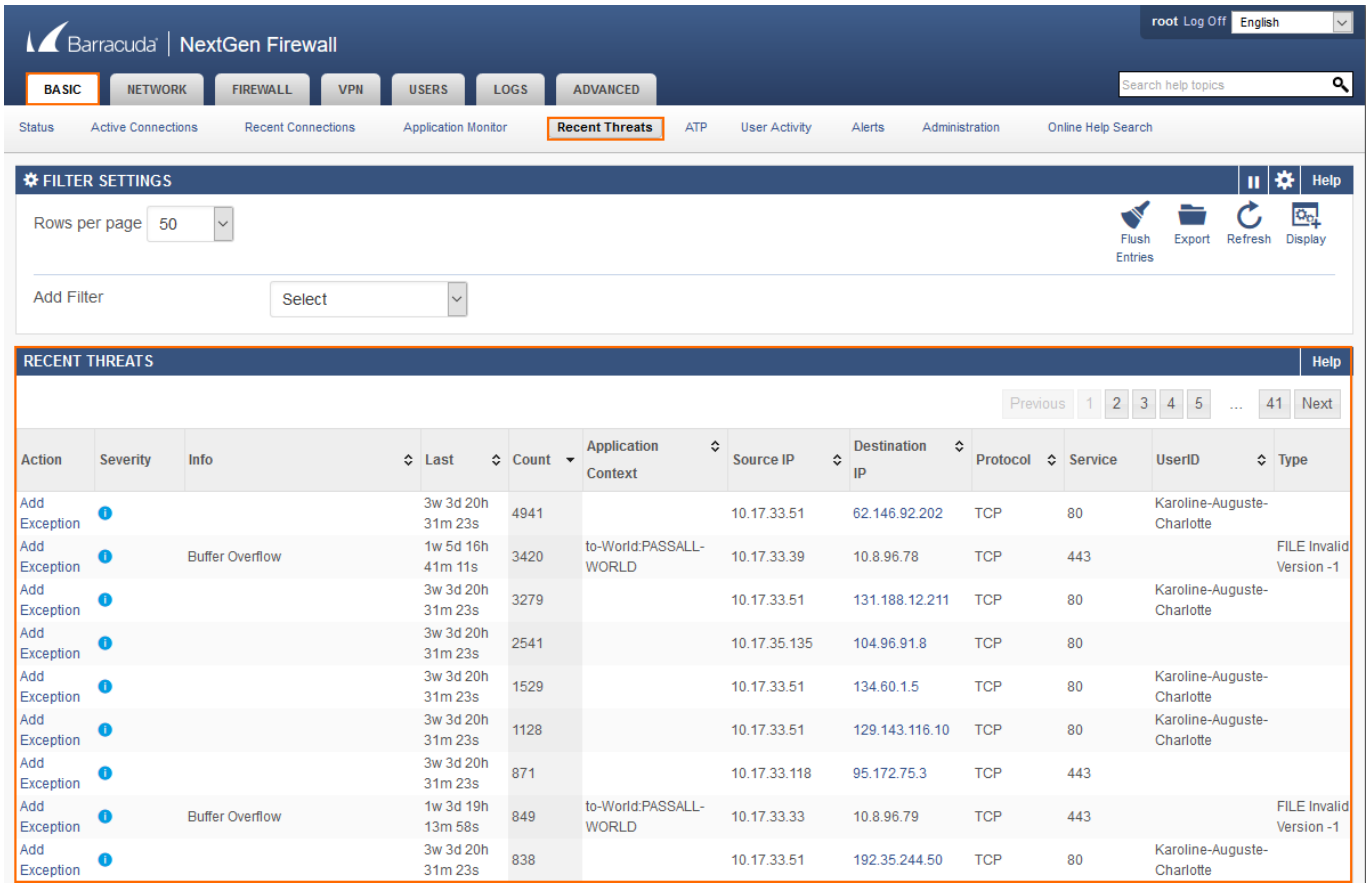
How to Manage Threats

https://campus.barracuda.com/doc/72516499/

Threats that are detected by the IPS engine are listed in the **BASIC > Recent Threats** tab. This table provides detailed information on each detected threat.

Recent Threats Table

In the image below, you can see a list of threats detected by the IPS system of the firewall.



