
Interface	The affected interface.
Source	The source IP address.
Src. Port	The source port.
Destination	The destination IP address.
Port	The destination port (or internal ICMP ID).
User	The username of the affected user and group.
Bit/s	The bits per second (during the last second).
Idle	Time since the last data transfer.
Total	The total number of bytes that have been transferred over this connection.
In	The total number of bytes that have been transferred over this connection from the source.
Out	The total number of bytes that have been transferred over this connection to the source.
Start	Time since the connection was established.
SNAT	The source NAT address.
DNAT	The destination NAT address.
Output-IF	The outgoing interface.
Policy	The affected policy. For descriptions of the available policies, see the Policy Overview section.
QoS	QoS Band used by this session.
FWD Shape	The forward Traffic Shaping (IN/OUT). The shape connectors for ingress and egress shaping, respectively, in the forward direction. Ingress shaping takes place at the inbound interface. Egress shaping takes place at the outbound interface.
REV Shape	The reverse Traffic Shaping (IN/OUT).
Protocol	The affected protocol.
Status	The status of the connection. For descriptions of the available status types, see Status Overview .
Src. Geo	The geographic source of the active connection.
Dst. Geo	The geographic destination of the active connection.

TI ID	The transport rating setting (Bulk, Quality, or Fallback with IDs 0-7). For more information, see Traffic Shaping .
REV Shape	The shape connectors for ingress and egress shaping, respectively, in the reverse direction. Ingress shaping takes place at the outbound interface. Egress shaping takes place at the inbound interface.
URL Category	Category of the destination URL.

The general status of firewall connections is indicated by the following icons:

Icon	Description
	Transfer Rate
	UDP Session creating, connection not fully established (TCP) / one-way traffic (all other protocols)
	Connection established (TCP) - Two-way traffic (all other protocols)
	UDP session failing
	Session one-sided down
	HA Synced Session
	IPS Scan
	App Scan
	Wan Optimization
	Session State: <i>ACPF Slot Deny</i>

Filter Options

You can filter the list of sessions by traffic type, status, and properties. The following filter settings are provided:

- **Traffic Selection** – From the **Traffic Selection** list, you can select the following options to filter for certain traffic types:
 - **Forward** – Sessions handled by the Forwarding Firewall.
 - **Loopback** – System internal data exchanged by the loopback interface.
 - **Local In** – Incoming sessions handled by the box firewall.
 - **Local Out** – Outgoing sessions handled by the box firewall.
 - **IPv4** – Show IPv4 sessions.
 - **IPv6** – Show IPv6 sessions.
- **Status Selection** – From the **Status Selection** list, you can select the following options to filter for certain traffic statuses:
 - **Closing** – Closing connections.
 - **Established** – Established connections.

- **Failing** - Failed connections.
- **Pending** - Connections that are currently being established.
- **Application** - Shows the detected application.

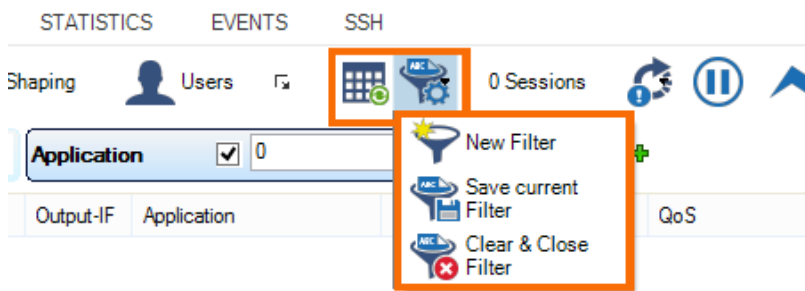
The filter section also allows you to add filters for very specific properties by clicking the + icon.

Note that some fields allow the use of wildcards (*?; !*?). Example: !Amazon* excludes all entries starting with Amazon; Y*|A* includes all entries starting with "Y" or "A".

