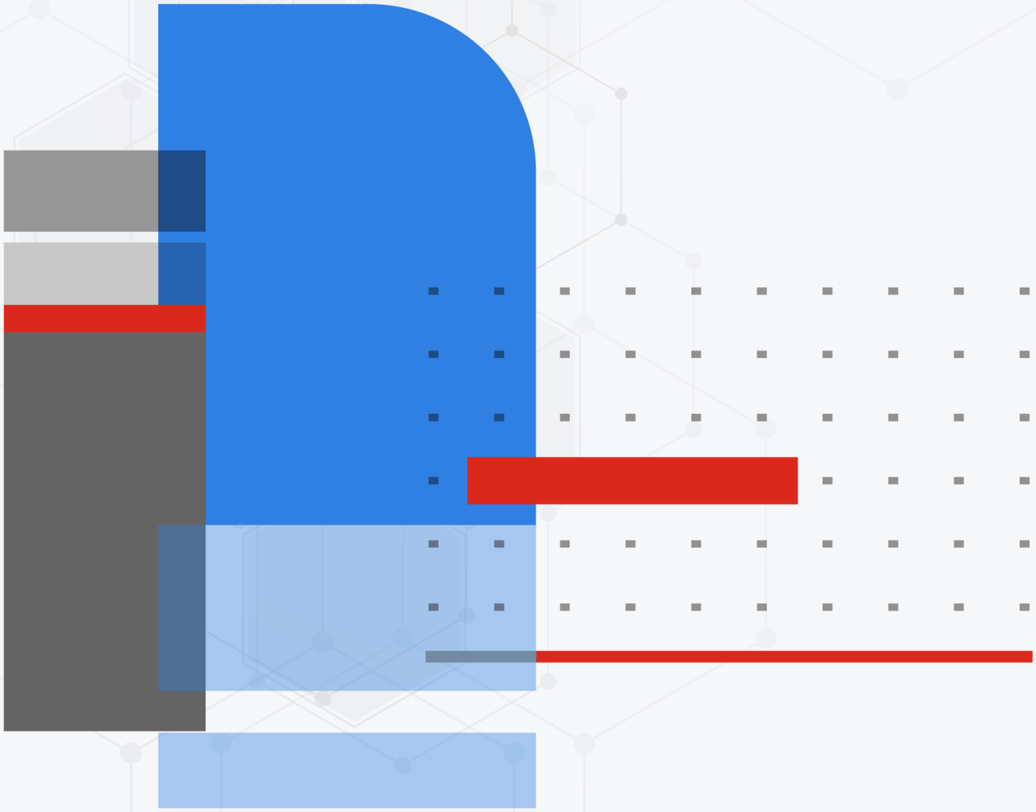
Packet Flow

FortiProxy 7.4



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

March 7, 2025
FortiProxy 7.4 Packet Flow
45-740-935624-20250307

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-07-24	Initial release.

UTM packet flow: proxy-based inspection

When a FortiProxy unit is configured for proxy-based inspection, packets initially encounter the IPS engine, which applies single-pass IPS and Application Control if configured in the firewall policy accepting the traffic.

The packets are then sent to the FortiProxy UTM/NGFW proxy for proxy-based inspection. The proxy first determines if the traffic is SSL traffic that should be decrypted for SSL inspection. SSL traffic to be inspected is decrypted by the proxy. SSL decryption is offloaded to and accelerated by CP8 or CP9 processors.