Managing the Recent Threats List

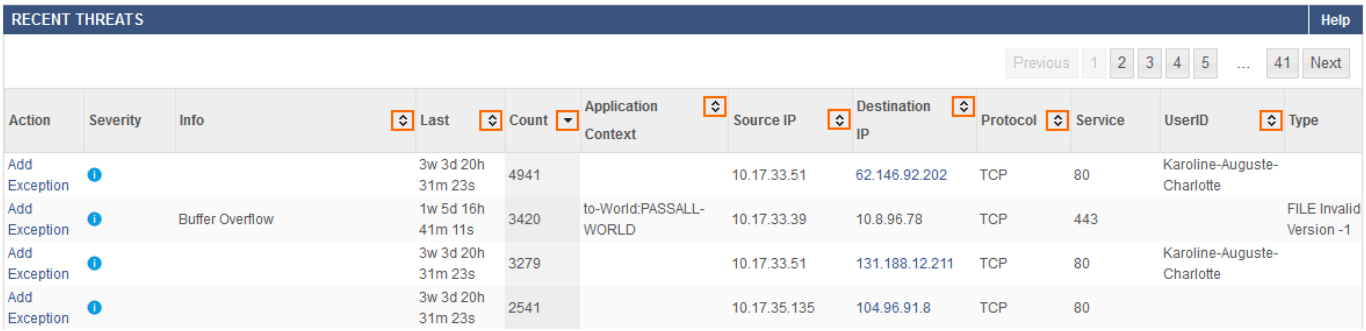
Over time, the list of threats will grow and, therefore, span multiple pages, making it very difficult to keep track of special threats. To provide a better overview, you have the following options:

- Applying a sort filter

- Applying a content filter
- Adding exceptions to a threat

Sort Filter

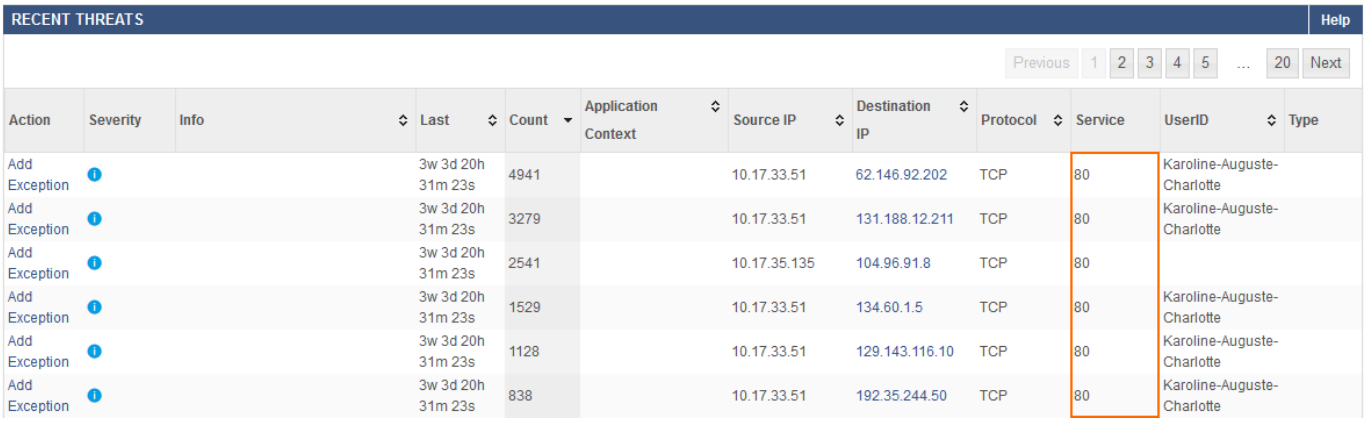
Apply a sort filter if you want to display threats in ascending or descending order. To do so, click either the 'up' or 'down' triangle in one of the column headers.



