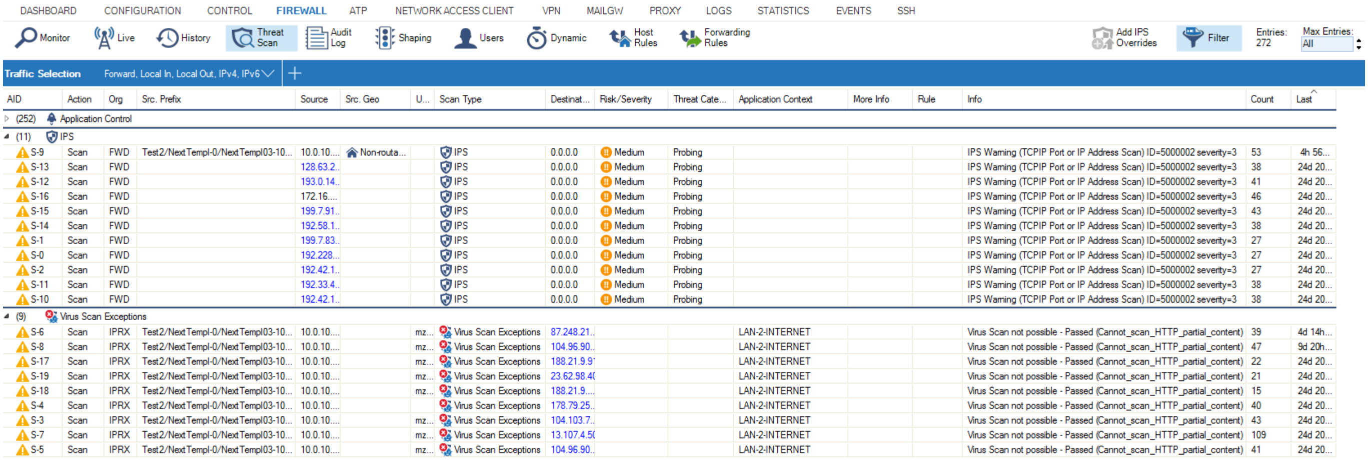
Threat Scan Page

https://campus.barracuda.com/doc/79463240/

The **Threat Scan** page lists all threats 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, click the **FIREWALL** tab and select the **Threat Scan** icon.



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 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 firewall.

The columns display the following details:

- AID – The application ID.
- **Action** – The action performed by the IPS engine.
- **Scan Type** – The scan type.
- **Org** – The origin of the session.
- **Application** – The affected application.
- **Protocol** – The protocol used by the session.
- **Application Context** – The application context.
- **Risk/Severity** – The event severity.
- **Threat Category** – The event category.
- **Info** – Additional information (for example: IPS Warning).
- **Rule** – The affected firewall rule.
- **Affected Operating System** – The affected system.
- **Count** – Displays the count.
- **Last** – The time (h/m/s) of the last access.
- **IP Proto** – The IP protocol.
- **Port** – The affected port.
- **Source** – The affected source IP address.
- **Destination** – The affected destination IP address.

- **User** – The affected user.
- **Interface** – The affected interface.
- **MAC** – The MAC address of the affected system.
- **Src / Dst NAT** – The source / destination NAT address.
- **Output-IF** – The output interface.
- **OutRoute** – The routing details.
- **Next Hop** – The next hop address.
- **URL Category** – The URL category.
- **Src / Dst Geo** – Displays the source / destination geolocation.
- **Src / Dst Prefix** – Displays the source / destination prefix.
- **More Info** – Displays additional information.

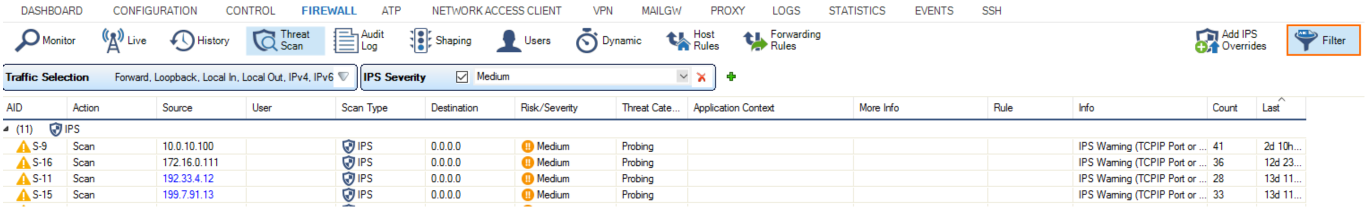
Status Icons

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

Icon	Description
✓	Allow
🚫	Block
⚠	Fail (audit Log) Warning/Scan (History Threat Scan)
🚫⚠	Drop
✅	Box Selected (audit Log)
i ! !! !!! ⚡	IPS Severity
🔔	Threat Type = App Ctrl
🐞	Threat Type = Virus Scan
🛡	Threat Type = IPS

Filter Options

Use the filtering functions on the **Threat Scan** page to display specific entries.



