

Intrusion Prevention System (IPS)

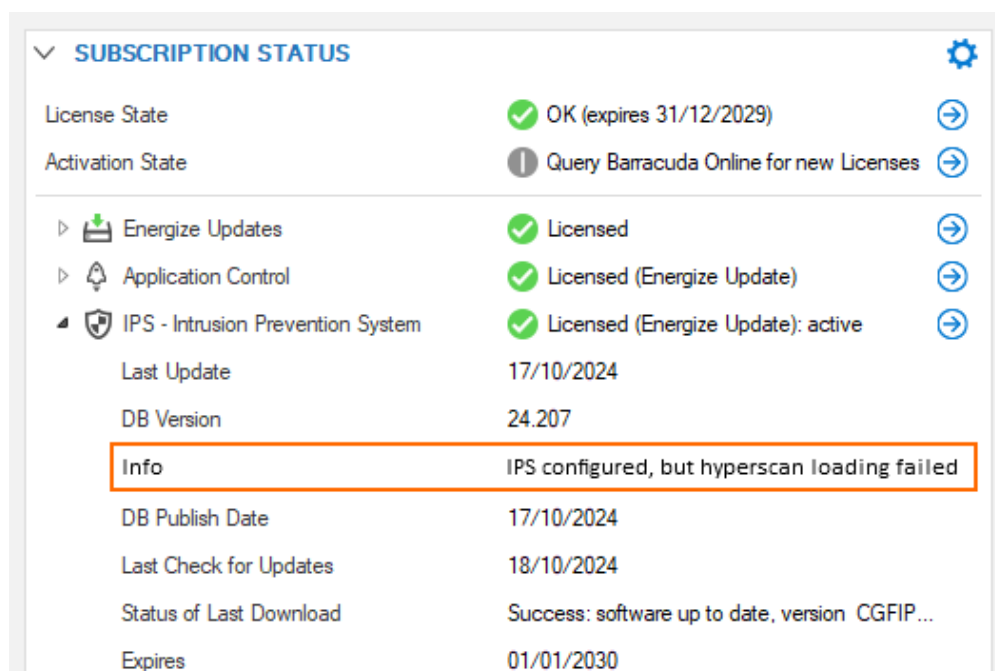
<https://campus.barracuda.com/doc/22910/>

The Intrusion Prevention System (IPS) actively monitors local and forwarding traffic for malicious activities and can also block suspicious traffic. The IPS engine analyzes the network traffic and continuously compares the bitstream with its internal signatures database for malicious code patterns. You can create, edit, and override the default and custom IPS signature handling policies. After configuring your IPS policies, you can also apply them to your access rules. IPS policies are based on SNORT rules.

Prerequisite for Running IPS (Only relevant for virtual systems)

IPS requires large amounts of data to be scanned in a very short time period. To do so, the CPU must support the SSE4.2 instruction set. If this instruction set is present in your firewall's CPU, and your firewall is licensed, IPS will work as expected.

However, if this instruction set is not present, and even if IPS is licensed, the IPS module cannot be loaded and thus will not work. This will also be displayed in the **Status Map** of the CC and in the **SUBSCRIPTION STATUS** element in the firewall's **DASHBOARD**, as shown in the following screenshot:



SUBSCRIPTION STATUS	
License State	OK (expires 31/12/2029)
Activation State	Query Barracuda Online for new Licenses
Energy Updates	Licensed
Application Control	Licensed (Energize Update)
IPS - Intrusion Prevention System	Licensed (Energize Update): active
Last Update	17/10/2024
DB Version	24.207
Info	IPS configured, but hyperscan loading failed
DB Publish Date	17/10/2024
Last Check for Updates	18/10/2024
Status of Last Download	Success: software up to date, version CGFIP...
Expires	01/01/2030

This is also reported with a corresponding error message in the firewall.log file:

```
16.10.2024 11:43:12 [i] Info firewall: [Request] Configuration: ENABLE IPS
16.10.2024 11:43:12 [!] Error firewall: [Request] Configuration: hyperscan: CPU architecture not supported
16.10.2024 11:43:12 [!] Error firewall: [Request] Configuration: IPS: failed to load hyperscan, IPS not available
16.10.2024 11:43:12 [i] Info firewall: [Request] Configuration: DISABLE IPS
```

There are two possible reasons for this problem:

1. The virtualized CPU does not support the required instruction set (SSE4.2).
2. The hypervisor is not passing through the hyperscan instruction set properly.

