Trace Page

https://campus.barracuda.com/doc/41116107/

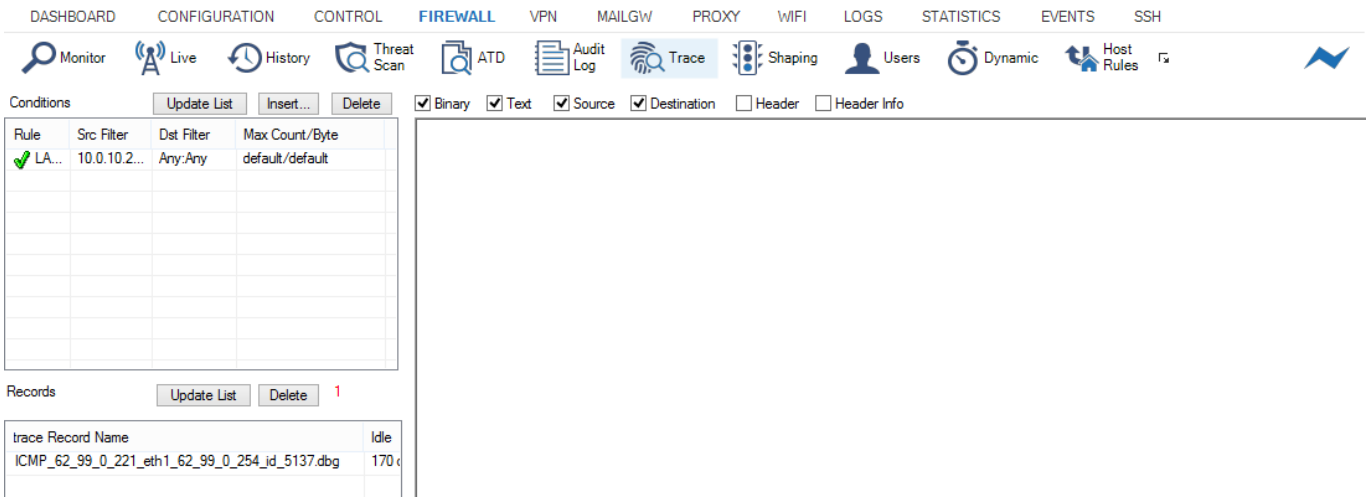
Tracing is no longer supported for firmware version 6.0.0 and higher. Contact Barracuda Networks Technical Support if you need to trace connections.

Connection tracing is a powerful tool for firewall management. The Barracuda NG Firewall is able to record every data byte that makes its way through the firewall engine. This is vital for detecting errors in network-based applications and is essential for network administrators who deal with an ever-changing environment.

In this article:

Define Tracing Conditions

On the **Trace** page, you can specify tracing conditions for Forwarding Firewall traffic. To access the **Trace** page, open the **Firewall** tab, expand the ribbon bar and select the **Trace** icon.



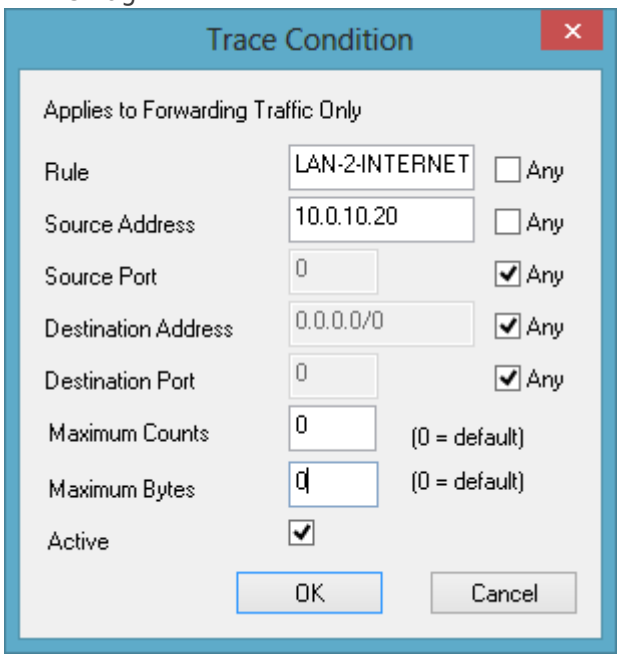
Trace conditions cannot be applied for local traffic. Tracing of local traffic is only available for active connections (see: Tracing of Active Connections).

If you select tracing conditions that are too general, performance will suffer. It will also be very

difficult to find the connection you actually need to trace.

To define tracing conditions,

1. Open the **Firewall > Trace** page.
2. In the **Conditions** section, click **Insert**.
3. Specify as follows the conditions when connections should be traced:
   - **Rule** – Name of the rule to be traced.
   - **Source Address** – IP address of the source; single IPs or netmasks allowed.
   - **Source Port** – Port of the source address.
   - **Destination Address** – IP address of the destination; single IPs or netmasks allowed.
   - **Destination Port** – Port of the destination address.
   - **Maximum Counts** – Only the first n packets are recorded. 0 is the service default, which can be set in the firewall service parameters. The default is 512.
   - **Maximum Bytes** – Only the first n kilobytes are recorded. 0 is the service default, which can be set in the firewall service parameters. The default is 256 KB.
   - **Active** – You can keep a list of predefined trace conditions and switch them on/off by settings in this flag.



4. Click **OK**.

Connections are monitored from the moment a corresponding connection is initiated. The introduction of a new trace condition has no effect on already established sessions.

When configured, the Conditions list provides the following details:

- **Rule** – Name of the rule to be traced.
- **Src Filter** – IP address / port of the source.

- **Dst Filter** – IP address / port of the destination.
- **Max. Count / Byte** – The first n packets or kilobytes that are recorded.

View Tracing Sessions

With tracing configured, the Records list on the left-hand side provides the following details:

- **Trace Record Name** – Name of the traced record.
- **Idle** – Idle time of the traced record.
- **Size** – Size of the traced record.

To view session details, double-click on a trace record to open the session in the trace window.

> The trace window lists all available tracing sessions. The notation is *rule_sourceIP_sourcePORT_destIP_destPORT.dbg.* The corresponding files are located in */var/phion/debug/trans.* The maximum number of recorded tracing sessions can be set in the firewall basic configuration. The default is 512.

The trace window displays the connection traffic as follows:

- **Green** – Data sent by source.
- **Blue** – Data sent by destination.
- **Yellow** – Messages from firewall (closing of connections).

Use the following checkboxes for filtering the view:

- **Binary** – Show traffic in binary notation.
- **Text** – Show traffic in text notation.
- **Source** – Show traffic generated by source.
- **Destination** – Show traffic generated by destination.
- **Header** – Show traffic header.
- **Header Info** – Show header information.

Tracing of Active Connections

A current connection can be selected in the **Live** tab of the firewall monitoring interface and monitored from the moment tracing is activated:

1. Open the Live Page page.

2. Right-click the session(s) to be traced and select **Toggle Trace**.

The selected connections immediately be traced, and you will be able to see all data transferred within these connections in the Trace view. Traced connections get an additional -*Trace* entry in the **Type** column. To stop tracing, select the traced connections, and select **Toggle Trace** again.

Figures

1. trace.png
2. tr_edit.png