Content Filter

Apply a content filter if you want to display list entries of only a special type, e.g., only threats relating to service port 80. Double-click the small magnifying glass icon to display only threats that apply to service port 80:

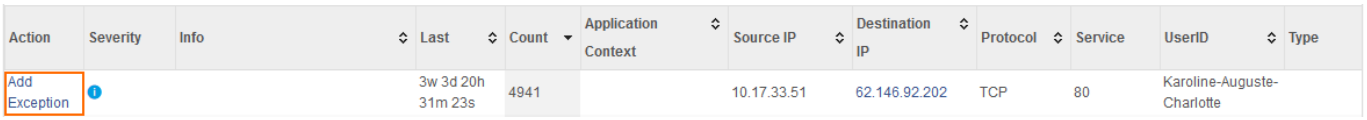
After double-clicking the filter, the firewall displays only threats that apply to service port 80:



To remove the filter, click **X** in the section of the filter settings:

Adding Exceptions to a Threat

Apply an exception if you consider a listed entry not to be a threat and want to exclude it from the threats list. To add an entry to the exceptions, click **Add Exception** in the column of the entry in question:

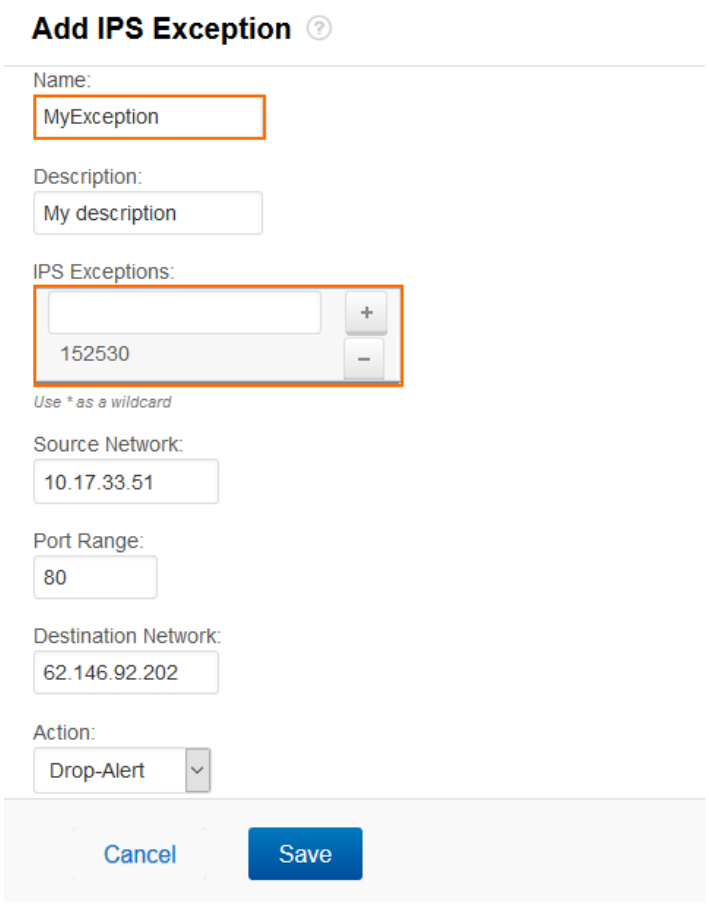


In the **Add IPS Exception** window, configure the exception entry. You will need to fill in the following two fields:

- **Name** — Name for the IPS exception entry.
- **IPS Exceptions** — A list of malware IDs you want to exclude from the threats list.
  To add a specific malware item:
  1. Start typing the numeric ID or the name of the malware.
  2. As you type, a list of matching suggestions is displayed in autocomplete–like style.
  3. If your desired malware appears, click or use **Arrow** and **Enter** keys to select it.
  4. The malware is added as an item to the list and displayed as a combination of ID and name.
  5. Click the **– (Minus)** button next to an item to remove it from the list.

Optional parameters:

- **Description** — Textual description for your IPS exception.
- **Source Network** — The source network of the traffic caused by the malware. Enter an IP address or a subnet in CIDR notation.
- **Port Range** — Single port or port range for this IPS exception.
- **Destination Network** — The destination network of the traffic caused by the malware. Enter an IP address or a subnet in CIDR notation.
- **Action** — The action to be performed if the IPS exception matches. The following actions are available:
  - **Drop-Alert** — Drops the traffic and generates an alert. Default.
  - **Drop-Warn** — Drops the traffic and generates a warning.
  - **Drop** — Silently drops the traffic. No notification is generated.
  - **Log-Alert** — Logs the event and generates an alert.
  - **Log-Warn** — Logs the event and generates a warning.
  - **Log** — Logs the event.
  - **None** — No action is performed except for not scanning the traffic.



Click **Save** to save or **Cancel** to discard the changes.

Figures

1. recent_threats.png
2. sort_filter.png
3. apply_content_filter.PNG
4. filter_applied.png
5. remove_filter.png
6. add_exception.png
7. configure_ips_exception.png