If you are unsure of either of the following:

- your firewall's CPU supports the SSE4.2 instruction set
- the hypervisor passes through the instruction set

You can check this via SSH. To do so, perform the following steps:

1. Log into your firewall.
2. Go to **SSH**.
3. Log into **SSH**.
4. Enter the following command into the terminal window: `cat /proc/cpuinfo | grep flags | grep sse4`
5. You will see an output similar to the following:

```
[root@FW:~]# cat /proc/cpuinfo | grep flags | grep sse4
flags               : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc
arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid pni pclmulqdq sse3
fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx
f16c rdrand hypervisor iaht_l1m abm 3dnowprefetch invpcid_single ssbd ibrs ibpb
stibp ibrs_enhanced fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid avx512f
avx512dq rdseed adx smap clflushopt clwb avx512cd avx512bw avx512vl xsaveopt
xsavec xsaves arat pku ospke md_clear flush_l1d arch_capabilities
```

6. If the string **sse4_2** is present, then IPS can be handled by the firewall.

If you see **IPS configured, but hyperscan loading failed** on the firewall's **DASHBOARD**, or if you see **CPU architecture not supported** in the Firewall log, make sure your hypervisor exposes the required CPU flags. For KVM/Proxmox, you must set the **CPU Type** to host in order to pass the required flags.

IPS Features

TCP Stream Reassembly

The firewall engine provides support for TCP Stream Reassembly (SRA). In general, TCP streams are broken into TCP segments that are encapsulated into IP packets. By manipulating how a TCP stream is segmented, it is possible to evade detection, for example, by overwriting a portion of a previous segment within a stream with new data in a subsequent segment. This method allows the hacker to hide or obfuscate the network attack. The firewall engine receives the segments in a TCP conversation, buffers them, and reassembles the segments into a correct stream, for example, by checking for segment overlaps, interleaved duplicate segments, invalid TCP checksums, and so forth. Afterward, the firewall engine passes the reassembled stream to the IPS engine for inspection.

URL Obfuscation

The IPS engine provides various countermeasures to avert possible network attacks based on the following URL encoding techniques:

- Escape encoding (% encoding)
- Microsoft %u encoding
- Path character transformations and expansions (/./ , //, \)
- Premature URL ending
- Long URL
- Fake parameter
- TAB separation
- FTP Evasion

The IPS engine can avert FTP exploits where the attacker tries to evade the IPS by inserting additional spaces and Telnet control sequences in FTP commands.