- **IP Protocol** - Displays the IP protocol.
- **Port** - Displays the port.
- **Source** - The source IP address/range.
- **Source/Destination** - IP address/range that matches either source or destination.
- **Interface** - Displays the interface (for example eth0).
- **User** - Displays the user.
- **Destination** - The destination IP address/range.
- **Output-IF** - The output interface.
- **Application** - Name of the affected application.
- **App Context** - Context of the affected application.
- **Rule** - Displays the rule that affects the traffic.
- **Any Interface** - Shows the forward or reverse interface.
- **Idle Time [s]** - The time sessions are in idle state. If specified, the idle time and less (<) in seconds is implied. Entering < and > is possible.
- **Protocol** - Shows the protocol.
- **File Content** - Shows the file type.
- **User Agent** - User agent for HTTP- and HTTPS connections.
- **URL Category** - Shows the URL category.
- **Source Geo** - The source host's geographic location.
- **Destination Geo** - The destination host's geographic location.

Filter Icons

Clicking the **Open History with same filter** icon on the top right of the ribbon bar above the filters allows you to switch to the [History Page](#) but with the same filters applied. Clicking the **Save and Restore Filter and Column Settings** icon in the ribbon bar will open a drop-down menu that lets you save, restore, or delete filter and column view settings.



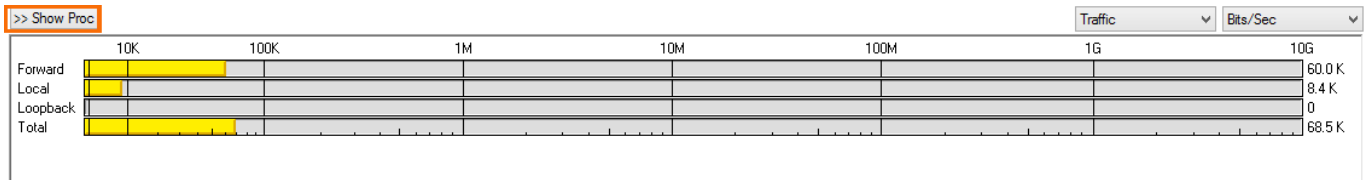
Managing Sessions

You can control, copy, print, export, and organize the sessions that are listed on the **Firewall > Live** page. When you right-click a session, you are provided with the following options:

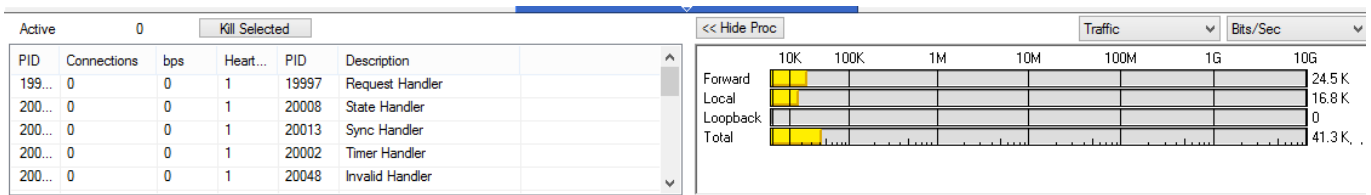
Option	Description
Terminate Session	Ends the session.
Abort Session (No TCP RST)	Ends the session without a TCP request.
Change QoS / Reverse QoS	Lets you change the QoS Band. For more information, see Traffic Shaping .
Change TI Settings	Lets you change the Traffic Intelligent settings. For more information, see Traffic Intelligence .
Show Session Details	Displays the session details.
Save Traffic Selection Policy	Saves the traffic selection policy.
Find	Opens the search window at the top of the list.
Select / Deselect All	Selects or deselects all of the sessions.
Copy <...> to Clipboard	Copies the selected entry to the clipboard.
Copy List to Clipboard	Copies the list to the clipboard.
Copy selected to Clipboard	Copies the selected row to the clipboard.
Export to File	Exports the selected entry to a text file.
Print List	Prints the Firewall Live view.
Group by Interface	Groups access cache entries by their interface.
Columns	Lets you select the columns to hide or show. The following options are also provided: <ul style="list-style-type: none"> • Default Columns - Offers the standard view. • Optimize All Columns - Adjusts the column size for best display. • Adjust All Columns - Displays all columns that are selected.

Work Processes

In the lower left of the **Live** page, you can view and control firewall-related processes and workers. To access the status, simply click >> **Show Proc** on the lower left of the window.



