

# CC FWAUDIT Tab

The **FWAUDIT** tab provides access to the Firewall Audit viewer. The Firewall Audit viewer displays information related to firewall sessions on managed Barracuda NextGen F-Series Firewalls. The type of data collected depends on the FW Audit settings on the individual units (see [FW Audit](#)). Similar to the [Log Viewer](#) directly on the NextGen Firewall F-Series, the Firewall Audit viewer supports navigating to a dedicated date/time and browsing backward and forward.

Box	Date/Time	Box	Operation	Type	Proto	Src IF	Src IP	Src Port	Src MAC	Dst IP	Dst Port	Dst Servi...	Dst IF	Rule	Info	Dst NA
HQ-NG1	2014 08 1...	HQ-NG...	LocalRemove	LOUT	TCP	eth0	10.0.10...	61318		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
BO2-NG1	2014 08 1...	HQ-NG...	LocalAllow	LOUT	TCP	eth0	10.0.10...	61318		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalRemove	LOUT	TCP	eth0	10.0.10...	61319		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalAllow	LOUT	TCP	eth0	10.0.10...	61319		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalRemove	LOUT	TCP	eth0	10.0.10...	61320		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalAllow	LOUT	TCP	eth0	10.0.10...	61320		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalAllow	LOUT	TCP	eth0	10.0.10...	51147		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalRemove	LOUT	TCP	eth0	10.0.10...	51147		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalRemove	LOUT	TCP	eth0	10.0.10...	51148		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalAllow	LOUT	TCP	eth0	10.0.10...	51148		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalAllow	LOUT	TCP	eth0	10.0.10...	51149		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	
	2014 08 1...	HQ-NG...	LocalRemove	LOUT	TCP	eth0	10.0.10...	51149		10.0.10.1...	5049	ivocalize	eth0	BOX...	Norma...	

## In this article:

### Information Display

The **FWAUDIT** page lists firewall audit data information and provides several filtering options. To display log files for one or several managed Barracuda NextGen Firewall F-Series units, double-click the Barracuda NextGen Firewall F-Series in the left column to select it and click the down arrow icon in the upper right of the ribbon bar (↓).

The columns on the **FWAUDIT** page display the following information:

- **Date/Time** – Date and time when the operation was performed.
- **Box** – The affected Barracuda NextGen Firewall F-Series.
- **Operation** – Displays the operation.
- **Type** – The operation type.
- **Proto** – The protocol used.
- **Src IF** – The source interface.
- **Src IP** – The source IP address.
- **Src Port** – The source port.
- **Src MAC** – The source MAC address, if applicable.
- **Dst IP** – The destination IP address.
- **Dst Port** – The destination port.
- **Dst Service** – The destination service.
- **Dst IF** – The destination interface.
- **Rule** – The access or application rule that applies.
- **Info** – Displays additional information, if available.
- **DstNAT** – The destination NAT address.
- **SrcNAT** – The source NAT address.
- **Count** – Displays how often the operation was carried out.



- **Duration** – Duration time of the operation.
- **In Bytes** – Amount of incoming traffic in Bytes.
- **In Pkts** – Amount of incoming traffic in Pkts.
- **Out Bytes** – Amount of outgoing traffic in Bytes.
- **Out Pkts** – Amount of outgoing traffic in Pkts.
- **Total Bytes** – Total traffic in Bytes.
- **User** – The user affected by the operation.

**Filtering Options**

Clicking the first filter icon (**Selection**) in the ribbon bar opens the **Selection** menu, which provides the following options:

Box	Date/Ti...	Box	Operation	Type	Proto	Src IF	Src IP	Src Port	Src MAC	Dst IP	Dst Port	Dst Servi...	Dst IF	R...	I...	Dst N...	S...	D..	In...	Total Bytes	U	
HQ-NG1	✓ 201...	B...	LocalAllow	LO...	ICMP	tap3	10.0.11...	48757		10.0.10.77	48757	icmp-echo	tap3	B...	N...			0s	2	336		
BO2-NG1	✓ 201...	B...	LocalRe...	LO...	ICMP	tap3	10.0.11...	16423		10.0.10.77	16423	icmp-echo	tap3	B...	N...							
BO1-NG4	✓ 201...	B...	LocalAllow	LO...	ICMP	tap3	10.0.11...	64039		10.0.10.77	64039	icmp-echo	tap3	B...	N...							
	201...	B...	LocalRe...	LO...	ICMP	tap3	10.0.11...	48757		10.0.10.77	48757	icmp-echo	tap3	B...	N...			0s	2	336		

- **Traffic Selection** – From the **Traffic Selection** list, you can select the following options to filter for certain traffic types:
  - **Forward** – Displays the traffic on the Forwarding Firewall.
  - **Local In** – Displays the incoming traffic on the Host Firewall.
  - **Local Out** – Displays the outgoing traffic from the Host Firewall.
  - **Loopback** – Traffic over the loopback interface.
- **Event Selection** – From the **Event Selection** list, you can select the following options to filter for certain traffic types:
  - **Allowed** – Displays all allowed events.
  - **Blocked** – Displays all blocked events.
  - **Dropped** – Displays all dropped events.
  - **Fail** – Displays all failed events.
  - **ARP** – Displays all ARP requests.
  - **IPS Hit** – Displays all events detected by the IPS.
  - **Removed** – Displays all removed events.

