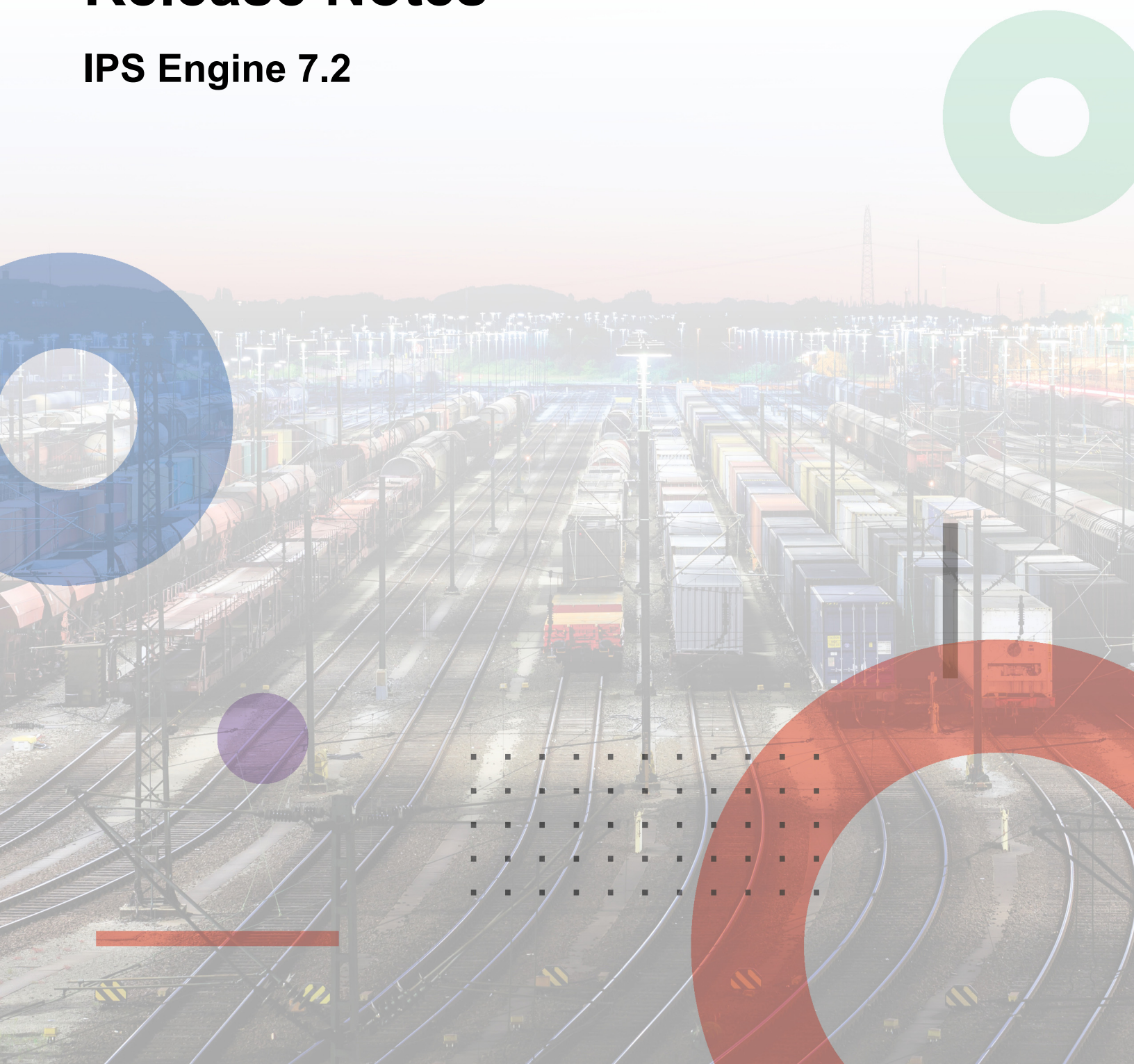
FORTINET

Release Notes

IPS Engine 7.2



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

October 16, 2024
IPS Engine 7.2 Release Notes
43-720-1086921-20241016

TABLE OF CONTENTS

Change log

Date	Change description
2024-10-16	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 7.2 build 349 (7.00349).

IPS Engine 7.2 build 349 is a release to FortiGuard for FortiOS 7.2. It is not a built-in release for FortiOS.

