

## Monitoring Active and Recent Connections

<https://campus.barracuda.com/doc/13306421/>

To monitor network sessions or connections, view the following pages from the **BASIC** tab:





- **Active Connections** – Lists all of the open and established sessions on the appliance.
- **Recent Connections** – Lists all of the connections that were established on the Barracuda NextGen X-Series Firewall or that were trying to access the firewall.

You can find the information that you are interested in by filtering the lists. For a description of the displayed fields and information on how to add filters, click **Help** on the product page.

### Active Connections

The **BASIC > Active Connections** page lists all of the open and established sessions on the appliance. You can terminate any session by clicking on the red x (✘). If QoS is enabled for a connection, you can manually override the bandwidth policy for the connection by clicking on the arrow next to it and selecting a different policy from the drop-down menu.

In the **State** column, the following arrows tell you if the connection is established or closing:







Arrow	Status
	One-way traffic.
	Connection established (TCP). Two-way traffic (all other).
	Connection could not be established.
	Closing connection.

To view the status of a connection, hover over the arrow for a status code. For more information about these status codes, see the [Status Code Overview](#).

### Recent Connections

The **BASIC > Recent Connections** page lists all of the connections that were established on the X-Series Firewall or that were trying to access the firewall. Use the information on this page for troubleshooting.

In the **Action** column, the following graphics tell you what action was performed for each connection:

Graphic	Action
	IPS Rule Applied
	Allowed
	Terminated
	Failed
	Blocked
	Dropped

To see if there is still incoming or outgoing traffic for a specific session, click **Refresh** and then look at its **Last** or **Count** value.

Sometimes, you might need to view ARP-Update traffic to troubleshoot in more detail. To display ARP-Update info, select the **Include ARPs** check box.

To delete the whole history, click **Flush Entries**.

## Status Code Overview

The following table provides more details on the status codes that you might see on the **BASIC > Active Connections** page.

Status Code	Origin	Description
FWD-NEW	TCP Packet Forwarding Outbound	Session is validated by the firewall rule set, no traffic was forwarded so far.
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 acknowledge 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 indicating 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 indicating 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. A wait period of 5 seconds will silently discard all packet belonging to that session.
FWD-TERM	TCP Packet Forwarding Outbound	The session is terminated and will shortly be removed from the session list.
IFWD-NEW	TCP Packet Forwarding Inbound	Session is validated by the firewall rule set, no traffic was forwarded so.
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 the SYN with a SYN/ACK. The session is established.
IFWD-RET	TCP Packet Forwarding Inbound	Either source or destination are re transmitting packets. The connection might be dysfunctional.
IFWD-FFIN-RCV	TCP Packet Forwarding Inbound	The session source sent a FIN datagram indicating 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 indicating 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. A wait period of 5 seconds will silently discard all packet belonging to that session.
IFWD-TERM	TCP Packet Forwarding Inbound	The session is terminated and will shortly be removed from the session list.
PXY-NEW	TCP Stream Forwarding Outbound	Session is validated by the firewall rule set, no traffic was forwarded so far.
PXY-CONN	TCP Stream Forwarding Outbound	A socket connection to the destination is in progress of being established.
PXY-ACC	TCP Stream Forwarding Outbound	A socket connection to the source is in progress of being accepted.
PXY-EST	TCP Stream Forwarding Outbound	Two established TCP socket connection 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 shortly be removed from the session list.
IPXY-NEW	TCP Stream Forwarding Inbound	Session is validated by the firewall rule set, no traffic was forwarded so far.
IPXY-ACC	TCP Stream Forwarding Inbound	A socket connection to the source is in progress of being accepted.
IPXY-CONN	TCP Stream Forwarding Inbound	A socket connection to the destination is in progress of being established.
IPXY-EST	TCP Stream Forwarding Inbound	Two established TCP socket connection 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 shortly be removed from the session list.
UDP-NEW	UDP Forwarding	Session is validated by the firewall rule set, no traffic was forwarded so far.
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 further traffic after having received 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 serviced.
ECHO-NEW	ECHO Forwarding	Session is validated by the firewall rule set, no traffic was forwarded so far.
ECHO-RECV	ECHO Forwarding	Traffic has been received from the source and was 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 racing 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 serviced.

OTHER-NEW	OTHER Protocols Forwarding	Session is validated by the firewall rule set. No traffic was forwarded so far.
OTHER-RECV	OTHER Protocols Forwarding	Traffic has been received from the source and was 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 serviced.
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 close 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.

## Figures

1. red.png
2. one-way traffic.PNG
3. two-way traffic.PNG
4. unestablished.PNG
5. closing.PNG
6. IPS rule.png
7. allow.png
8. term.png
9. fail.png
10. block.png
11. drop.png

© 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.