

Intrusion Prevention System (IPS)

<https://campus.barracuda.com/doc/96026213/>

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.

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.

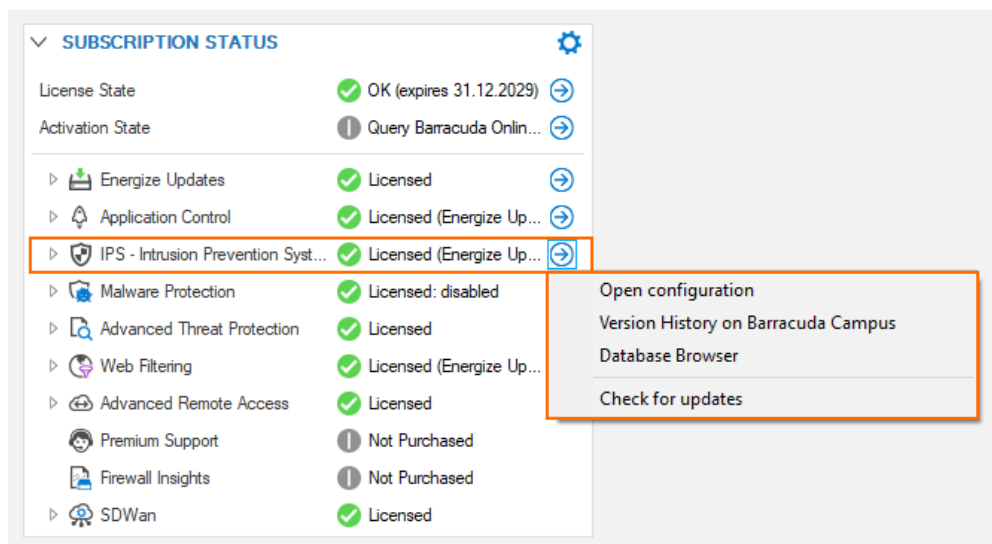
TCP Split Handshake

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.

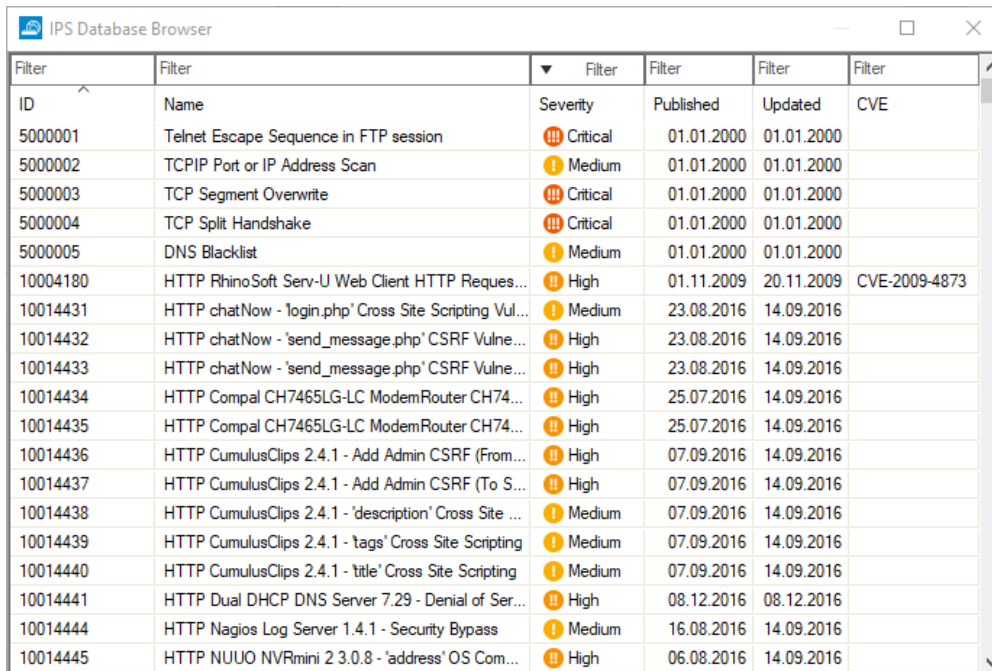


Version History on Barracuda Campus

You can inspect a version history on Barracuda Campus by clicking this link:
<https://campus.barracuda.com/to/ipsversions>.

