

<https://campus.barracuda.com/doc/96026515/>

FILTER SETTINGS

Top 50 ▾ Last 7 days ▾ All ▾

Displaying data from: 20:03.2019 00:00:00 - 27:03.2019 00:00:00

Click on list items to change the scope of the displayed information.

RISK RATING

4.5 GB

4.5 GB

GEO DESTINATION

Non-routable or Private IP ... 4.5 GB

Austria 119.0 MB

United States 20.3 MB

Germany 2.9 MB

Unknown 287.4 KB

Italy 6.5 KB

APPLICATION DETAIL

VIRUS SCAN

APPLICATION PROPERTY

NONE 4.6 GB

APPLICATION

APPLICATION CATEGORY

Uncategorized 4.6 GB

RISK

4.6 GB

USER

Not set 4.6 GB

SOURCE

10.17.94.54 4.5 GB

10.17.94.96 84.9 MB

127.0.0.1 10.7 MB

10.17.4.75 6.4 MB

192.168.200.200 716.9 KB

127.0.0.9 304.0 B

ATP

USER AGENT

FILE CONTENT

GEO SOURCE

Non-routable or Private IP ... 4.6 GB

Unknown 287.4 KB

DOMAIN

URL CATEGORY

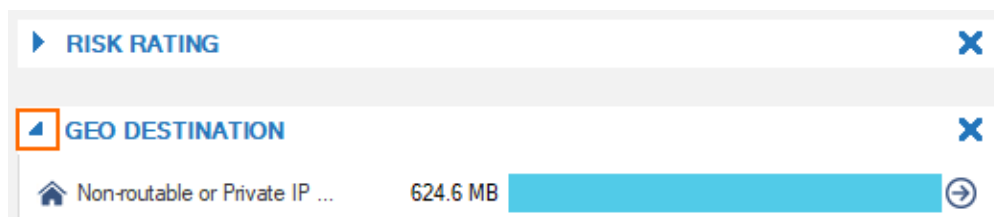
IPS

PROTOCOL

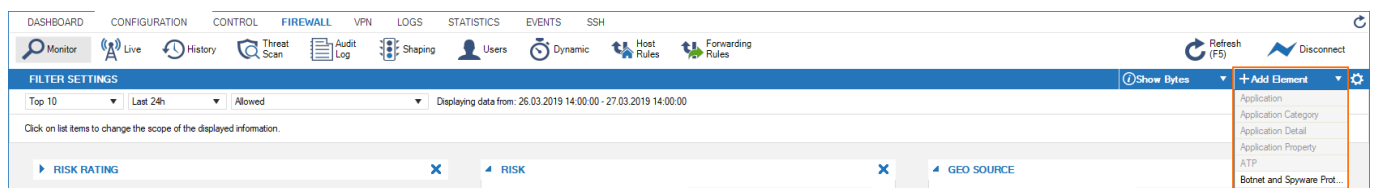
- **Risk Rating** – Displays the overall risk rating of all applications that apply to currently displayed traffic information.
- **Application Detail** – Allows in-depth inspection of the application rule handling process.
- **URL Category** – Provides traffic load information related to URL categories.
- **ATP** – Shows traffic affecting Advanced Threat Protection (ATP), if configured.
- **Application Property** – Provides traffic load information related to application properties.
- **Botnet and Spyware Protection** – Provides traffic load information related to botnet and spyware detection.
- **File Content** – Provides traffic load information related to application content.
- **Application Category** – Provides traffic load information related to categories.
- **Geo Source** – Displays the geographic location of the application source, if available.
- **Geo Destination** – Displays the geographic location of the application destination, if available.
- **User** – Provides information on users and groups that are accessing the application.
- **User Agent** – Displays the user agents for HTTP and HTTPS connections.
- **Domain** – Displays the domains involved in the application rule handling process.
- **Source** – Provides information on the application source, if available.
- **Virus Scan** – Provides traffic load information related to virus and malware detection.

- **IPS** – Shows traffic affecting the Intrusion Prevention System (IPS).
- **Application** – Displays the applications that are referred to by application rules as soon as the rules apply to incoming or outgoing network traffic.
- **Protocol** – Displays the protocols that the applications affect and that are involved in the application rules process.
- **Risk** – Provides traffic load information related to risk levels (1 - 4).

To view or collapse a section, click the arrow icon to the left of each section heading.