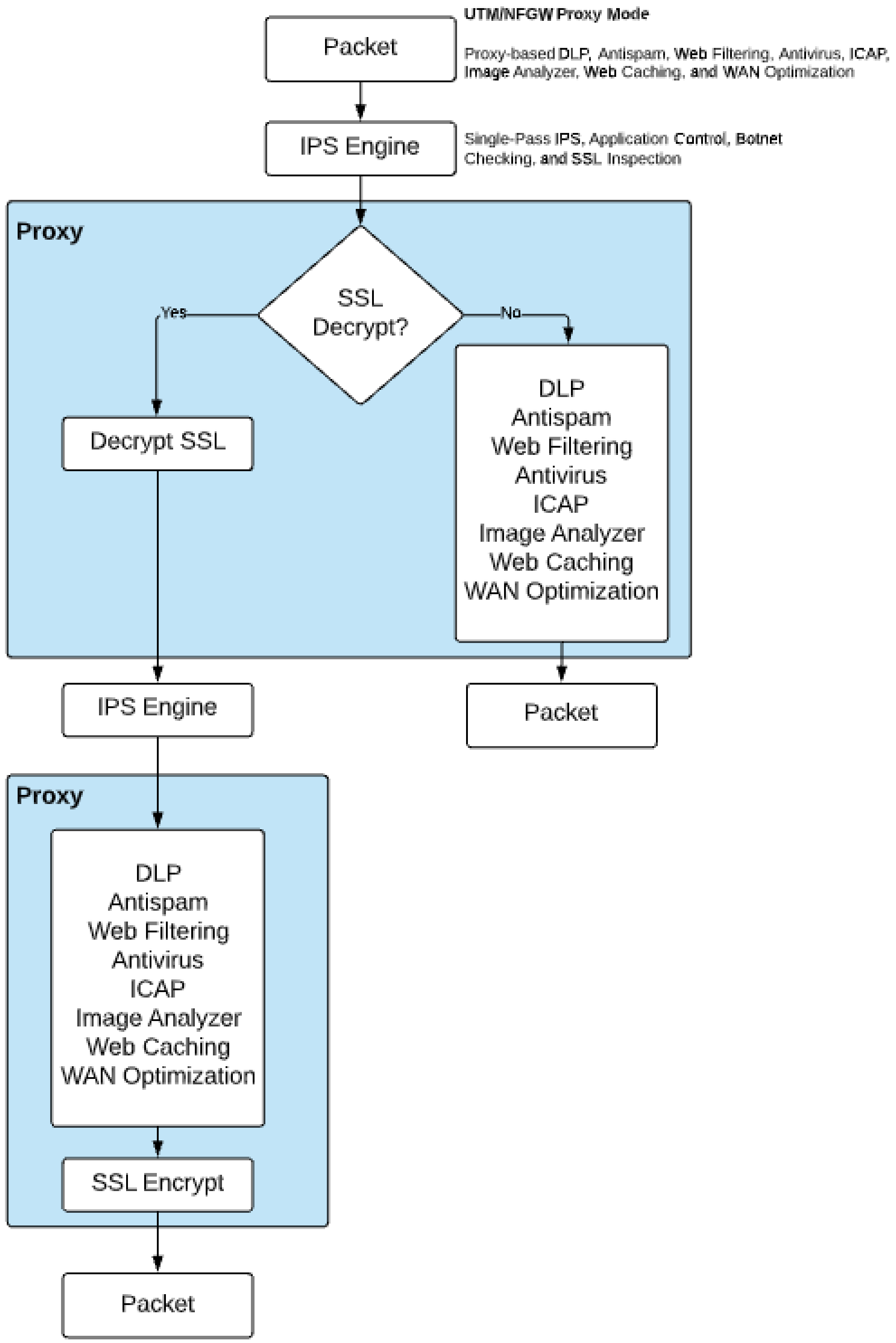
Proxy-based inspection extracts and caches content, such as files and web pages, from content sessions and inspects the cached content for threats. Content inspection happens in the following order:

1. DLP
2. Anti-Spam
3. Web Filtering
4. ICAP
5. Antivirus and Image Analyzer
6. Web caching and WAN optimization

If no threat is found, the proxy relays the content to its destination. If a threat is found, the proxy can block the threat and replace it with a replacement message.

Decrypted SSL traffic is sent to the IPS engine (where IPS and Application Control can be applied) before reentering the proxy where actual proxy-based inspection is applied to the decrypted SSL traffic. After decrypted SSL traffic has been inspected, it is re-encrypted and forwarded to its destination. SSL encryption is offloaded to and accelerated by CP8 or CP9 processors. If a threat is found, the proxy can block the threat and replace it with a replacement message.

ICAP intercepts HTTP and HTTPS traffic and forwards it to an ICAP server. The FortiProxy unit is the surrogate, or “middle-man”, and carries the ICAP responses from the ICAP server to the ICAP client; the ICAP client then responds back, and the FortiProxy unit determines the action that should be taken with these ICAP responses and requests.


UTM/NFGW Proxy Mode
Packet
Proxy-based DLP, Antispam, Web Filtering, Antivirus, ICAP, Image Analyzer, Web Caching, and WAN Optimization
IPS Engine
Single-Pass IPS, Application Control, Botnet Checking, and SSL Inspection
Proxy
SSL Decrypt?
Yes
No
Decrypt SSL
DLP
Antispam
Web Filtering
Antivirus
ICAP
Image Analyzer
Web Caching
WAN Optimization
IPS Engine
Packet
Proxy
DLP
Antispam
Web Filtering
Antivirus
ICAP
Image Analyzer
Web Caching
WAN Optimization
SSL Encrypt
Packet

UTM packet flow: explicit web proxy

If the explicit web proxy is enabled on a FortiProxy unit, proxy-based inspection occurs. One or more interfaces configured to listen for web browser sessions on the configured explicit web proxy port (by default 8080) accept all HTTP and HTTPS sessions on the explicit proxy port that match an explicit web proxy policy.

