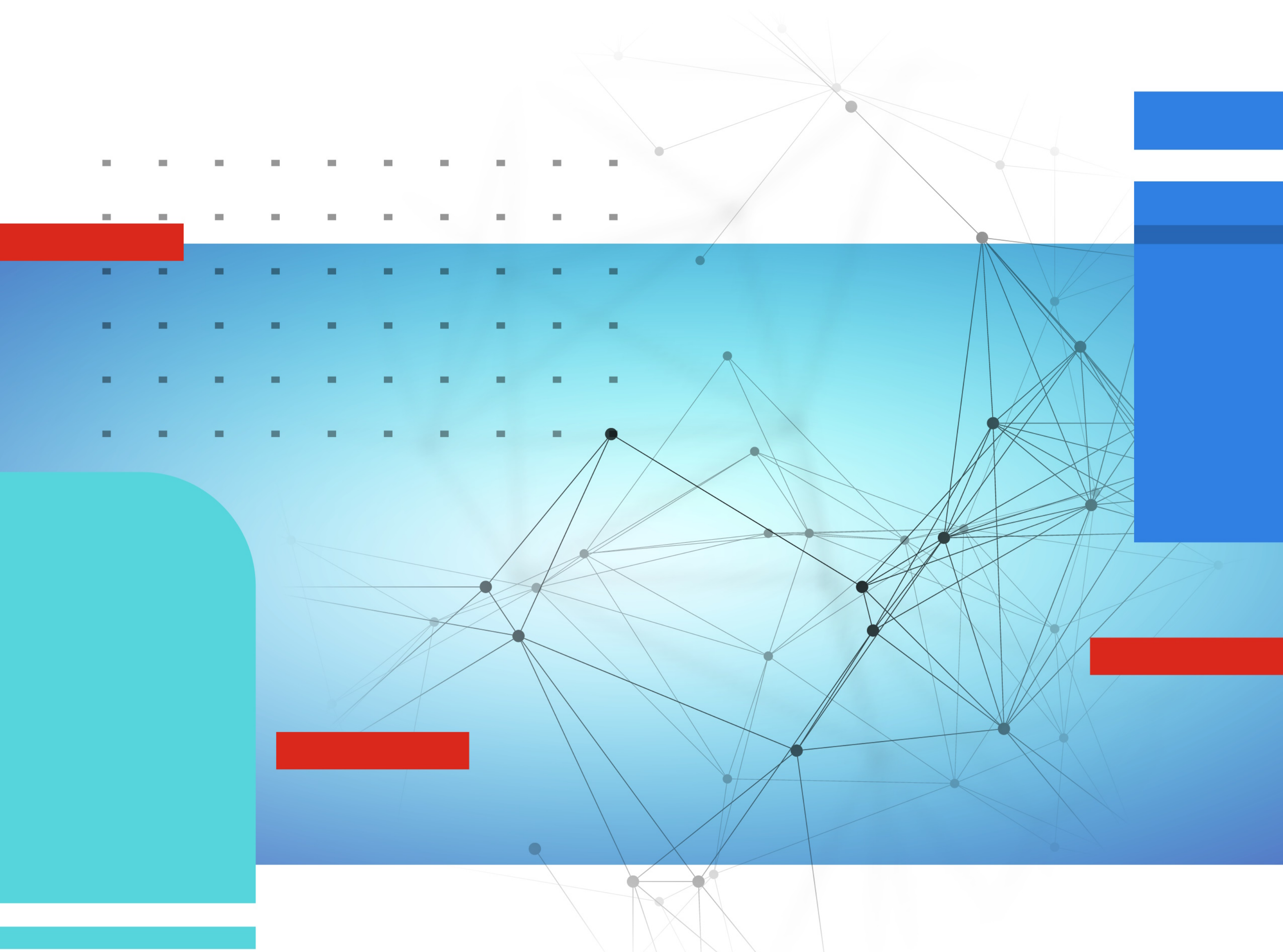
Packet Flow

FortiProxy 7.6



March 25, 2025
FortiProxy 7.6 Packet Flow
45-760-1100092-20250325

TABLE OF CONTENTS

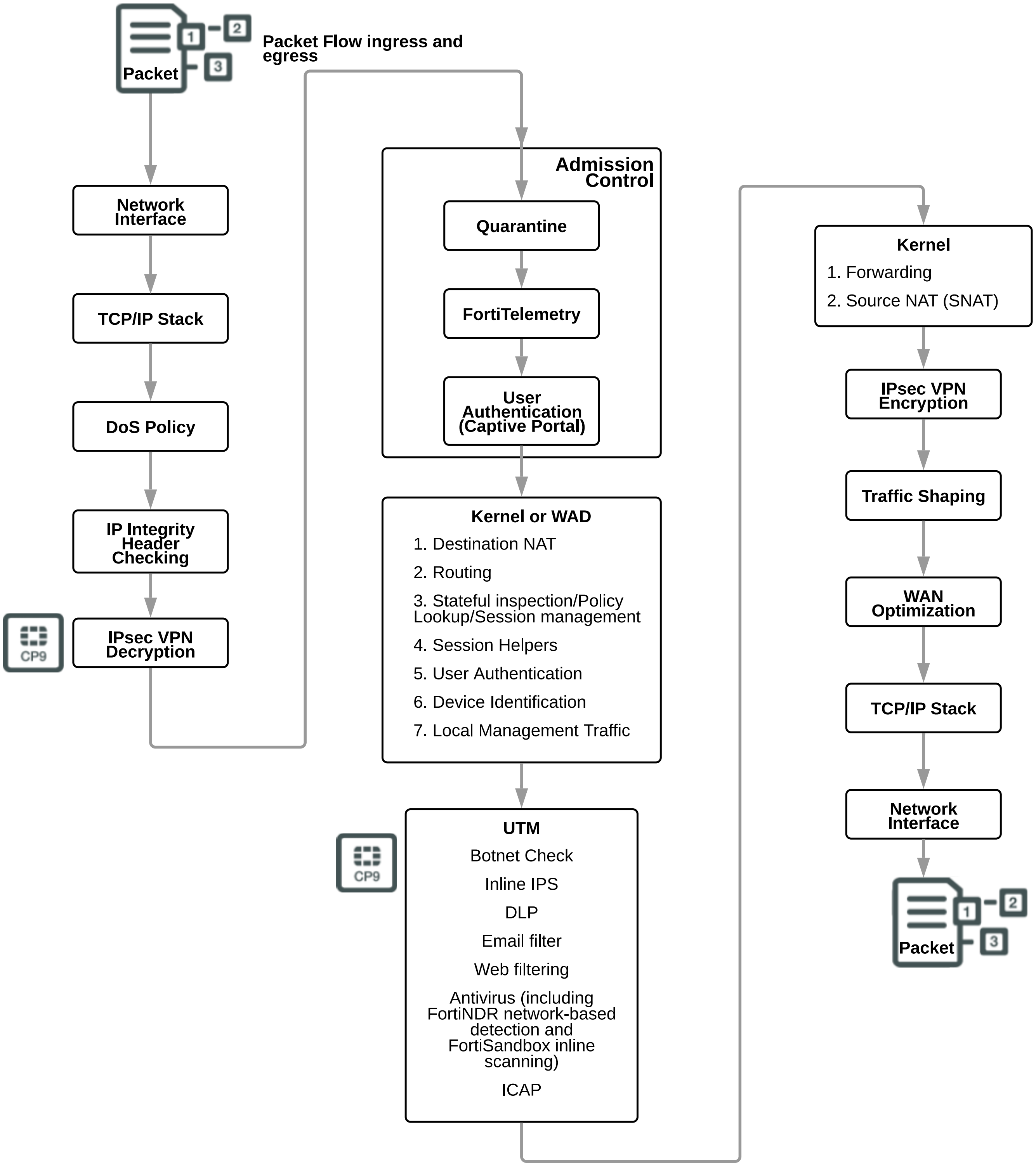
Change Log 4
Packet flow ingress and egress 5
Ingress 6
Admission control 6
Kernel or WAD 6
UTM 8
Antivirus with FortiSandbox and FortiNDR 8
Kernel 9
Egress 9