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

IPS Severity ☑ Medium

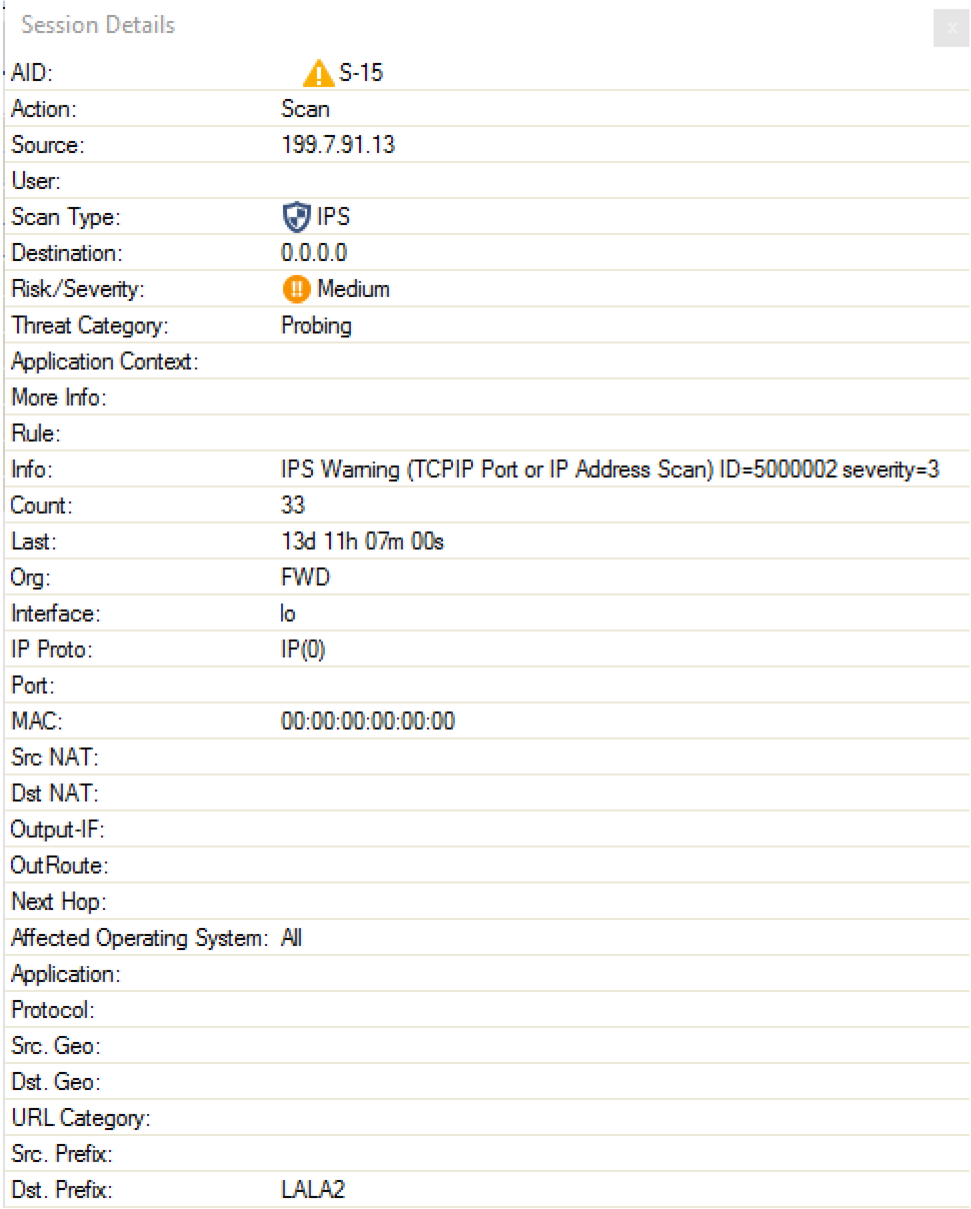
◢ (11) IPS

AID	Action	Source	User	Scan Type	Destination	Risk/Severity	Threat Cate...	Application Context	More Info	Rule	Info	Count	Last
⚠ S-9	Scan	10.0.10.100		IPS	0.0.0.0	!! Medium	Probing				IPS Warning (TCPIP Port or ...	41	2d 10h...
⚠ S-16	Scan	172.16.0.111		IPS	0.0.0.0	!! Medium	Probing				IPS Warning (TCPIP Port or ...	36	12d 23...
⚠ S-11	Scan	192.33.4.12		IPS	0.0.0.0	!! Medium	Probing				IPS Warning (TCPIP Port or ...	28	13d 11...
⚠ S-15	Scan	199.7.91.13		IPS	0.0.0.0	!! Medium	Probing				IPS Warning (TCPIP Port or ...	33	13d 11...

