FortiOS - Parallel Path Processing (Life of a Packet)

Version 6.0.4

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdocs@fortinet.com

April 8, 2019
FortiOS 6.0.4 Parallel Path Processing (Life of a Packet)
01-604-480928-20190408

TABLE OF CONTENTS

Change log

Date	Change description
April 8, 2019	New format.
March 15, 2019	Corrections to information about the access control list (ACL) feature.
November 19, 2018	Minor updates.
November 16, 2018	Changes to Packet flow: NP6 and NP6lite sessions on page 14.
November 9, 2018	Added information about SD-WAN and SD-WAN application control to Routing (including SD-WAN) on page 10.
June 5, 2018	FortiOS 6.0.1 document release. New section: UTM/NGFW packet flow: explicit web proxy on page 23. Information about SSL mirroring added to UTM/NGFW packet flow: flow-based inspection on page 19 and UTM/NGFW packet flow: proxy-based inspection on page 21.
March 29, 2018	FortiOS 6.0 document release. Minor updates.

Packet flow and security inspection

Directed by security policies, a FortiGate screens network traffic from the IP layer up through the application layer of the TCP/IP stack. The steps involved in this inspection depend on the FortiGate hardware configuration (the presence or absence of network processors such as the NP6 and content processors such as the CP8 and CP9) and on the Unified Threat Management (UTM)/Next Generation Firewall (NGFW) inspection mode (flow-based or proxy-based) of the FortiGate or VDOM.

This chapter describes what happens to a packet as it travels through a FortiGate running FortiOS 6.0.

The FortiGate performs three types of security inspection:

- Kernel-based stateful inspection, that provides individual packet-based security within a basic session state
- Flow-based inspection, that takes a snapshot of content packets and uses pattern matching to identify security threats in the content
- Proxy-based inspection, that reconstructs content passing through the FortiGate and inspects the content for security threats.

Each inspection component plays a role in the processing of a packet as it traverses the FortiGate en route to its destination.

Parallel Path Processing

Parallel Path Processing (PPP) uses the firewall policy configuration to choose from a group of parallel options to determine the optimal path for processing a packet. Most FortiOS features are applied through Firewall policies and the features applied determine the path a packet takes. Using firewall policies you can impose UTM/NGFW processing on content traffic that may contain security threats (such as HTTP, email and so on). Many UTM/NGFW processes are offloaded and accelerated by CP8 or CP9 processors. Using the policy configuration you can apply a range of protection from basic IPS attack protection that looks for network-based attacks to full scale advanced threat management (ATM), application control, antivirus, DLP and so on.

You can also create policies for traffic that does not pose security threats and bypass UTM/NGFW checking. This control allows you to improve network performance without compromising security. On FortiGates with network processors (for example the NP6) much of the traffic that does not require UTM/NGFW processing can be offloaded to the NP6 processors freeing up FortiGate processing resources for other higher risk traffic.

In addition, many FortiGate models support NTurbo to offload flow-based UTM/NGFW sessions to network processors. Flow-based sessions can also be accelerated using IPSA technology to enhance offloading of pattern matching to CP8 and CP9 content processors.

This chapter begins with an overview of packet flow ingress and egress and includes a section that shows how NP6 offloading optimizes packet flow for packets that don't require UTM/NGFW processing and for packets that use NTurbo to offload flow-based UTM/NGFW processing.

Next this chapter breaks down how packets pass through UTM/NGFW processing both for a single-pass flow-based UTM/NGFW processing and a proxy-based UTM/NGFW processing.