Clicking the second filter icon (**Filter**) opens the **Filter** menu, which provides the following options:

Box	Date/Time	Box	Operation	Type	Proto	Src IP	Src Port	Dst IP	Dst Port	Dst Service	Total Bytes	
HQ-NG1	✓ 201...	HQ-NG1...	Allow	FWD	UDP	eth0	10.0.10.100	53925	00:0c:29:...	216.239...	53	62.9...
BO2-NG1	✓ 201...	HQ-NG1...	Allow	FWD	UDP	eth0	10.0.10.100	53925	00:0c:29:...	216.239...	53	62.9...
BO1-NG4	✓ 201...	HQ-NG1...	Allow	FWD	UDP	eth0	10.0.10.100	54160	00:0c:29:...	8.8.4.4	53	62.9...

- **Rule** – Allows setting a filter for a specific rule.
- **Proto** – Allows setting a filter for a specific protocol.
- **Source/Dest.** – Allows setting a filter for a specific IP address/range that matches either source or destination.
- **Interface** – Allows setting a filter for a specific interface (for example, eth0).
- **Addr.** – Allows setting a filter for a specific destination IP address/range.
- **Srv.** – Allows setting a filter for a specific service.
- **Port** – Allows setting a filter for a specific port.



- **Src/Dst-Interface** - Allows setting a filter for the source/destination interface.
- **Source** - Allows setting a filter for the source NAT address.
- **Dest. NAT** - Allows setting a filter for the destination NAT address.
- **User** - Allows setting a filter for the user affected by the operation.

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".

On the top right of the ribbon bar of the **Audit Log** page, you can specify a time and date to view logs that were created within a set time interval.

### Log File Display Modes

The **FWAUDIT** page lists firewall audit data information according to the specified filter selection and time interval. By default, all entries are shown line by line in the list (**Log File Mode**). The **Log File Mode** dropdown provides two display options.

- **Log File Mode** - Log files are shown line by line according to the specified filter selection and time interval.
- **Accumulation Mode** - Log files are shown accumulated by specified merging criteria. This provides a more general overview of similar event or session categories.

### Log File Mode

By default, all entries are shown line by line in the list (**Log File Mode**). In the navigation bar on the top right of the ribbon bar, you can select how information is displayed in the list. Use the **Max Entries** field to adjust the number of entries displayed in the list. To view a log entry, double-click it.

EVENTS PKI NAC **FWAUDIT**

Accumulation
 Log File Mode
 13:14:25 03.09.2015
 Max Entries: 500

Port	Src MAC	Dst IP	Dst Port	Dst Servi...	Dst IF	R...	I...	Dst N...	S...	D..	In...	Total Bytes
5		10.0.10.77	3665	icmp-echo		B...	N...					
		10.0.10.70	123	ntp		B...	S...		1...	0s	1	76
5		10.0.10.77	3665	icmp-echo	tap3	B...	N...			0s	2	336

You can navigate through the log entries with the following navigation buttons:



- Browse backward from the current entry.



- Display log files / filtering results for selected criteria such as the specified time and date.



- Browse forward from the current entry.



- Browse to the end of the log.

### Accumulation Mode

Accumulation allows you to group events by specific criteria, such as source, protocol, or access rule. To accumulate events, you must select a time interval from the fields provided in the ribbon bar. Select **Accumulated Event Mode** from the **Log File Mode** dropdown, and click the icon next to the filter (**Accumulation**) to open the **Accumulation** filter.



Selection Filter Accumulation Accumulated Event Mode 12:39:44 15.07.2015 12:39:44 04.09.2015 Max Entries: 500

Accumulation

Operation  Source Address  Service  Rule  Boxname

Type  DstAddr  Protocol  Info  User

The **Accumulation** filter provides the following options:

- **Operation** - Accumulate entries by operation.
- **Type** - Accumulate entries by operation type.
- **Source Address** - Accumulate entries by source IP address/range.
- **Destination Address** - Accumulate entries by destination IP address.
- **Service** - Accumulate entries by service.
- **Protocol** - Accumulate entries by the protocol used.
- **Rule** - Accumulate entries by access or application rule.
- **Info** - Accumulate entries by additional information.
- **Boxname** - Accumulate entries by box name
- **User** - Accumulate entries by affected user.

To display the log files and filtering results for the selected criteria, click the down arrow icon in the upper right of the ribbon bar ( ↓ ).

Selection Filter Accumulation Accumulated Event Mode 12:39:44 15.07.2015 12:39:44 04.09.2015 Max Entries: 500 ↓

Accumulation

Operation  Source Address  Service  Rule  Boxname

Type  DstAddr  Protocol  Info  User

Box	Last	Box	Operation	Type	Proto	Src IP	Det ...	Det S ...	Rule	Info	Count	In Bytes	In Pkts	Out Byte
✓ HQ-NG1	1m 30s	HQ-NG1_...		FWD	UDP				BLOCKALL	Block by Rule	3308			
BO2-NG1	1m 30s	HQ-NG1_...		FWD	UDP	10.0.10.100			LAN-2-INTERNET	Block Broadcast	1962			
BO1-NG4	1m 30s	HQ-NG1_...		LRD	TCP	10.0.10.11			GuestAccess	Connection R...	7811	5.8 M	45.7 K	8.8 M
	1m 31s	HQ-NG1_...		LOUT	TCP	10.0.10.88			PASSALL	Normal Operat...	112381	4.1 M	70.3 K	1.5 M
	1m 32s	HQ-NG1_...		FWD	TCP	10.0.10.70			LAN-2-INTERNET	Normal Operat...	588			

Use the **Max Entries** field to adjust the number of entries displayed in the list.