1. Click the **Filter** icon on the top right of the ribbon bar. The **Traffic Selection** section opens on top of the list.
2. Expand the **Traffic Selection** drop-down menu and select the required check boxes:
    - **Forward** – The traffic on the Forwarding Firewall.
    - **Loopback** – The traffic over the loopback interface.
    - **Local In** – The incoming traffic on the box firewall.
    - **Local Out** – The outgoing traffic from the box firewall.
    - **IPv6** – IPv6 traffic.
3. To define filters for specific properties:
    1. Click the **+** icon.
    2. Select the required criteria.
    3. Select or enter the value in the blank field.

Managing Threats Information

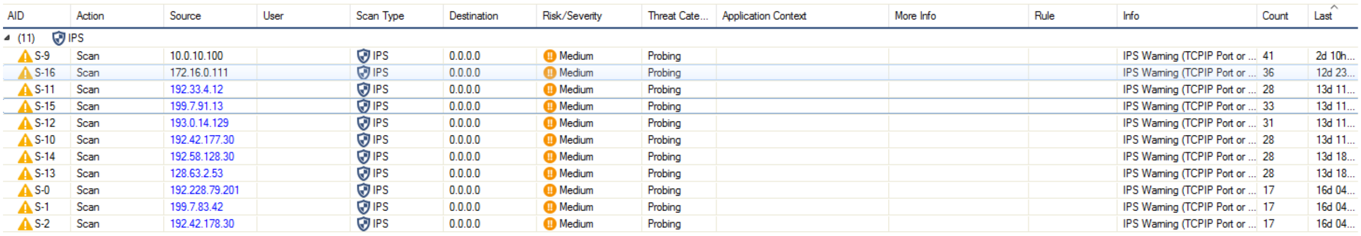
To view detailed information for a threat entry, double-click it. The **Session Details** window displays the ID, action, source, scan type, and destination of the threat.



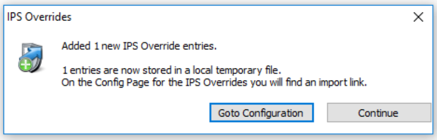
Session Details

AID:	S-15
Action:	Scan
Source:	199.7.91.13
User:	
Scan Type:	IPS
Destination:	0.0.0.0
Risk/Severity:	Medium
Threat Category:	Probing
Application Context:	
More Info:	
Rule:	
Info:	IPS Warning (TCPIP Port or IP Address Scan) ID=5000002 severity=3
Count:	33
Last:	13d 11h 07m 00s
Org:	FWD
Interface:	lo
IP Proto:	IP(0)
Port:	
MAC:	00:00:00:00:00:00
Src NAT:	
Dst NAT:	
Output-IF:	
OutRoute:	
Next Hop:	
Affected Operating System:	All
Application:	
Protocol:	
Src. Geo:	
Dst. Geo:	
URL Category:	
Src. Prefix:	
Dst. Prefix:	LALA2

To add IPS Override entries, click the **Add IPS Overrides** icon next to the filter on the top right of the ribbon bar. Entries will be stored in the configuration.



AID	Action	Source	User	Scan Type	Destination	Risk/Severity	Threat Cate...	Application Context	More Info	Rule	Info	Count	Last
(11) IPS													
S-9	Scan	10.0.10.100		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	41	2d 10h...
S-16	Scan	172.16.0.111		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	36	12d 23...
S-11	Scan	192.33.4.12		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	28	13d 11...
S-15	Scan	199.7.91.13		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	33	13d 11...
S-12	Scan	193.0.14.129		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	31	13d 11...
S-10	Scan	192.42.177.30		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	28	13d 11...
S-14	Scan	192.58.128.30		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	28	13d 18...
S-13	Scan	128.63.2.53		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	28	13d 18...
S-0	Scan	192.228.79.201		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	17	16d 04...
S-1	Scan	199.7.83.42		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	17	16d 04...
S-2	Scan	192.42.178.30		IPS	0.0.0.0	Medium	Probing				IPS Warning (TCPIP Port or ...	17	16d 04...



Added 1 new IPS Override entries.

1 entries are now stored in a local temporary file.
On the Config Page for the IPS Overrides you will find an import link.

To access the IPS Overrides configuration, click **Goto Configuration**. For information on this feature, see: How to Manage Threats.

Figures