High-level list of processes that affect packets

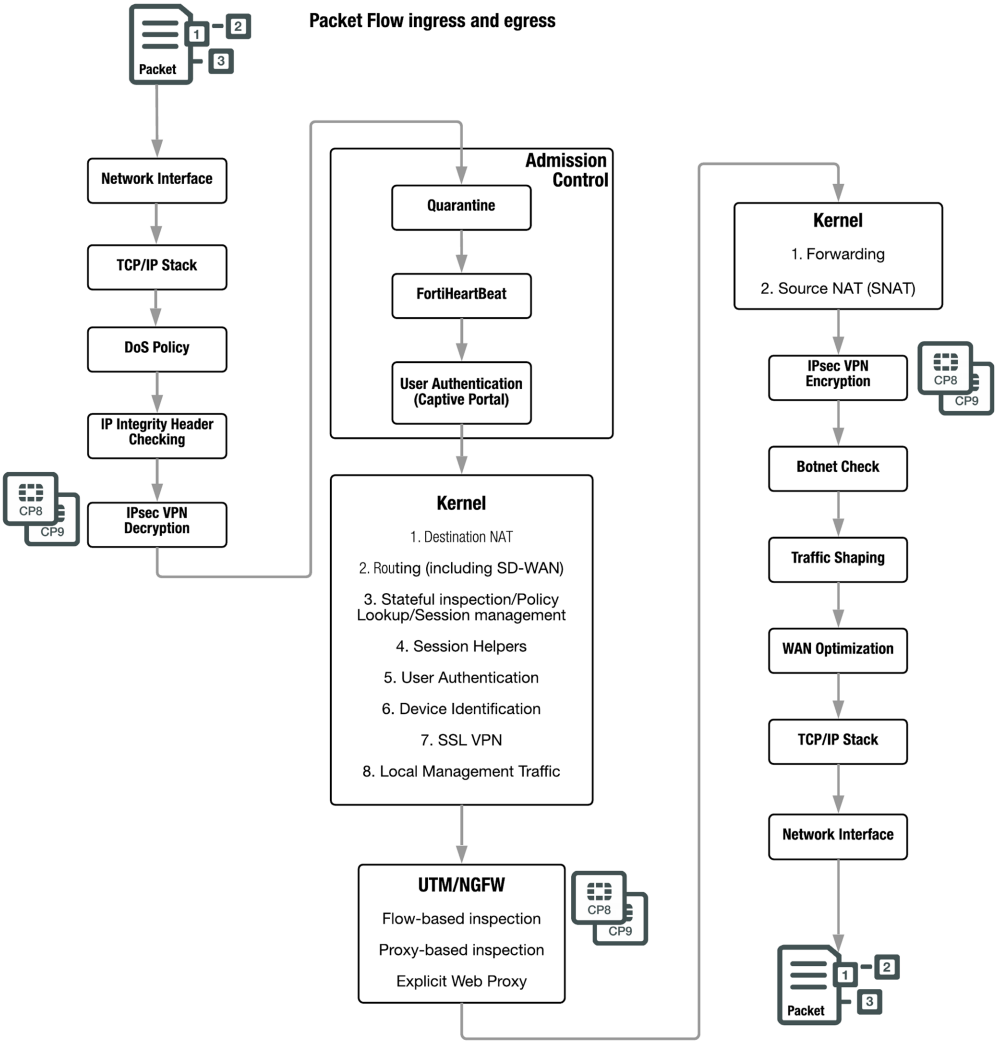
In general packets passing through a FortiGate can be affected by the following processes. This is a complete high-level list of all of the processes. Not all packets see all of these processes. The processes a packet encounters depends on the type of packet and on the FortiGate software and hardware configuration.

- **Ingress packet flow**
- Network Interface
- TCP/IP stack
- DoS Policy
- IP integrity header checking
- IPsec VPN decryption
- **Admission Control**
- Quarantine
- FortiTelemetry
- User Authentication
- **Kernel**
- **UTM/NGFW**
- Flow-based inspection
  - NTurbo
  - IPSA
- Proxy-based inspection
- Explicit Web Proxy
- **Kernel**
- Forwarding
- Source NAT (SNAT)
- **Egress packet flow**
- IPsec VPN Encryption

- Destination NAT
- Routing (including SD-WAN)
- Stateful inspection/Policy Lookup/Session management
- Session Helpers
- User Authentication
- Device Identification
- SSL VPN
- Local Management Traffic
- Botnet check
- Traffic shaping
- WAN Optimization
- TCP/IP stack
- Network Interface

Packet flow ingress and egress: FortiGates without network processor offloading

This section describes the steps a packet goes through as it enters, passes through and exits from a FortiGate. This scenario shows all of the steps a packet goes through if a FortiGate does not contain network processors (such as the NP6).



Ingress

All packets accepted by a FortiGate 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 FortiGate 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 and accelerated by CP8 or CP9 processors.

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

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

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 FortiGate. 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 FortiGate can route packets to the correct destination.