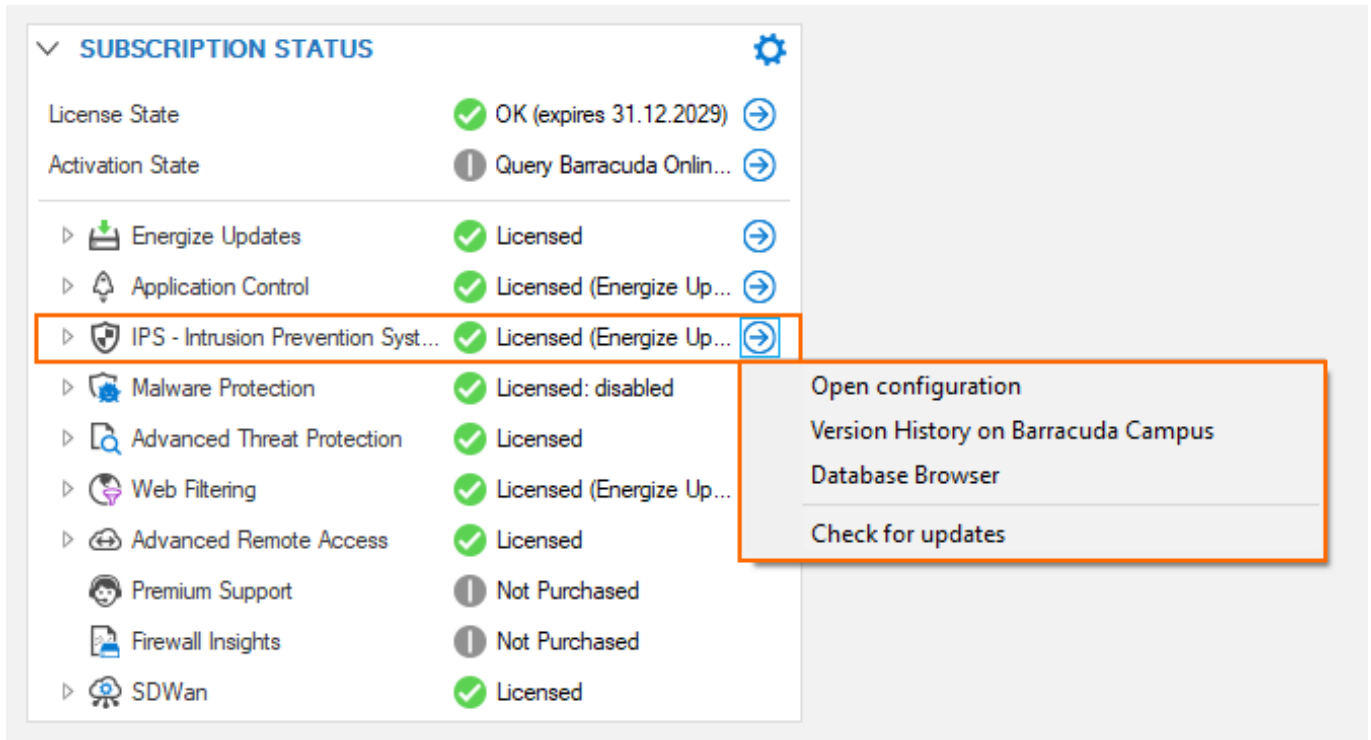
TCP Split Handshake

The IPS engine provides an evasion countermeasure technique that can block the usage of TCP split handshakes attacks. Although the TCP split handshake is a legitimate way to start a TCP connection (RFC793), it can also be used by hackers to execute various network attacks by gaining access to the internal network by way of establishing a trusted IP connection, thereby evading firewall and IPS policies.

IPS in the DASHBOARD

Because the IPS system is part of a subscription license, its status is displayed in the related DASHBOARD element SUBSCRIPTION STATUS. When clicking the blue arrow icon to the right of IPS license status, a menu list displays the available options for IPS. Clicking one of these options will trigger different actions:

- **Open Configuration** - Opens the view for configuring the IPS system.
- **Version History on Barracuda Campus** - Opens a browser window displaying the version history on a Campus web page.
- **Database Browser** - Opens a window that lets you inspect the IPS database.
- **Check for Updates** - Checks for updates.



SUBSCRIPTION STATUS

License State	✓ OK (expires 31.12.2029)	→
Activation State	ⓘ Query Barracuda Onlin...	→
▶ Energize Updates	✓ Licensed	→
▶ Application Control	✓ Licensed (Energize Up...	→
▶ IPS - Intrusion Prevention Syst...	✓ Licensed (Energize Up...	→
▶ Malware Protection	✓ Licensed: disabled	
▶ Advanced Threat Protection	✓ Licensed	
▶ Web Filtering	✓ Licensed (Energize Up...	
▶ Advanced Remote Access	✓ Licensed	
▶ Premium Support	ⓘ Not Purchased	
▶ Firewall Insights	ⓘ Not Purchased	
▶ SDWan	✓ Licensed	

- Open configuration
- Version History on Barracuda Campus
- Database Browser
- Check for updates

Version History on Barracuda Campus

You can inspect a version history on Barracuda Campus by clicking this link:

<https://campus.barracuda.com/to/ipsversions>.

Database Browser

The database browser displays a list of known, common vulnerabilities and exposures (CVEs) that could be or become a threat. The list view provides the option of filtering and searching certain CVEs based on the string which you can enter at the top of a related column category.