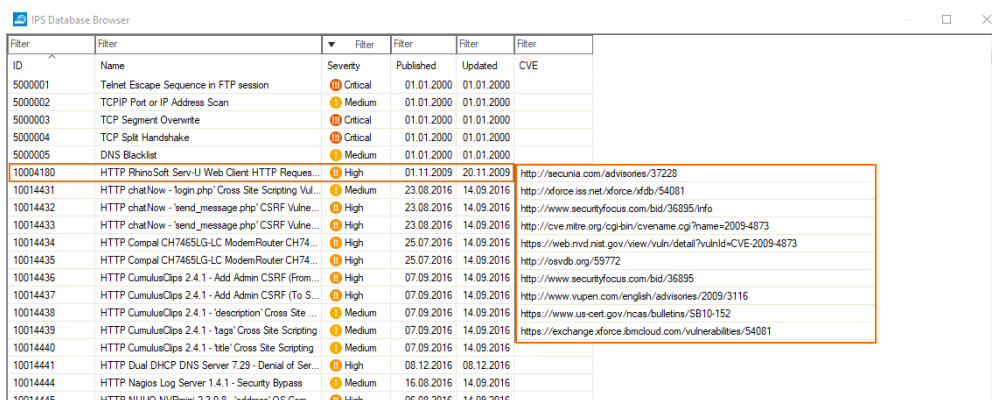
Database Browser

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.



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:



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=CVE-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	https://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

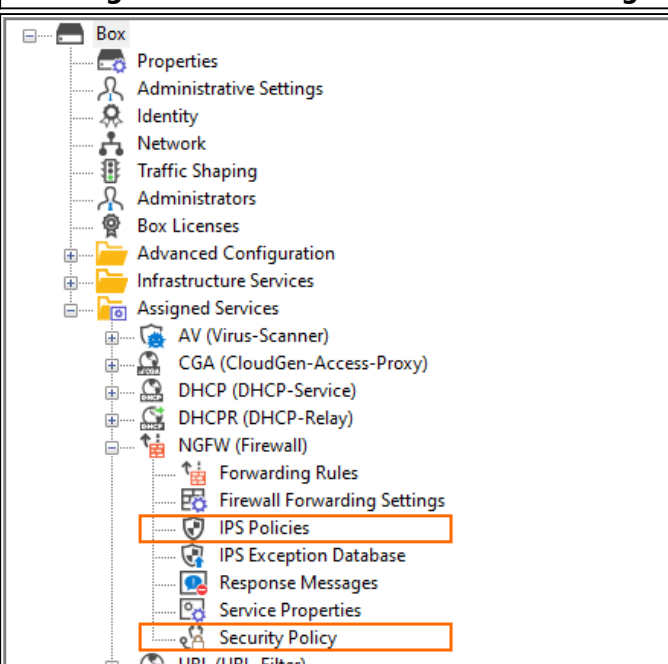
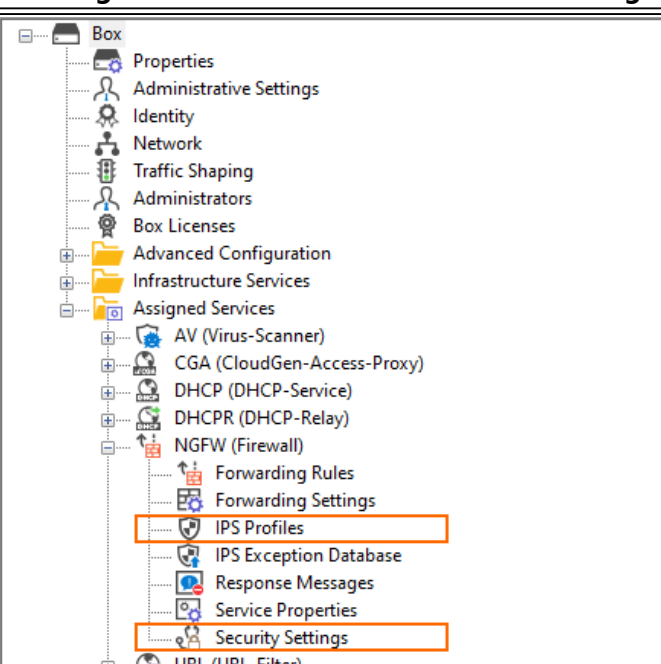
There are 3 special nodes in the configuration tree that are affected by the improvements of firmware 8.3.0.

