

## Threat Scan Page

<https://campus.barracuda.com/doc/46209231/>

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](#). To access the **Threat Scan** page, open the **FIREWALL** tab and select the **Threat Scan** icon.

AID	Action	Source	U...	Scan Type	D...	Risk/Severity	Threat Category	Application Context	More Info	Rule	Info	Count	Last
DASHBOARD CONFIGURATION CONTROL <b>FIREWALL</b> VPN MAILGW PROXY WIFI LOGS STATISTICS EVENTS SSH													
Monitor Live History Threat Scan ATP Audit Log Trace Add IPS Overrides Entries: 33 Max Entries: All													
(1) Application Control													
S-13	Scan	10.0.10.11		Applicati...	0...						Normal Operation	30	22d 19...
(8) ATP													
S-1	Scan	10.0.10.11	m...	ATD		None	.exe	ophcrack-win32-ins...	More Info		Malicious Content Detect...	6	3d 00h...
S-6	Scan	10.0.10.11	m...	ATD	195..	None	.exe	ServiceChecker-2.5...	More Info		Malicious File Blocked by...	4	6d 01h...
S-32	Scan	10.0.10.11	m...	ATD	195..	None	.exe	ServiceChecker-2.5...	More Info		Malicious File Blocked by...	6	6d 02h...
S-7	Scan	10.0.10.11	m...	ATD		None	.exe	ServiceChecker-2.5...	More Info		Malicious Content Detect...	8	7d 03h...
S-12	Scan	10.0.10.11	m...	ATD		None			More Info		Malicious File Blocked by...	1100	24d 20...
S-11	Scan	10.0.10.11	m...	ATD		None			More Info		Malicious File Blocked by...	20	24d 20...
S-9	Scan	0.0.0.0		ATD		None			More Info		Malicious File Blocked by...	24	24d 20...
S-10	Scan	10.0.10.11	m...	ATD		None			More Info		Malicious File Blocked by...	20	24d 20...
(1) IPS													
S-8	Scan	10.0.10.11		IPS	0...	Medium	Probing				IPS Warning (TCP/IP Port...	51	22d 20...
(2) Virus Scan													
S-0	Scan	10.0.10.11	m...	Virus Scan	188..			eicar.com.bt			Virus Blocked (Eicar-Test...	4	3d 00h...
S-5	Scan	10.0.10.11	m...	Virus Scan	54...			miranda-im-v0.10.2...			Virus Blocked (ADWARE...	4	3d 00h...
(21) Virus Scan Exceptions													

## 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 NextGen Firewall F-Series. 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

© Barracuda Networks Inc., 2019 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.