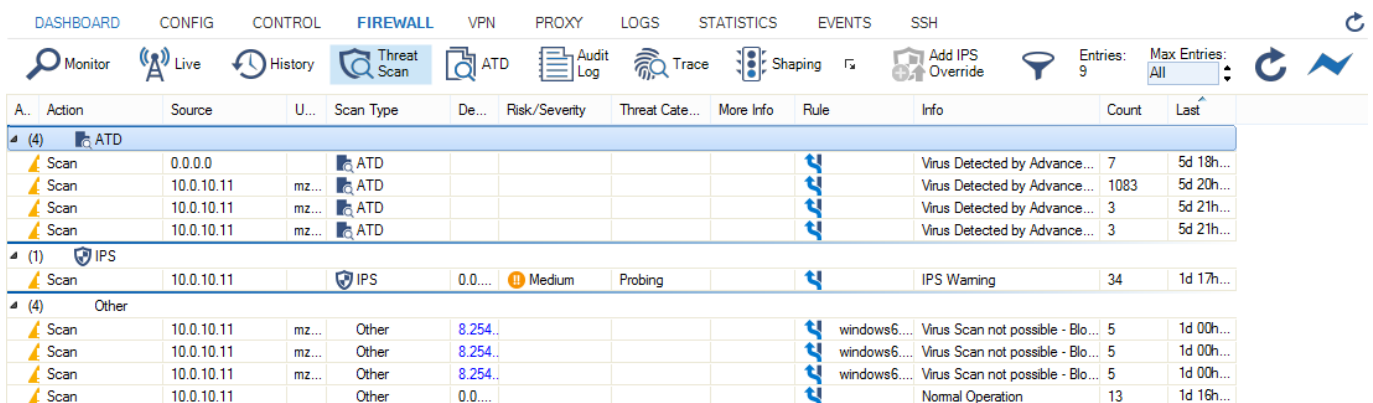


How to Manage Threats

<https://campus.barracuda.com/doc/48202703/>

Threats that are detected by the IPS engine are listed in the **Threat Scan** tab of the **FIREWALL** page of the NextGen Firewall F-Series. This user interface provides a detailed view of information to each detected threat.

Firewall Threat Scan Interface



A.	Action	Source	U...	Scan Type	De...	Risk/Severity	Threat Cate...	More Info	Rule	Info	Count	Last
(4) ATD												
	Scan	0.0.0.0		ATD						Virus Detected by Advance...	7	5d 18h...
	Scan	10.0.10.11	mz...	ATD						Virus Detected by Advance...	1083	5d 20h...
	Scan	10.0.10.11	mz...	ATD						Virus Detected by Advance...	3	5d 21h...
	Scan	10.0.10.11	mz...	ATD						Virus Detected by Advance...	3	5d 21h...
(1) IPS												
	Scan	10.0.10.11		IPS	0.0...	Medium	Probing			IPS Warning	34	1d 17h...
(4) Other												
	Scan	10.0.10.11	mz...	Other	8.254..				windows6...	Virus Scan not possible - Blo...	5	1d 00h...
	Scan	10.0.10.11	mz...	Other	8.254..				windows6...	Virus Scan not possible - Blo...	5	1d 00h...
	Scan	10.0.10.11	mz...	Other	8.254..				windows6...	Virus Scan not possible - Blo...	5	1d 00h...
	Scan	10.0.10.11		Other	0.0...					Normal Operation	13	1d 16h...

The **Threat Scan** interface can also be used to detect and manage false positives. If one of the entries listed was detected as malicious but should be allowed instead,

1. Select the desired entry.
2. Select **Add IPS Overrides** in the upper bar.
3. In the **False Positive** interface, click **Send Changes** and **Activate**.

The entries are added to the IPS False Positives list of the firewalls and, if present, also to the Control Center. Entries added to the IPS False Positive list will automatically get the **None** action and can be edited in the **IPS False Positive** interface.

IPS Exceptions

With IPS enabled, it may happen that the engine detects network traffic that seems to be suspicious, but in special circumstances needs to be allowed by the system administrator. To manage these threats, proceed as follows:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > IPS Exception Database**.

2. Click **Lock**.

DASHBOARD **CONFIG** CONTROL FIREWALL VPN PROXY LOGS STATISTICS EVENTS SSH

Simple Config Config Tree IPS Exception Database - X (ATDFW (Firewall)) State Info Activate Undo Disconnect

IPS Exception Database Discard Lock Send Changes Im/Export

False Positives from Threat Scan: Import Remo...

Name	IPS Si...	IPS Signature	Source	Port	Destination	Action	Comment
From Scan Cache	5000...	DNS Blacklist	10.0.10.110	57524	10.0.11.92	→ None	added on 16.09...
From Scan Cache	5000...	DNS Blacklist	10.0.10.110	36549	10.0.11.92	→ None	added on 16.09...

By selecting an entry, further modifications can be done by simply clicking the desired cell in the table. To extend a matching policy it is possible to enter * (ALL) in the columns **IPS Signature ID**, **Source**, **Port** and **Destination**. A blank cell represents * (All). It is also possible to manually create or copy false positives entries. To do so, click **Add** to create a new entry and configure as desired.

Figures

1. threat_scan.png
2. f_pos.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.