Routing (including SD-WAN)

Routing uses the routing table to determine the interface to be used by the packet as it leaves the FortiGate. 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.

SD-WAN is a special application of routing that provides route selection, load balancing, and failover among two or more routes. SD-WAN also supports using the Internet Services Database (ISDB) and Application Control to select a route in the following way:

- SD-WAN uses Application Control to compare the first packet of a new session against the layer 4 ISDB.
- If Application Control can identify the new session as a known application, SD-WAN is applied to the session according to the matching SD-WAN rule. SD-WAN then routes all of the packets in the session according to the selected SD-WAN rule.
- If Application Control cannot match a new session with an application in the layer 4 ISDB, the implicit SD-WAN rule is applied to the session.

As the session is being processed by the implicit SD-WAN rule, layer 7 Application Control attempts to identify the application. If the application can be identified, the ISDB is extended by adding a layer 4 match record for the application to the ISDB cache. New sessions can then be matched and routed by SD-WAN using both the ISDB and the ISDB cache.

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.

Session helpers

Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. For example, the SIP VoIP protocol uses TCP control packets with a standard destination port

to set up SIP calls. To successfully process SIP VoIP calls, FortiOS must be able to extract information from the body of the SIP packet and use this information to allow the voice-carrying packets through the firewall.

FortiOS 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. FortiOS includes the following session helpers:

- PPTP
- H323
- RAS
- TNS
- TFTP
- RTSP
- FTP
- MMS
- PMAP
- SIP
- DNS-UDP
- RSH
- DCERPC
- MGCP

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.

Device identification

Device identification is applied if required by the matching policy.

SSL VPN

Local SSL VPN traffic is treated like special management traffic as determined by the SSL VPN destination port. Packets are decrypted and are routed to an SSL VPN interface. Policy lookup is then used to control how packets are forwarded to their destination outside the FortiGate. SSL encryption and decryption is offloaded to and accelerated by CP8 or CP9 processors.

Local management traffic

Local management traffic terminates at a FortiGate interface. This can be any FortiGate interface including dedicated management interfaces. In multiple VDOM mode local management traffic terminates at the management interface. In transparent mode, local management traffic terminates at the management IP address.

Local management traffic includes administrative access, some routing protocol communication, central management from FortiManager, communication with the FortiGuard network and so on. Management traffic is allowed or blocked according to the Local In Policy list which lists all management protocols and their access control settings. You configure local management access indirectly by configuring administrative access and so on.

Management traffic is processed by applications such as the web server which displays the FortiOS 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 is not involved in subsequent stateful inspection steps.

SSL VPN traffic terminates at a FortiGate interface similar to local management traffic. However, SSL VPN traffic uses a different destination port number than administrative HTTPS traffic and can thus be detected and handled differently.

UTM/NGFW

If the policy matching the packet includes security profiles, then the packet is subject to Unified Threat Management (UTM)/Next Generation Firewall (NGFW) processing. UTM/NGFW processing depends on the inspection mode of the FortiGate: Flow-based (single pass architecture) or proxy-based. Proxy-based processing can include Explicit web proxy traffic. Many UTM/NGFW processes are offloaded and accelerated by CP8 or CP9 processors.

Single pass flow-based UTM/NGFW inspection identifies and blocks security threats in real time as they are identified using single-pass Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats.

Proxy-based UTM/NGFW inspection can apply both flow-based and proxy-based inspection. Packets initially encounter the IPS engine, which can apply single-pass flow-based IPS and Application Control (as configured). The packets are then sent to the proxy for proxy-based inspection. Proxy-based inspection can apply VoIP inspection, DLP, AntiSpam, Web Filtering, Antivirus, and ICAP.

Explicit web proxy inspection is similar to proxy based inspection.

CP9 content processors

Most FortiGate models contain Security Processing Unit (SPU) Content Processors (CPs) that accelerate many common resource intensive security related processes. CPs work at the system level with tasks being offloaded to them as determined by the main CPU. Capabilities of the CPs vary by model. Newer FortiGate units include CP9 processors. Older CP versions still in use in currently operating FortiGate models include the CP4, CP5, CP6, and CP8.

CP9 capabilities

The CP9 content processor provides the following services:

- