

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.

Action	Severity	Info	Last	Count	Application Context	Source IP	Destination IP	Protocol	Service	UserID	Type
Add Exception	ⓘ		3w 3d 20h 31m 23s	4941		10.17.33.51	62.146.92.202	TCP	80	Karoline-Auguste-Charlotte	
Add Exception	ⓘ	Buffer Overflow	1w 5d 16h 41m 11s	3420	to-World:PASSALL-WORLD	10.17.33.39	10.8.96.78	TCP	443		FILE Invalid Version -1
Add Exception	ⓘ		3w 3d 20h 31m 23s	3279		10.17.33.51	131.188.12.211	TCP	80	Karoline-Auguste-Charlotte	
Add Exception	ⓘ		3w 3d 20h 31m 23s	2541		10.17.35.135	104.96.91.8	TCP	80		
Add Exception	ⓘ		3w 3d 20h 31m 23s	1529		10.17.33.51	134.60.1.5	TCP	80	Karoline-Auguste-Charlotte	
Add Exception	ⓘ		3w 3d 20h 31m 23s	1128		10.17.33.51	129.143.116.10	TCP	80	Karoline-Auguste-Charlotte	
Add Exception	ⓘ		3w 3d 20h 31m 23s	871		10.17.33.118	95.172.75.3	TCP	443		
Add Exception	ⓘ	Buffer Overflow	1w 3d 19h 13m 58s	849	to-World:PASSALL-WORLD	10.17.33.33	10.8.96.79	TCP	443		FILE Invalid Version -1
Add Exception	ⓘ		3w 3d 20h 31m 23s	838		10.17.33.51	192.35.244.50	TCP	80	Karoline-Auguste-Charlotte	

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.

RECENT THREATS													Help							
												Previous	1	2	3	4	5	...	41	Next
Action	Severity	Info	Last	Count	Application Context	Source IP	Destination IP	Protocol	Service	UserID	Type									
Add Exception	1		3w 3d 20h 31m 23s	4941		10.17.33.51	62.146.92.202	TCP	80	Karoline-Auguste-Charlotte										
Add Exception	1	Buffer Overflow	1w 5d 16h 41m 11s	3420	to-World:PASSALL-WORLD	10.17.33.39	10.8.96.78	TCP	443		FILE Invalid Version -1									
Add Exception	1		3w 3d 20h 31m 23s	3279		10.17.33.51	131.188.12.211	TCP	80	Karoline-Auguste-Charlotte										
Add Exception	1		3w 3d 20h 31m 23s	2541		10.17.35.135	104.96.91.8	TCP	80											

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:

Action	Severity	Info	Last	Count	Application Context	Source IP	Destination IP	Protocol	Service	UserID	Type	
Add Exception	1		3w 3d 20h 31m 23s	4941		10.17.33.51	62.146.92.202	TCP	80	Karoline-Auguste-Charlotte		
Add Exception	1	Buffer Overflow	1w 5d 16h 41m 11s	3420	to-World:PASSALL-WORLD	10.17.33.39	10.8.96.78	TCP	443		FILE Invalid Version -1	

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

RECENT THREATS												Help							
											Previous	1	2	3	4	5	...	20	Next
Action	Severity	Info	Last	Count	Application Context	Source IP	Destination IP	Protocol	Service	UserID	Type								
Add Exception	🟡		3w 3d 20h 31m 23s	4941		10.17.33.51	62.146.92.202	TCP	80	Karoline-Auguste-Charlotte									
Add Exception	🟡		3w 3d 20h 31m 23s	3279		10.17.33.51	131.188.12.211	TCP	80	Karoline-Auguste-Charlotte									
Add Exception	🟡		3w 3d 20h 31m 23s	2541		10.17.35.135	104.96.91.8	TCP	80										
Add Exception	🟡		3w 3d 20h 31m 23s	1529		10.17.33.51	134.60.1.5	TCP	80	Karoline-Auguste-Charlotte									
Add Exception	🟡		3w 3d 20h 31m 23s	1128		10.17.33.51	129.143.116.10	TCP	80	Karoline-Auguste-Charlotte									
Add Exception	🟡		3w 3d 20h 31m 23s	838		10.17.33.51	192.35.244.50	TCP	80	Karoline-Auguste-Charlotte									

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

FILTER SETTINGS ⏸ ⚙ Help

Rows per page:

🗑 Flush Entries
📁 Export
🔄 Refresh
🖨 Display

Add Filter:

Service (= 80)

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:

Action	Severity	Info	Last	Count	Application Context	Source IP	Destination IP	Protocol	Service	UserID	Type
Add Exception	🟡		3w 3d 20h 31m 23s	4941		10.17.33.51	62.146.92.202	TCP	80	Karoline-Auguste-Charlotte	

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.

Add IPS Exception ?

Name:

Description:

IPS Exceptions:

*Use * as a wildcard*

Source Network:

Port Range:

Destination Network:

Action:

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

© Barracuda Networks Inc., 2020 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.