The entry **Active** displays the currently active worker processes. The feature **Kill Selected** is used for terminating single workers.



Active	0	Kill Selected			
PID	Connections	bps	Heart...	PID	Description
199...	0	0	1	19997	Request Handler
200...	0	0	1	20008	State Handler
200...	0	0	1	20013	Sync Handler
200...	0	0	1	20002	Timer Handler
200...	0	0	1	20048	Invalid Handler

The entry on the right of the **Kill Selected** button shows the status of the synchronization in case of active Transparent Failover ([High Availability](#)) and consists of the following possible states:

- **Active Sync (UP)** – shown on active HA partner; synchronization works.
- **Active Sync (DOWN)** – shown on active HA partner; sync would work, but Box Firewall is down.
- **Passive Sync (UP)** – shown on passive HA partner; synchronization works.
- **Passive Sync (DOWN)** – shown on passive HA partner; sync would work, but Box Firewall is down.

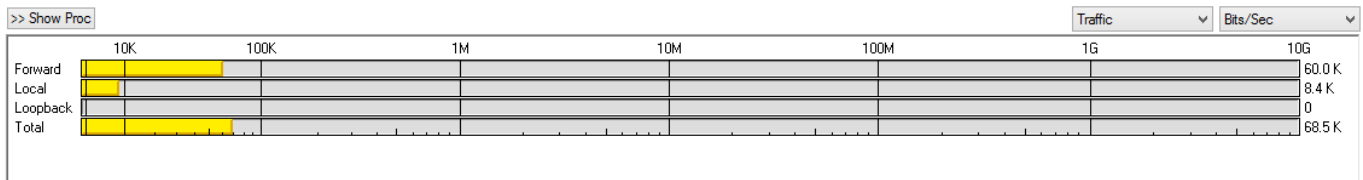
The window provides the following information about the processes:

- **PID** – System process ID.
- **Connections** – Number of connections handled by worker.
- **Bit/s** – Bytes per second (during the last second).
- **Heartbeat** – Time in seconds the process stopped to answer. Should never be more than 2.
- **PID** – System process ID; allows view on PID and fully extended description column.
- **Description** – Role description of worker.

Traffic Meter

A traffic meter is integrated on the lower right of the page. The firewall engine samples the amount of

traffic over 10 seconds and the traffic meter shows it based on the traffic origin (Forward, Loopback, Local, Total). Traffic can be displayed as Bits/sec, Bytes/sec or Packets/sec.



The second available view is called **TF Sync** (click the **Traffic** drop-down arrow) and contains detailed information concerning the **Transparent Failover** function of an HA Forwarding Firewall. The pull-down menu for the statistics type (with the options **Bits/sec**, **Bytes/sec** and **Packets/sec**) has no function for this type of view. The display consists of the following entries:

- **My Sync Addr** - IP address and connection port for synchronisation of this box.
- **Partner Sync Addr** - IP address and connection port for synchronisation of the HA partner box.
- **Synced Sessions** - Number of sessions successfully synchronized.
- **Pending Sessions** - Number of pending sessions that are not synchronized.

Status Overview

This table provides descriptions of the possible statuses that are displayed in the Status column for each session on the **Firewall > Live** page:

Status Name	Origin	Description
FWD-NEW	TCP Packet Forwarding Outbound	The session is validated by the firewall ruleset. Traffic has not been forwarded yet.
FWD-FSYN-RCV	TCP Packet Forwarding Outbound	The initial SYN packet received from the session source was forwarded.
FWD-RSYN-RSV	TCP Packet Forwarding Outbound	The session destination answered the SYN with a SYN/ACK packet.
FWD-EST	TCP Packet Forwarding Outbound	The SYN/ACK packet was acknowledged by the session source. The TCP session is established.
FWD-RET	TCP Packet Forwarding Outbound	Either source or destination are retransmitting packets. The connection might be dysfunctional.
FWD-FFIN-RCV	TCP Packet Forwarding Outbound	The session source sent a FIN datagram to terminate the session.
FWD-RLACK	TCP Packet Forwarding Outbound	The session destination answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet.

FWD-RFIN-RCV	TCP Packet Forwarding Outbound	The session destination sent a FIN datagram to terminate the session.
FWD-FLACK	TCP Packet Forwarding Outbound	The session source answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet.
FWD-WAIT	TCP Packet Forwarding Outbound	The session was reset by one of the two participants by sending a RST packet. During a wait period of five seconds, all packets belonging to the session will be discarded.
FWD-TERM	TCP Packet Forwarding Outbound	The session is terminated and will be removed from the session list.
IFWD-NEW	TCP Packet Forwarding Inbound	The session is validated by the firewall rule set. Traffic has not been forwarded yet.
IFWD-SYN-SND	TCP Packet Forwarding Inbound	A SYN packet was sent to the destination initiating the session. Note that the session with the source is already established.
IFWD-EST	TCP Packet Forwarding Inbound	The destination replied to the SYN with a SYN/ACK. The session is established.
IFWD-RET	TCP Packet Forwarding Inbound	Either source or destination are retransmitting packets. The connection might be dysfunctional.
IFWD-FFIN-RCV	TCP Packet Forwarding Inbound	The session source sent a FIN datagram to terminate the session.
IFWD-RLACK	TCP Packet Forwarding Inbound	The session destination answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet.
IFWD-RFIN-RCV	TCP Packet Forwarding Inbound	The session destination sent a FIN datagram to terminate the session.
IFWD-FLACK	TCP Packet Forwarding Inbound	The session source answered the FIN packet with a FIN reply and awaits the last acknowledgement for this packet.
IFWD-WAIT	TCP Packet Forwarding Inbound	The session was reset by one of the two participants by sending a RST packet. During a wait period of five seconds, all packets belonging to the session will be discarded.
IFWD-TERM	TCP Packet Forwarding Inbound	The session is terminated and will be removed from the session list.
PXY-NEW	TCP Stream Forwarding Outbound	The session is validated by the firewall rule set. Traffic has not been forwarded yet.
PXY-CONN	TCP Stream Forwarding Outbound	A socket connection to the destination is being established.
PXY-ACC	TCP Stream Forwarding Outbound	A socket connection to the source is being accepted.

PXY-EST	TCP Stream Forwarding Outbound	Two established TCP socket connections to the source and destination exist.
PXY-SRC-CLO	TCP Stream Forwarding Outbound	The socket to the source is closed or is in the closing process.
PXY-DST-CLO	TCP Stream Forwarding Outbound	The socket to the destination is closed or is in the closing process.
PXY-SD-CLO	TCP Stream Forwarding Outbound	The source and the destination socket are closed or in the closing process.
PXY-TERM	TCP Stream Forwarding Outbound	The session is terminated and will be removed from the session list.
IPXY-NEW	TCP Stream Forwarding Inbound	The session is validated by the firewall rule set. Traffic has not been forwarded yet.
IPXY-ACC	TCP Stream Forwarding Inbound	A socket connection to the source is being accepted.
IPXY-CONN	TCP Stream Forwarding Inbound	A socket connection to the destination is being established.
IPXY-EST	TCP Stream Forwarding Inbound	Two established TCP socket connections to the source and destination exist.
IPXY-SRC-CLO	TCP Stream Forwarding Inbound	The socket to the source is closed or is in the closing process.
IPXY-DST-CLO	TCP Stream Forwarding Inbound	The socket to the destination is closed or is in the closing process.
IPXY-SD-CLO	TCP Stream Forwarding Inbound	The source and the destination socket are closed or in the closing process
IPXY-TERM	TCP Stream Forwarding Inbound	The session is terminated and will be removed from the session list.
UDP-NEW	UDP Forwarding	The session is validated by the firewall rule set. Traffic has not been forwarded yet.
UDP-RECV	UDP Forwarding	Traffic has been received from the source and was forwarded to the destination.
UDP-REPL	UDP Forwarding	The destination replied to the traffic sent by the source.
UDP-SENT	UDP Forwarding	The source transmitted more traffic after receiving a reply from the destination.
UDP-FAIL	UDP Forwarding	The destination or a network component on the path to the destination sent an ICMP indicating that the request cannot be fulfilled.
ECHO-NEW	ECHO Forwarding	The session is validated by the firewall rule set. Traffic has not been forwarded yet.
ECHO-RECV	ECHO Forwarding	Traffic has been received from the source and forwarded to the destination.
ECHO-REPL	ECHO Forwarding	The destination replied to the traffic sent by the source.

