FORTINET

Release Notes

IPS Engine 8.0

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

May 14, 2026
IPS Engine 8.0 Release Notes
43-800-1198928-20260514

TABLE OF CONTENTS

Change log

Date	Change description
2026-05-14	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 8.0 build 028 (8.0028):

IPS Engine 8.0 build 028 (8.0028) is a built-in release for FortiOS 8.0.0. 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	8.0.0

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
673117	Unexpected behavior occurs when FortiGate processes TFTP protocol data under certain conditions.
764143	SSL version restrictions not enforced in flow mode when using `min-allowed-ssl-version`.
983372, 1252636, 1269354	An error condition occurs in the IPS engine when a plain-text SSL alert is encountered.
1077638, 1129130	In NGFW Policy Mode, FortiGate may incorrectly block packets from established TCP sessions if no matching IPS session exists.
1080003	FGT memory is gradually increasing when FGT Flow AV Profile is inspecting TCP 6200 traffic with outbreak prevention enabled.
1091118, 1170304	Oversized packets exceeding the MTU cause delayed ACKs, leading to unintended behavior
1093769, 1096297	Unexpected IPS UTM logs may be generated in NGFW policy mode for unknown applications.
1094030	URL truncation occurs in logs due to mismatched length limits between FortiOS and IPS Engine.
1094870	FTPS data connections fail to establish when using flow mode firewall policies configured for FTP service.
1098739, 1156979, 1159041	SSL errors occur when accessing certain websites via IPv6 in FortiGate flow mode with SSL inspection enabled.
1107273	New packets on established SCTP sessions are dropped during processing after a four-way handshake when UTM is enabled.
1116052	In some cases, incorrect session blocking may occur when a URL rating query fails during security policy matching in NGFW policy mode.
1117043	Fatal errors occur when the IPS engine sends requests with zero-length data segments to IPSA.
1122188	Internal diagnostic commands fail or delay when ipsmonitor processes each request sequentially due to sequential forwarding to IPS daemon processes.
1131911	Memory usage issue observed in IPS Engine 7.00560 during high SMTP traffic due to improper memory management.
1140846	Unexpected behavior observed in the IPS Engine when handling HTTPS traffic using HTTP/2 in certain configurations.

Bug ID	Description
1144684	High CPU usage occurs when processing multiple RTSP streams due to inefficient resource management by the RTSP decoder.
1150204	File attachment names from naver.com are displayed as 'uploadByXHR' instead of their actual filenames.
1152040	An error condition occurs in custom IPS signature when using --log after upgrade to 7.4.5.
1152384	CPU usage issues observed during intense IPS packet scanning.
1156180	Unexpected behavior observed in the IPS Engine caused by an invalid numeric entity.
1156490	Some traffic may be dropped when inspection mode is proxy with `inspect-all` and `http-policy-redirect` enabled.
1158138, 1158586, 1158993	Some websites may fail to load when the web filter is enabled due to the server setting an initial window size that is too small.
1158524	Unexpected behavior observed in the IPS Engine when a DNS packet matches a policy with DNS Filter and Safe Search enabled.
1159485	Traffic duplication may occur on FortiGate due to retransmission of out-of-sync TCP streams when insecure ciphers are used.
1162794	Unintended behavior occurs in the IPS Engine caused by the SCADA dissector.
1168037, 1169917	Web service may not function as expected in Proxy Mode when Application Control is enabled and the SSL/SSH Inspection profile is configured with `inspect-all certificate-inspection`.
1168879	Dynamic content on webpages failed to load when the proxy layer was enabled specifically when WebFilter Safe Search or Strip-XFF options were active.
1178184	SSL errors occur when accessing a specific website due to an unexpected record type when Web Filtering and DPI are enabled in Flow mode.
1178742	ZTNA destination unreachable in rare cases where `sni-server-cert-check` is enabled on a FortiGate and the SNI field is missing.
1181573	SSL inspection does not correctly add the Authority Key Identifier (AKID) when operating in Flow mode with DPI enabled.
1182461	High memory usage occurs when multiple HTTP2 connections with many open streams are present.
1184183	Duplicated webfilter logs occur when `log-all-url` is enabled in NGFW policy mode, causing redundant entries for each traffic event.
1190395	Intermittent traffic disruption occurs due to an error condition in the IPS Engine caused by a DAC handler issue.
1191598	High CPU usage occurs when HTTP2 connections have a large number of open streams.
1193876	Memory usage issues caused by improper closure of HTTP2 streams.
1197659	An error condition in IPS engine occurs when processing HTTP traffic.

Bug ID	Description
1205692	FTP traffic is blocked when Application Control is enabled over Sock5.
1210836	Conserve mode occurs when IPSEngine memory usage increases due to gradual increase in AnonPages.
1212296	Package downloads may fail when an IPS profile is enabled in flow inspection mode due to an early FIN packet being sent.
1213957	TCP download rate drops when FortiGate uses SSL inspection with an antivirus profile in flow mode.
1216974	Intermittent traffic disruption caused by an error condition in the IPS Engine during hybrid key generation.
1217478	Incomplete IEC 60870-5-104 detection occurs when IPS session is cleared.
1218520	BFD flaps occur due to an error condition in the IPS engine caused by QUIC traffic.
1219051	MSI files may not be blocked by the file filter in flow mode due to improper filename extraction.
1225743	An error condition in IPS Engine occurs when executing ssl_add_defer_log during stress testing.
1229928	Malicious website traffic for non-existent domains is not blocked in flow-based DNS inspection with Redirect to Block Portal.
1229941	In policy-based NGFW mode, webfilter logs may be incorrect for some HTTPS traffic, showing only the host in the URL field or generating multiple logs when FortiGuard rating fails.
1239080	Incorrect session accounting observed in sniffer traffic logs when FortiGate runs in sniffer mode with `ips-sniffer-mode` enabled.
1241179	Video downloads using Wondershare UniConverter stall or stop mid-process when FortiGate's web filter encounters out-of-order packets during transfer.
1249177	CPU usage issue observed in the IPS engine caused by the incorrect detection of unidirectional SMB traffic.
1253472	Unexpected behavior observed in the IPS Engine during HTTP header processing involving buffer edit cases on FortiGate models.
1259235	An error condition in ipsengine occurs during upgrade to 7.4.11.
1260248	Protocol enforcement may fail to block DNS over TCP traffic due to delayed enforcement on port 53.

www.fortinet.com