Change Log

Date	Change Description
2024-11-18	Initial document release.
2025-03-06	• Added Packet flow ingress and egress on page 5. • Updated *UTM packet flow: proxy-based inspection* and *UTM packet flow: explicit web proxy*.
2025-03-25	• Updated Packet flow ingress and egress on page 5 • Deleted *UTM packet flow: proxy-based inspection* and *UTM packet flow: explicit web proxy* which have been moved to the FortiProxy Administration Guide.

Packet flow ingress and egress

This section describes the steps a packet goes through as it enters, passes through and exits from a FortiProxy.



Ingress

All packets accepted by a FortiProxy pass through a network interface and are processed by the TCP/IP stack. Then if **DoS policies** have been configured the packet must pass through these as well as automatic **IP integrity header checking**.

DoS scans are handled very early in the life of the packet to determine whether the traffic is valid or is part of a DoS attack. The DoS module inspects all traffic flows but only tracks packets that can be used for DoS attacks (for example, TCP SYN packets), to ensure they are within the permitted parameters. Suspected DoS attacks are blocked, other packets are allowed.

IP integrity header checking reads the packet headers to verify if the packet is a valid TCP, UDP, ICMP, SCTP or GRE packet. The only verification that is done at this step to ensure that the protocol header is the correct length. If it is, the packet is allowed to carry on to the next step. If not, the packet is dropped.

Incoming **IPsec packets** that match configured IPsec tunnels on the FortiProxy are decrypted after header checking is done.

If the packet is an IPsec packet, the IPsec engine attempts to decrypt it. If the IPsec engine can apply the correct encryption keys and decrypt the packet, the unencrypted packet is sent to the next step. Non-IPsec traffic and IPsec traffic that cannot be decrypted passes on to the next step without being affected. IPsec VPN decryption is offloaded to (by the main CPU) and accelerated by CP9 processors, which work at the system level .

Admission control

Admission control checks to make sure the packet is not from a source or headed to a destination on the quarantine list. If configured admission control then imposes FortiTelemetry protection that requires a device to have FortiClient installed before allowing packets from it. Admission control can also impose captive portal authentication on ingress traffic.

Kernel or WAD

Once a packet makes it through all of the ingress steps, the FortiProxy kernel or WAD performs the following checks to determine what happens to the packet next.

Step	Details
1. Destination NAT	Destination NAT checks the NAT table and determines if the destination IP address for incoming traffic must be changed using DNAT. DNAT is typically applied to traffic from the internet that is going to be directed to a server on a network behind the FortiProxy. DNAT means the actual address of the internal network is hidden from the internet. This step determines whether a route to the destination address actually exists. DNAT must take place before routing so that the FortiProxy can route packets to the correct destination.
2. Routing	Routing uses the routing table to determine the interface to be used by the packet

Step	Details
	as it leaves the FortiProxy. Routing also distinguishes between local traffic and forwarded traffic. Firewall policies are matched with packets depending on the source and destination interface used by the packet. The source interface is known when the packet is received and the destination interface is determined by routing.
3. Stateful inspection/policy lookup/session management	Stateful inspection looks at the first packet of a session and looks in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed. When the first packet of a session is matched in the policy table, stateful inspection adds information about the session to its session table. So when subsequent packets are received for the same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table). Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way. When the final packet in the session is processed, the session is removed from the session table. Stateful inspection also has a session idle timeout that removes sessions from the session table that have been idle for the length of the timeout. See the Stateful Firewall Wikipedia article (https://en.wikipedia.org/wiki/Stateful_firewall) for an excellent description of stateful inspection. See Policy matching for more details.
4. Session helpers	Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. FortiProxy uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow those protocols to send packets through the firewall. FortiProxy includes the following session helpers: • PPTP • H323 • RAS • TNS • TFTP • RTSP • FTP • MMS • PMAP • DNS-UDP • RSH • DCERPC • MGCP
5. User authentication	User authentication added to security policies is handled by the stateful inspection, which is why Firewall authentication is based on IP address. Authentication takes place after policy lookup selects a policy that includes authentication.
6. Device identification	Device identification is applied if required by the matching policy.

Step	Details
7. Local management traffic	Local management traffic, such as administrative access, routing protocol communication, central management from FortiManager, communication with the FortiGuard network, is processed by applications such as the web server which displays the FortiProxy GUI, the SSH server for the CLI or the FortiGuard server to handle local FortiGuard database updates or FortiGuard Web Filtering URL lookups. Local management traffic terminates at the management IP address or a FortiProxy interface (such as the dedicated management interface) without going through subsequent stateful inspection steps. You configure local management access by configuring a management interface (see Transparent mode management or HA cluster out-of-band management) or by configuring administrative access.

UTM

If the policy matching the packet includes security profiles, then the packet is subject to Unified Threat Management (UTM) processing with explicit or transparent web proxy. Many UTM processes are offloaded and accelerated by CP9 processors.

Packets are then subject to botnet checking to make sure they are not destined for known botnet addresses.

Packets through the FortiProxy go through the following types of inspection: inline IPS, DLP, email filter (anti-spam), web filtering, antivirus (including FortiNDR network-based detection and FortiSandbox inline scanning), and ICAP.

Antivirus with FortiSandbox and FortiNDR

When FortiSandbox and FortiNDR are involved in antivirus, as soon as FortiProxy’s antivirus (AV) engine starts analysis, FortiNDR simultaneously receives the file for network-based detection. If the file or traffic is passed and not flagged as known malware after FortiProxy’s AV engine analysis, FortiSandbox is invoked serially (inline) for further scanning.

FortiSandbox behavior depends on the *fortisandbox-mode* setting:

- When set to *inline*, file delivery is delayed until analysis is complete. FortiSandbox analyzes the file and returns a verdict (Clean / Suspicious / Malicious). Based on the verdict and FortiSandbox's configuration settings, FortiProxy will allow, block, or quarantine the file.
- If *fortisandbox-mode* is set to *analytics-suspicious* or *analytics-everything*, FortiProxy will allow the traffic immediately, and FortiSandbox will perform post-transfer scanning in the background. In this case, if a threat is later detected, FortiProxy may block or quarantine the file in subsequent transactions.

If FortiSandbox or any other AV method returns an "infected" verdict, the FortiNDR inspection is aborted. Otherwise, FortiProxy will allow, block, or quarantine the file based on FortiNDR's verdict.

See FortiSandbox inline scanning and Using FortiNDR inline scanning with antivirus for more details.

Kernel

Traffic is now in the process of exiting the FortiProxy. The kernel uses the routing table to forward the packet out the correct exit interface.

The kernel also checks the NAT table and determines if the source IP address for outgoing traffic must be changed using SNAT. SNAT is typically applied to traffic from an internal network heading out to the internet. SNAT means the actual address of the internal network is hidden from the internet.

Egress

Before exiting the FortiProxy, outgoing packets that are entering an IPsec VPN tunnel are encrypted and encapsulated. IPsec VPN encryption is offloaded to and accelerated by CP9 processors.

Traffic shaping is then imposed, if configured, followed by WAN Optimization. The packet is then processed by the TCP/IP stack and exits out the egress interface.

FORTINET®

www.fortinet.com