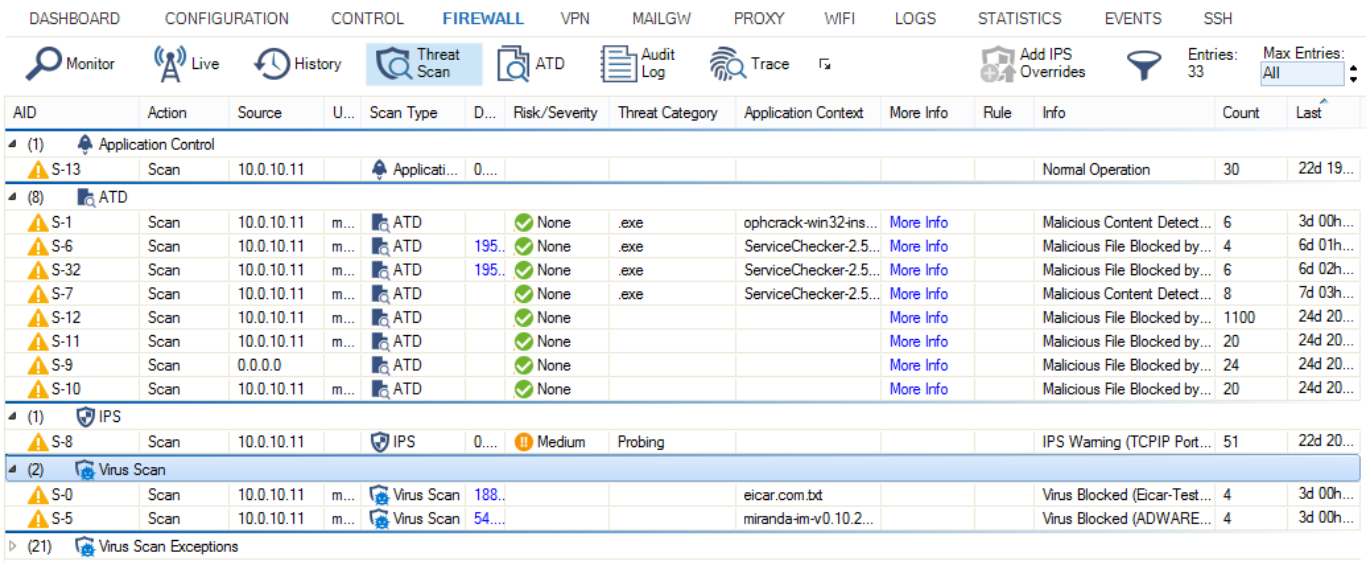
Threat Scan Page

https://campus.barracuda.com/doc/41116060/

The **Threat Scan** page lists all threats that are detected by the Intrusion Prevention System (IPS), the Virus Scanner service, and Advanced Threat Protection (ATP). For information on these features, see: Application Control 2.0. To access the **Threat Scan** page, open the **Firewall** tab and select the **Threat Scan** icon.



Information Display

The information on the **Threat Scan** page is listed according to the security features (e.g., IPS, ATP, Virus Scanner service etc...) that are enabled on the Barracuda NG Firewall. The columns display the following details:

- **AID** – Displays the application ID.
- **Action** – The action performed by the IPS engine.
- **Scan Type** – The scan type.
- **Org** – The origin of the session.
- **Scan Result** – The scan result.
- **IPS Severity** – The event severity.
- **IPS Category** – The event category.
- **Ref/CVE** – Displays the reference.
- **Info** – Additional information (for example: IPS Warning).
- **Rule** – The affected firewall rule.
- **Affected Operating System** – The affected system.
- **Count** – Displays the count.
- **Last** – The last access time (h/m/s).

- **IP Proto** – The IP protocol.
- **Port** – The affected port.
- **Service** – The affected service.
- **Source** – Displays the affected source IP address.
- **Destination** – Displays the affected destination IP address.
- **User** – The affected user.
- **Interface** – The affected interface.
- **MAC** – The MAC address of the affected system.
- **Src / Dst NAT** – Displays the source / destination NAT address.
- **Output-IF** – The output Interface.
- **OutRoute** – Displays the routing details.
- **Next Hop** – Displays the next hop address.
- **IPS Rule Id** – The ID of the IPS rule.
- **URL Category** – Displays the URL category.

Status Icons

The status of firewall connections is indicated by the following icons:

New Icon	Old Icon	Description
		Allow
		Block
		Fail (audit Log) Warning/Scan (History Threat Scan)
		Drop
		Box Selected (audit Log)
		IPS Severity
		Threat Type = App Ctrl
		Threat Type = Virus Scan
		Threat Type = IPS

Available Filter Options

To create a filter, click the arrow icon next to the **Traffic Selection** section to expand the dropdown list and select the required checkboxes:

- **Forward** – Displays the traffic on the Forwarding Firewall.
- **Loopback** – Traffic over the loopback interface.

- **Local In** – Displays the incoming traffic on the box firewall.
- **Local Out** – Displays the outgoing traffic from the box firewall.
- **IPv6** – IPv6 traffic.

To define filters for specific properties, click the **+** icon.

Figures

1. threat_scan.png
2. allow.png
3. allow_old.png
4. block.png
5. block_old.png
6. fail.png
7. fail_old.png
8. drop.png
9. drop_old.png
10. select.png
11. select_old.png
12. ips_sev.png
13. ips_sev_old.png
14. app1.png
15. app1_old.png
16. appctrl.png
17. appctrl_old.png
18. ips.png
19. ips_old.png