IPS Database Browser

Filter	Filter	Filter	Filter	Filter	Filter
ID	Name	Severity	Published	Updated	CVE
5000001	Telnet Escape Sequence in FTP session	Critical	01.01.2000	01.01.2000	
5000002	TCPIP Port or IP Address Scan	Medium	01.01.2000	01.01.2000	
5000003	TCP Segment Overwrite	Critical	01.01.2000	01.01.2000	
5000004	TCP Split Handshake	Critical	01.01.2000	01.01.2000	
5000005	DNS Blacklist	Medium	01.01.2000	01.01.2000	
10004180	HTTP RhinoSoft Serv-U Web Client HTTP Reques...	High	01.11.2009	20.11.2009	CVE-2009-4873
10014431	HTTP chatNow - 'login.php' Cross Site Scripting Vul...	Medium	23.08.2016	14.09.2016	
10014432	HTTP chatNow - 'send_message.php' CSRF Vulne...	High	23.08.2016	14.09.2016	
10014433	HTTP chatNow - 'send_message.php' CSRF Vulne...	High	23.08.2016	14.09.2016	
10014434	HTTP Compal CH7465LG-LC ModemRouter CH74...	High	25.07.2016	14.09.2016	
10014435	HTTP Compal CH7465LG-LC ModemRouter CH74...	High	25.07.2016	14.09.2016	
10014436	HTTP CumulusClips 2.4.1 - Add Admin CSRF (From...	High	07.09.2016	14.09.2016	
10014437	HTTP CumulusClips 2.4.1 - Add Admin CSRF (To S...	High	07.09.2016	14.09.2016	
10014438	HTTP CumulusClips 2.4.1 - 'description' Cross Site ...	Medium	07.09.2016	14.09.2016	
10014439	HTTP CumulusClips 2.4.1 - 'tags' Cross Site Scripting	Medium	07.09.2016	14.09.2016	
10014440	HTTP CumulusClips 2.4.1 - 'title' Cross Site Scripting	Medium	07.09.2016	14.09.2016	
10014441	HTTP Dual DHCP DNS Server 7.29 - Denial of Ser...	High	08.12.2016	08.12.2016	
10014444	HTTP Nagios Log Server 1.4.1 - Security Bypass	Medium	16.08.2016	14.09.2016	
10014445	HTTP NUUO NVRmini 2.3.0.8 - 'address' OS Com...	High	06.08.2016	14.09.2016	

Clicking the tiny blue arrow to the right of a CVE entry makes another list display that contains numerous links that are directly associated with the CVE entry:

IPS Database Browser

Filter	Filter	Filter	Filter	Filter	Filter
ID	Name	Severity	Published	Updated	CVE
5000001	Telnet Escape Sequence in FTP session	Critical	01.01.2000	01.01.2000	
5000002	TCPIP Port or IP Address Scan	Medium	01.01.2000	01.01.2000	
5000003	TCP Segment Overwrite	Critical	01.01.2000	01.01.2000	
5000004	TCP Split Handshake	Critical	01.01.2000	01.01.2000	
5000005	DNS Blacklist	Medium	01.01.2000	01.01.2000	
10004180	HTTP RhinoSoft Serv-U Web Client HTTP Reques...	High	01.11.2009	20.11.2009	http://secunia.com/advisories/37228
10014431	HTTP chatNow - 'login.php' Cross Site Scripting Vul...	Medium	23.08.2016	14.09.2016	http://xforce.iss.net/xforce/xfdb/54081
10014432	HTTP chatNow - 'send_message.php' CSRF Vulne...	High	23.08.2016	14.09.2016	http://www.securityfocus.com/bid/36895/info
10014433	HTTP chatNow - 'send_message.php' CSRF Vulne...	High	23.08.2016	14.09.2016	http://cve.mitre.org/cgi-bin/cvename.cgi?name=2009-4873
10014434	HTTP Compal CH7465LG-LC ModemRouter CH74...	High	25.07.2016	14.09.2016	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4873
10014435	HTTP Compal CH7465LG-LC ModemRouter CH74...	High	25.07.2016	14.09.2016	http://osvdb.org/59772
10014436	HTTP CumulusClips 2.4.1 - Add Admin CSRF (From...	High	07.09.2016	14.09.2016	http://www.securityfocus.com/bid/36895
10014437	HTTP CumulusClips 2.4.1 - Add Admin CSRF (To S...	High	07.09.2016	14.09.2016	http://www.vupen.com/english/advisories/2009/3116
10014438	HTTP CumulusClips 2.4.1 - 'description' Cross Site ...	Medium	07.09.2016	14.09.2016	https://www.us-cert.gov/ncas/bulletins/SB10-152
10014439	HTTP CumulusClips 2.4.1 - 'tags' Cross Site Scripting	Medium	07.09.2016	14.09.2016	https://exchange.xforce.ibmcloud.com/vulnerabilities/54081
10014440	HTTP CumulusClips 2.4.1 - 'title' Cross Site Scripting	Medium	07.09.2016	14.09.2016	
10014441	HTTP Dual DHCP DNS Server 7.29 - Denial of Ser...	High	08.12.2016	08.12.2016	
10014444	HTTP Nagios Log Server 1.4.1 - Security Bypass	Medium	16.08.2016	14.09.2016	
10014445	HTTP NUUO NVRmini 2.3.0.8 - 'address' OS Com...	High	06.08.2016	14.09.2016	

Clicking one of the links opens the favorite browser that will then try to load the associated web page.

