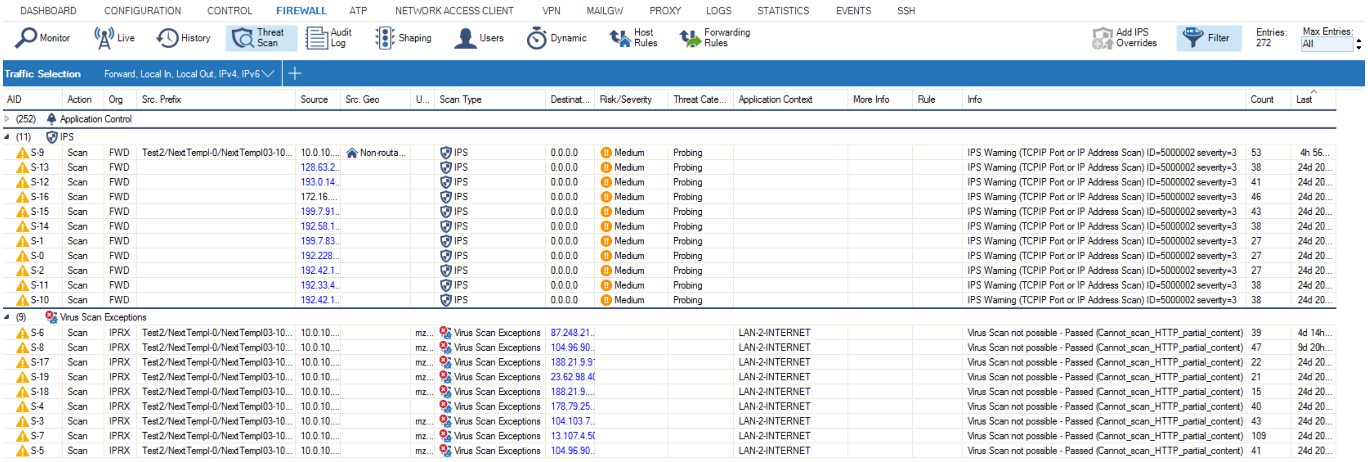
How to Manage Threats

https://campus.barracuda.com/doc/79462946/

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

Firewall Threat Scan Interface



Entries: 272
Max Entries: All

Traffic Selection: Forward, Local In, Local Out, IPv4, IPv6

AID	Action	Org	Src. Prefix	Source	Src. Geo	U...	Scan Type	Destinat...	Risk/Severity	Threat Cate...	Application Context	More Info	Rule	Info	Count	Last
(252) Application Control																
(11) IPS																
S-9	Scan	FWD	Test2/NextTempl-0/NextTempl03-10...	10.0.10....	Non-routa...		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	53	4h 56...
S-13	Scan	FWD		128.63.2..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	38	24d 20...
S-12	Scan	FWD		193.0.14..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	41	24d 20...
S-16	Scan	FWD		172.16....			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	46	24d 20...
S-15	Scan	FWD		199.7.91..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	43	24d 20...
S-14	Scan	FWD		192.58.1..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	38	24d 20...
S-1	Scan	FWD		199.7.83..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	27	24d 20...
S-0	Scan	FWD		192.228...			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	27	24d 20...
S-2	Scan	FWD		192.42.1..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	27	24d 20...
S-11	Scan	FWD		192.33.4..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	38	24d 20...
S-10	Scan	FWD		192.42.1..			IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3	38	24d 20...
(9) Virus Scan Exceptions																
S-6	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	87.248.21..			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	39	4d 14h...
S-8	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	104.96.90..			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	47	9d 20h...
S-17	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	188.21.9.9			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	22	24d 20...
S-19	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	23.62.98.4			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	21	24d 20...
S-18	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	188.21.9....			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	15	24d 20...
S-4	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....			Virus Scan Exceptions	178.79.25..			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	40	24d 20...
S-3	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	104.103.7..			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	43	24d 20...
S-7	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	13.107.4.5			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	109	24d 20...
S-5	Scan	IPRX	Test2/NextTempl-0/NextTempl03-10...	10.0.10....		mz...	Virus Scan Exceptions	104.96.90..			LAN-2-INTERNET			Virus Scan not possible - Passed (Cannot_scan_HTTP_partial_content)	41	24d 20...

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,

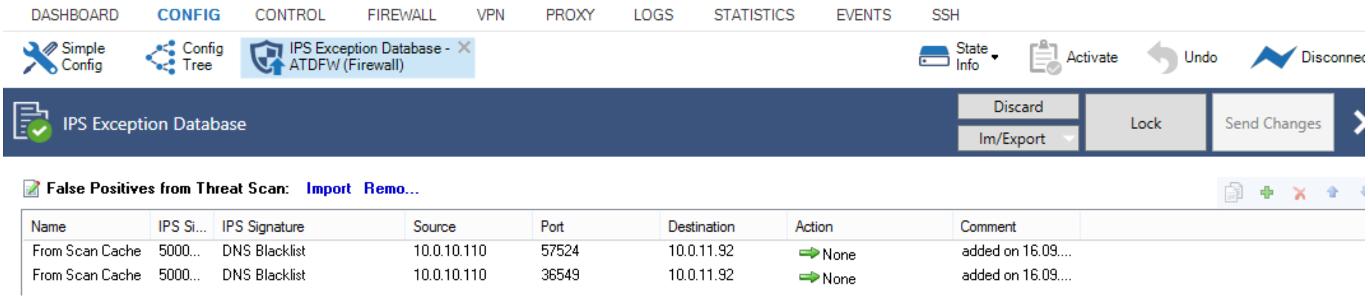
1. Select the desired entry.
2. Select **Add IPS Overrides** in the upper bar.
3. In the **False Positive** interface, click **Send Changes** and **Activate** .

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 Tr ee > Box > Assigned Services > Firewall > IPS Exception Database** .
2. Click **Lock**.



False Positives from Threat Scan:

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., 2024 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.