ECHO-SENT	ECHO Forwarding	The source sent more traffic after receiving a reply from the destination.
ECHO-FAIL	ECHO Forwarding	The destination or a network component on the path to the destination sent an ICMP indicating that the request cannot be fulfilled.
OTHER-NEW	OTHER Protocols Forwarding	The session is validated by the firewall rule set. Traffic has not been forwarded yet.
OTHER-RECV	OTHER Protocols Forwarding	Traffic has been received from the source and forwarded to the destination.
OTHER-REPL	OTHER Protocols Forwarding	The destination replied to the traffic sent by the source.
OTHER-SENT	OTHER Protocols Forwarding	The source sent more traffic after receiving a reply from the destination.
OTHER-FAIL	OTHER Protocols Forwarding	The destination or a network component on the path to the destination sent an ICMP indicating that the request cannot be fulfilled.
LOC-NEW	Local TCP Traffic	A local TCP session was granted by the local rule set.
LOC-EST	Local TCP Traffic	The local TCP session is fully established.
LOC-SYN-SND	Local TCP Traffic	A Local-Out TCP session is initiated by sending a SYN packet.
LOC-SYN-RCV	Local TCP Traffic	A Local-In TCP session is initiated by receiving a SYN packet.
LOC-FIN-WAIT1	Local TCP Traffic	An established local TCP session started the closing process by sending a FIN packet.
LOC-FIN-WAIT2	Local TCP Traffic	A local TCP session in the FIN-WAIT1 state received an ACK for the FIN packet.
LOC-TIME-WAIT	Local TCP Traffic	A local TCP session in the FIN-WAIT1 or in the FIN-WAIT2 state received a FIN packet.
LOC-CLOSE	Local TCP Traffic	An established local TCP session is closed.
LOC-CLOSE-WAIT	Local TCP Traffic	An established local TCP session received a FIN packet.
LOC-LAST-ACK	Local TCP Traffic	Application holding an established TCP socket responded to a received FIN by closing the socket. A FIN is sent in return.
LOC-LISTEN	Local TCP Traffic	A local socket awaits connection request (SYN packets).
LOC-CLOSING	Local TCP Traffic	A local socket in the FIN_WAIT1 state received a FIN packet.
LOC-FINISH	Local TCP Traffic	A local TCP socket was removed from the internal socket list.

Policy Overview

This table provides descriptions of the possible policies that you might see in the **Policy** column for each session on the **Firewall > Live** page:

Policy	Description
NO_MATCH_IIF	The received packet (Forward Direction) must NOT match initial input interface.
NO_MATCH_OIF	The received packet (Reverse Direction) must NOT match initial output interface.
INBOUND	The Inbound Accept Policy is used.
FWD_FILTER	The content filter is applied for forward traffic.
REV_FILTER	The content filter is applied for reverse traffic.
TRACE	The session is traced.
NOTIFY_CONECT	The Firewall Service is notified about successful or failing TCP establishment. These notifications are required for multiple redirection status.
Source-Based NAT	The bind IP address is determined by the routing table.
NOLOG	Log file entries are not generated by the session.
NOSTAT	Statistics are not generated by the session.
NOCACHE	An access cache entry is not generated by the session.
NONAGLE	The Nagle algorithm is turned OFF.
LOG_STATE	Every state change of this session is logged.
OWN_LOG	The session will log to the firewall rule log file.
SRVSTAT	The session resolves service object names when generating statistics.
DYNAMIC_PORT	The session is dynamically NAT'd. The outgoing source port will differ from the original client port.
NOSYNC	The session is not synchronized for transparent failover.
CLEAR_ECN	The session clears any ECN bits in the IP header.

Figures

1. fw_live_01.png
2. transfer.png
3. tcp3.png
4. udp1.png
5. udp3.png
6. udp4.png
7. hasync.png
8. ips.png
9. app.png
10. wanopt.png
11. slot_deny.png
12. fw_tab_filter.png
13. fw_live_02.png
14. fw_live_03.png
15. fw_live_04.png

© Barracuda Networks Inc., 2020 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.