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	7.2

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
723764	A replacement message is not provided to the client when a DPI-enabled proxy mode firewall policy with application control enabled blocks traffic.
875577	Unexpected behavior occurs in IPS engine while processing PDF files.
887299	URL filter incorrectly obstructs traffic. An empty hostname, which matches any entry in the URL filter, causes this.
911118, 940344	Static URL filter may not function as anticipated due to erroneous URL filter matches stemming from TLS probe failures.
923173	IPS engine requires improvements to optimize memory usage when using GRE tunnel.
929019	Unexpected behavior occurs in IPS engine (7.002.314) due to an error case.
929110	The `strict` setting for the `sni-server-cert-check` option is treated the same as `enabled`, and no logs are generated on SNI mismatch with CN/SAN.
932111	IPS engine requires improvements to optimize memory usage due to HTTP2 stream not closing in a timely manner.
932956, 955961	Traffic may continue to flow when only deny security policies are in effect until the Policy Match Engine determines the correct policy to enforce.
941200	DNS translation does not work as anticipated, with FortiGate sending two responses when the web filter cache is enabled.
948186	File Filter does not generate file filter logs while in flow mode.
953382	CPU usage has issue in IPS engine due to database size.
961598	A rare error condition occurs in IPS engine while handling X.509 certificates when the sessions are released for the Quiche server.
964566	Unexpected behavior occurs in IPS Engine (07.002.328) due to a rare condition.
964709	Unexpected behavior occurs in IPS Engine (7.002.329) while processing application control rules.
968367	IPS engine requires improvements to optimize memory usage while inspecting email sessions
970013	Chrome Beta bypasses WebFiltering in flow-mode, which an unsupported SSL session causes.
976433	IPS engine requires improvements to optimize performance when SSL inspection and web filter are enabled. This is in response to Windows 11 and Windows Server 2022 updating

Bug ID	Description
	their TCP window size algorithm.
976702	In a rare situation, enabling IPS may cause throughput to decrease more than expected when used with a virtual wire pair.
982894, 1004084	Erroneous memory allocation occurs in IPS engine while handling DNS traffic.
982987	The engine drops the ClientHello packet in asymmetric flows when the web filter is enabled in a specific scenario.
989005	The DPI SSL profile may interrupt large file downloads due to an issue with TCP packet handling.
992073	Unexpected behavior occurs in IPS Engine (7.002.326) due to a rare condition.
992967	TLS session resumption using session ID does not work when DPI is enabled.
997071	Unexpected behavior occurs in IPS Engine due to an error case.
1005185	Unexpected behavior occurs in IPS Engine (06.004.171) due to an error case that an SSL session with CBC cipher causes.
1006643	Clear static domain list so if session is reused, it does not match incorrectly on static domain list.
1007795	Support zstd content encoding in HTTP traffic.
1008630	TLS active probe fails in a closed network due to lack of routes to remote hosts.
1009871	Memory usage issue that many HTTP/3 sessions cause occurs in the IPS engine.
1025114	Insufficient free memory on entry-level FortiGate devices with 2 GB RAM may cause unexpected behavior in IPS engine.
1030032	The table size of Application List Parameter is limited to 256 entries after upgrade to 7.2.5.
1032532	A high number of IPS sniffer sessions may lead to increased memory usage.
1032643	A rare error condition occurs in IPS engine when performing the SSL deep inspection.
1039549	Custom TLS client stack receiving ServerKeyExchange message with unexpected value causes a rare error condition observed in IPS Engine.
1048289	DNS requests with uppercase characters in the domain name are not blocked when the policy is in flow mode with an external domain threat feed.
1069190	After upgrade to FortiOS 7.2.9, the FortiGate may experience high CPU usage due to IPS engine 7.00342 when there is a large amount of proxy-inspected traffic via application control and IPS sensor. **Workaround**: downgrade IPS engine to 7.00341.
1073306	ClientKeyExchange message with unexpected value causes a rare error condition observed in IPS Engine.
1082748	Unexpected behavior occurs in IPS Engine (07.002.346) due to a rare condition.

Known issues

There are no known issues with this release of IPS engine version 7.2 for FortiOS.

To report a bug, please contact Customer Service & Support.

www.fortinet.com