IPS in the Configuration Tree

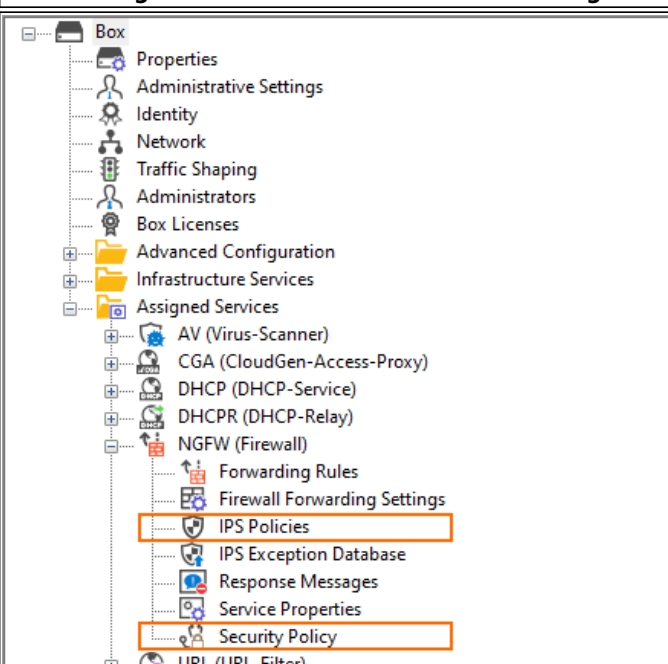
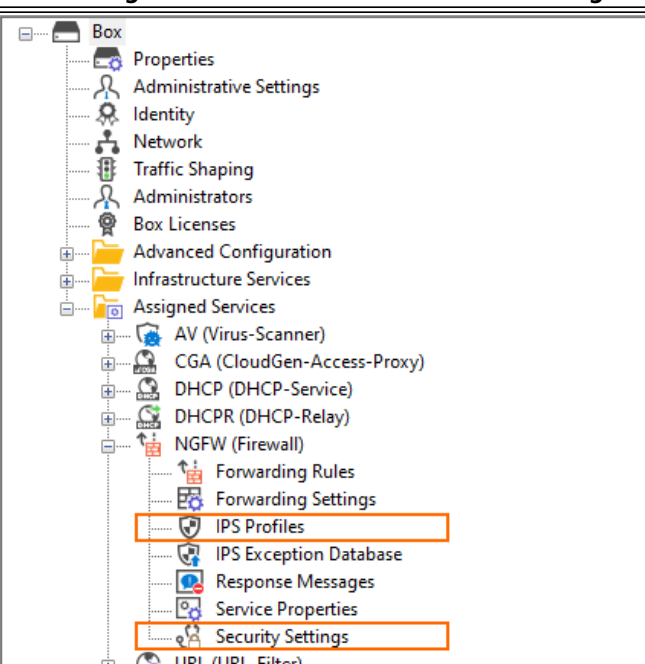
There are 3 special nodes in the configuration tree that are affected by the improvements of firmware 8.3.0.