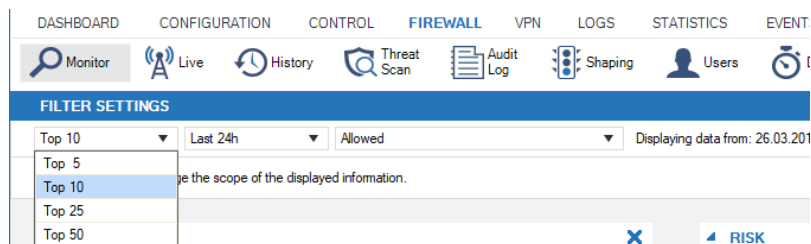
To show or hide an entire section, click **Add Element** on the top right of the page, and choose the sections you want.



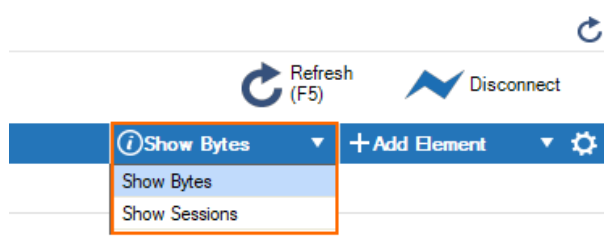
## Filtering Functions

The **FILTER SETTINGS** section on top of the page provides drop-down menus that allow you to filter for the following criteria:

- **Applications** – Show all application traffic or drill down the displayed information to a selected number of top applications.
- **Time** – Select a time interval for application traffic information to be displayed. Information can be displayed on an hourly, daily, weekly, or monthly basis.
- **Traffic Type** – Filter display information based on application traffic affected by the Virus Scanner, Intrusion Prevention System (IPS), and Advanced Threat Protection (ATP). For example, select **Blocked** to filter for traffic blocked by application rules.

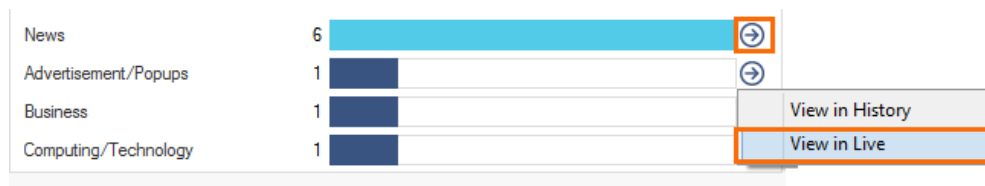


Expand the drop-down menu on the upper right to toggle displayed traffic information by bytes or the number of sessions.

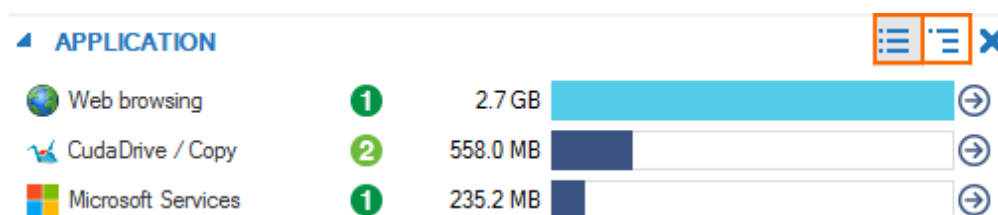


## Managing Traffic Information





Some sections, such as **Application** or **URL Category**, provide links to the **Live** and **History** views. When you click the arrow icon next to the entry, the **Live** or **History** page opens and automatically applies a filter for the selected application.



Some sections, such as **Application** or **Protocol**, offer icons to change the list to a flat or grouped display.



Clicking an entry in the **Application** section opens an information display window under the **Filter Settings** section. To exit the selection and return to standard view, click **x**.

FILTER SETTINGS				 Show Bytes ▾	+ Add Element ▾	
Top 25 ▾	Current month ▾	All ▾	Displaying data from: 01.03.2019 00:00:00 - 31.0			
Application: Debian Update ✕						
 <b>Debian Update</b>		This application identifies the download of Debian updates. Debian is a computer operating system composed of software packages released as free and open source software primarily under the GNU General Public License along with other free software licenses. This application is not SSL-interceptable, thus it is excluded from SSL-Interception automatically.				
 Software Update						

## Figures

1. fw\_monitor\_page\_01.png
2. fw\_monitor\_page\_03.png
3. fw\_monitor\_page\_04.png
4. fw\_monitor\_page\_02.png
5. fw\_monitor\_page\_02a.png
6. fw\_monitor\_page\_05.png
7. fw\_monitor\_page\_06.png
8. fw\_monitor\_page\_07.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.