- IPS Policies
- IPS Exception Database
- Security Policy

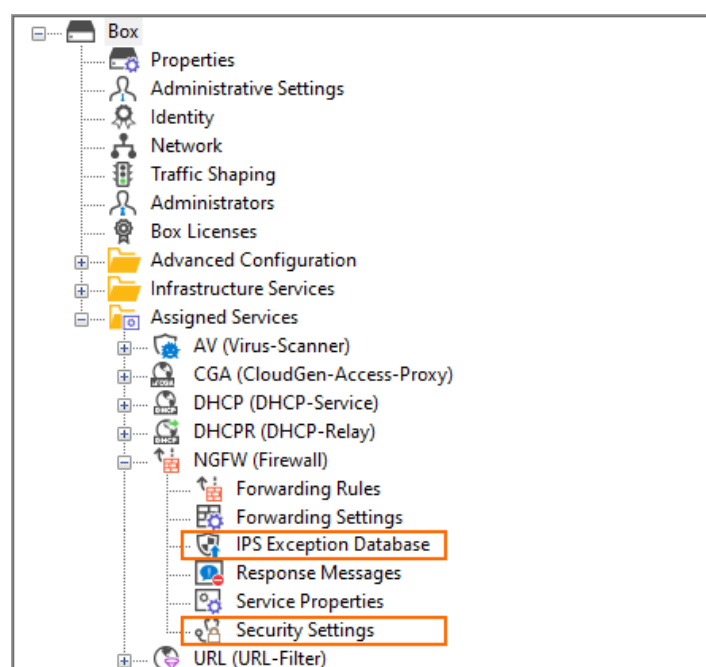
Some of these nodes have been renamed:

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 hierarchy of settings. The 'NGFW (Firewall)' node is expanded, showing 'Forwarding Rules', 'Firewall Forwarding Settings', 'IPS Policies' (highlighted with an orange box), 'IPS Exception Database', 'Response Messages', 'Service Properties', 'Security Policy' (highlighted with an orange box), and 'URL (URL-Filter)'.</p>	 <p>The configuration tree on the right shows the new naming convention. The 'Box' node is expanded, showing a hierarchy of settings. The 'NGFW (Firewall)' node is expanded, showing 'Forwarding Rules', 'Forwarding Settings', 'IPS Profiles' (highlighted with an orange box), 'IPS Exception Database', 'Response Messages', 'Service Properties', 'Security Settings' (highlighted with an orange box), and 'URL (URL-Filter)'.</p>

Because the IPS correlates with the CGF-Policies feature, the visibility of the IPS Profiles node in the configuration tree depends on the activation status of that feature. If the CGF-Policies 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:

Figures

1. ips_subscription_status_with_submenu.png
2. ips_data_browser_window.png
3. ips_database_browser_window_with_link_list_for_help.png
4. ips_new_node_naming_old.png
5. ips_new_node_naming_ips_profiles_security_settings.png
6. ips_configuration_tree_with_cgf_policies_enabled.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.