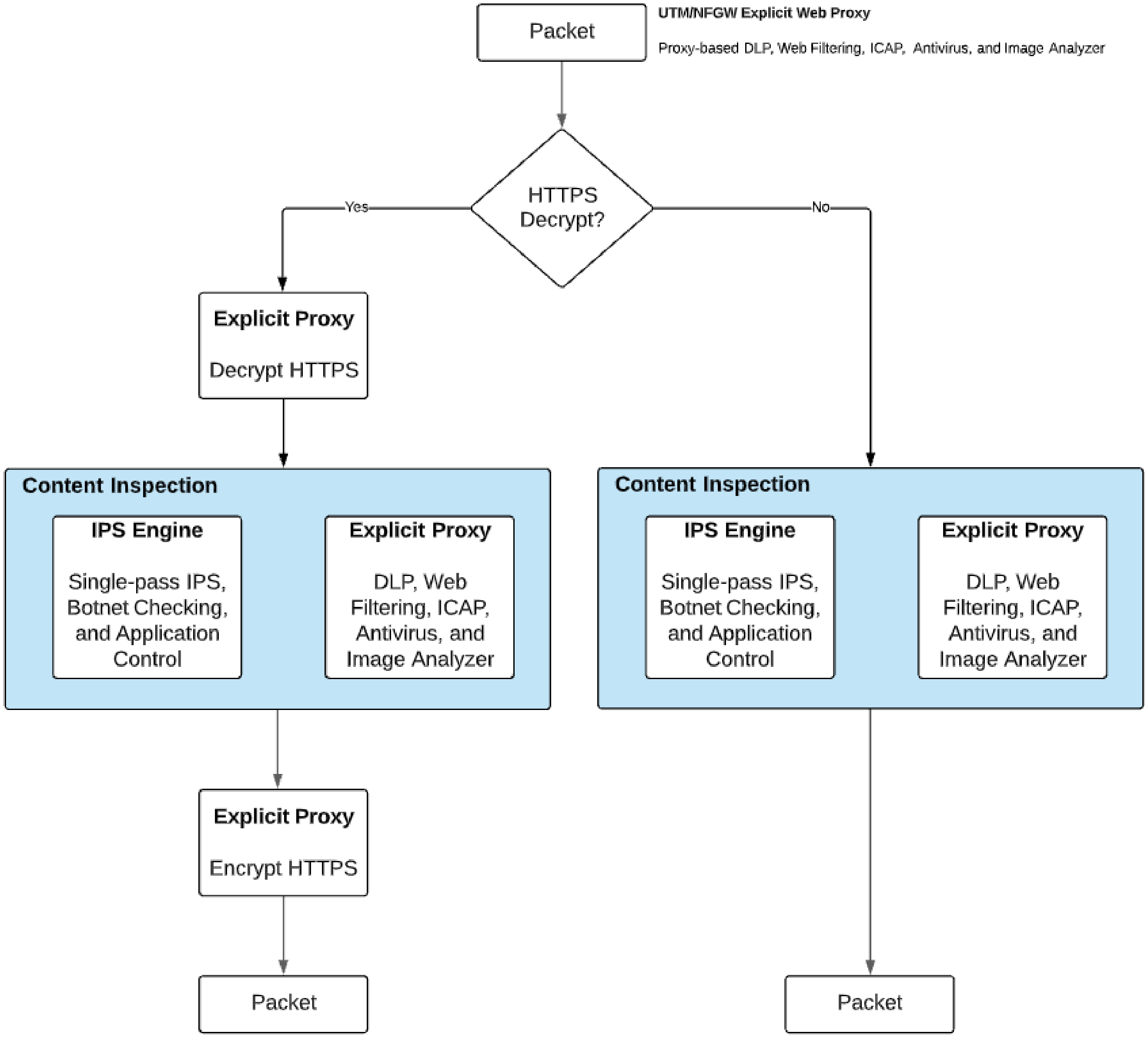
Plain text explicit web proxy HTTP traffic passes in parallel to both the IPS engine and the explicit web proxy for content scanning. The IPS engine applies IPS and application control content scanning. The explicit web proxy applies DLP, web filtering, and Antivirus content scanning.

If the IPS engine and the explicit proxy do not detect any security threats, the FortiProxy unit relays the content to a destination interface. If the IPS engine or the explicit proxy detect a threat, the FortiProxy unit can block the threat and replace it with a replacement message.

Encrypted explicit web proxy HTTPS traffic passes to the explicit web proxy for decryption. Decrypted traffic once again passes in parallel to the IPS engine and the explicit web proxy for content scanning.

If the IPS engine and the explicit proxy do not detect any security threats, the explicit proxy re-encrypts the traffic and the FortiProxy unit relays the content to its destination. If the IPS engine or the explicit proxy detect a threat, the FortiProxy unit can block the threat and replace it with a replacement message. The explicit proxy offloads HTTPS decryption and encryption to CP8 or CP9 processors.

The FortiProxy unit uses routing to route explicit web proxy sessions through the FortiProxy unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. A FortiProxy unit operating in transparent mode changes the source address to the transparent mode management IP address. You can also configure the explicit web proxy to keep the original client IP address.


Packet
UTM/NFGW Explicit Web Proxy
Proxy-based DLP, Web Filtering, ICAP, Antivirus, and Image Analyzer
HTTPS Decrypt?
Yes
No
Explicit Proxy
Decrypt HTTPS
Content Inspection
IPS Engine
Single-pass IPS, Botnet Checking, and Application Control
Explicit Proxy
DLP, Web Filtering, ICAP, Antivirus, and Image Analyzer
Content Inspection
IPS Engine
Single-pass IPS, Botnet Checking, and Application Control
Explicit Proxy
DLP, Web Filtering, ICAP, Antivirus, and Image Analyzer
Explicit Proxy
Encrypt HTTPS
Packet
Packet

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.