- IPS Policies
- IPS Exception Database
- Security Policy

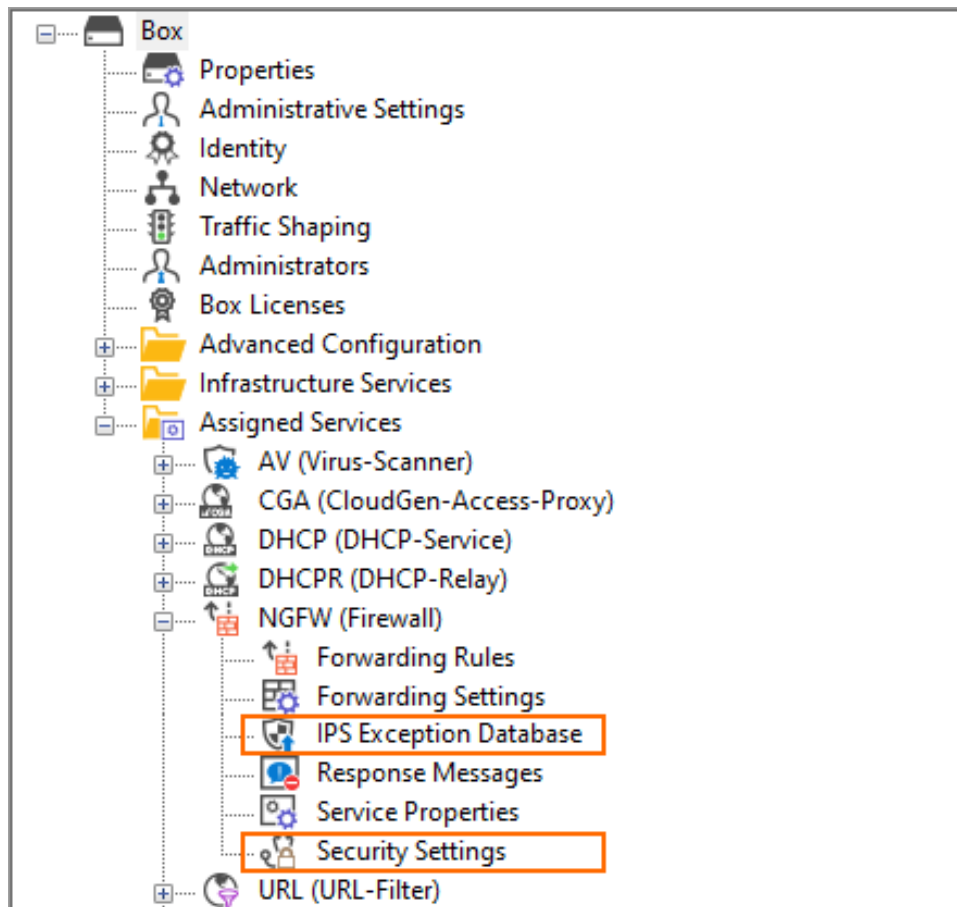
Some of these nodes have been renamed:

Firmware Version	IPS Policies	Security Policy
< 8.3.0 (old naming)	IPS Policies	Security Policy
= 8.3.0 (new naming)	IPS Profiles	Security Settings

Compare the old and new nodes in the configuration tree:

Configuration Tree Nodes with Old Naming	Configuration Tree Nodes with New Naming
 <p>The configuration tree on the left shows the old naming convention. The 'Box' node is expanded, showing a list of nodes. The 'IPS Policies' node is highlighted with an orange box. The 'Security Policy' node is also highlighted with an orange box. Other nodes include Properties, Administrative Settings, Identity, Network, Traffic Shaping, Administrators, Box Licenses, Advanced Configuration, Infrastructure Services, Assigned Services, AV (Virus-Scanner), CGA (CloudGen-Access-Proxy), DHCP (DHCP-Service), DHCP (DHCP-Relay), NGFW (Firewall), Forwarding Rules, Firewall Forwarding Settings, IPS Exception Database, Response Messages, Service Properties, and URL (URL-Filter).</p>	 <p>The configuration tree on the right shows the new naming convention. The 'Box' node is expanded, showing a list of nodes. The 'IPS Profiles' node is highlighted with an orange box. The 'Security Settings' node is also highlighted with an orange box. Other nodes include Properties, Administrative Settings, Identity, Network, Traffic Shaping, Administrators, Box Licenses, Advanced Configuration, Infrastructure Services, Assigned Services, AV (Virus-Scanner), CGA (CloudGen-Access-Proxy), DHCP (DHCP-Service), DHCP (DHCP-Relay), NGFW (Firewall), Forwarding Rules, Forwarding Settings, IPS Exception Database, Response Messages, Service Properties, and URL (URL-Filter).</p>

Because the IPS correlates with the Policy-Profiles feature, the visibility of the IPS Profiles node in the configuration tree depends on the activation status of that feature. If the Policy-Profiles feature is activated, then the node IPS Profiles will disappear in the configuration tree and only the nodes IPS Exception Database and Security Settings will remain visible:



Configuring and Managing IPS

For step-by-step instructions on how to configure and manage IPS, see the following articles:

- [How to Check the IPS Security Subscription Status](#)
- [How to Configure IPS Policies](#)
- [How to Configure the Intrusion Prevention System \(IPS\)](#)
- [How to Manage Threats](#)

Figures

1. IPS_hyperscan_loading_failed_subscription_status.png
2. IPS_hyperscan_loading_failed_error_message_output.png
3. IPS_hyperscan_check_instruction_set.png
4. ips_subscription_status_with_submenu.png
5. ips_data_browser_window.png
6. ips_database_browser_window_with_link_list_for_help.png
7. ips_new_node_naming_old.png
8. ips_new_node_naming_ips_profiles_security_settings.png
9. ips_configuration_tree_with_cgf_policies_enabled.png

© Barracuda Networks Inc., 2025 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.