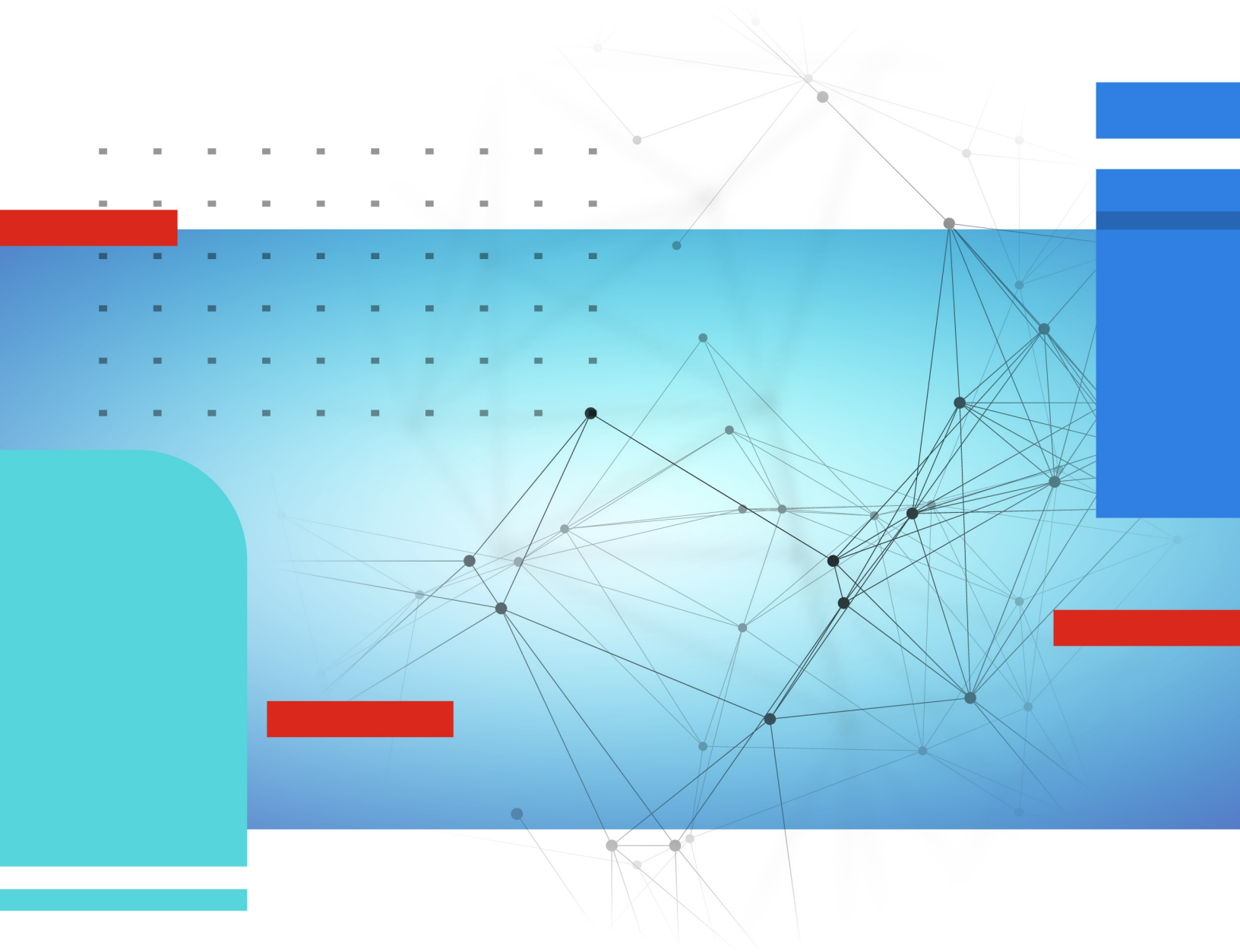
Release Notes

IPS Engine 7.6.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 07, 2025
IPS Engine 7.6.1 Release Notes
43-760-1063743-20250407

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Product integration and support **6**
Resolved issues **7**

Change log

Date	Change description
2024-12-11	Initial release.
2025-04-07	Updated Resolved issues on page 7.

Introduction

This document provides the following information for the Fortinet IPS Engine 7.6.1 build 1026 (7.001026):

- Product integration and support on page 6
- Resolved issues on page 7

IPS Engine 7.6.1 build 1026 is a built-in release for FortiOS 7.6.1. It is not a release to FortiGuard.

For additional FortiOS documentation, see the Fortinet Document Library.

Product integration and support

The following table lists IPS engine product integration and support information:

FortiOS	7.6.1

Resolved issues

The resolved issues listed do not list every bug that has been corrected with this release. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
970013, 1062962	Chrome Beta bypasses Web Filtering in flow mode, which an unsupported SSL session causes.
976702	In a rare situation, enabling IPS may cause throughput to decrease more than expected when used with a virtual wire pair.
977258	ECH-enabled websites fail to load with flow SSL deep inspection.
979200	In policy-based next generation firewall (NGFW) mode, if there is no rule hit in `central-snat` and session never establishes, there is no traffic log.
989005	The DPI SSL profile may interrupt large file downloads due to an issue with TCP packet handling.
990540	FortiGate does not generate traffic logs for established or denied TCP sessions that lack application data.
1004258	Strict-SNI SSL Profile may block TCP connections if the SNI cannot be verified due to an active probe failure.
1011320	Adding File Filter to a flow-based firewall policy may impact performance.
1025114	Insufficient free memory on entry-level FortiGate with 2 GB RAM may cause unexpected behavior in IPS engine.
1030032	Application list parameter table size is limited to 256 entries after upgrade to 7.2.5.
1034646, 1053156	Performance tests done for traffic decryption on 7.4.4 cause memory to enter conserve mode.
1040783	IPS engine session creation time needs improvement when using Application Control unified threat management profile.
1051890	Tunnel session packets may drop in NGFW policy mode due to a rare error condition.
1061343	SSL traffic subjected to DPI may cause certain websites to become inaccessible when SSL plain records are fragmented.
1062204	An unhandled error occurs within the IPS engine application (07.006.1014).
1062677	Security policy matching is incorrect for Fortinet single sign on Citrix groups.
1065116	DNS filter alters the response for non-existent domain for flow mode.
1066441	DAC signatures do not follow priority.
1069190	After upgrade to FortiOS 7.2.9, FortiGate may experience high CPU usage due to IPS engine version 7.00342 when there is a large amount of proxy-inspected traffic via application control and IPS sensor.

Bug ID	Description
	Workaround: downgrade IPS engine to 7.00341.
1069760	Offloaded traffic from unknown applications may match an incorrect firewall policy when the unknown application category is configured as an application group in the security policy.
1072802	Erroneous memory allocation causes memory usage issue in IPS engine.
1073306	ClientKeyExchange message with unexpected value causes rare error condition.
1090134	Updates of `thread-feed` make IPS engine reinitialize.
1092260	Rare condition that QUIC/HTTP3 traffic triggers causes unexpected behavior in IPS engine.
1097642	SSL traffic subjected to DPI may cause certain websites to become inaccessible, resulting in an ERR_SSL_PROTOCOL_ERROR.

www.fortinet.com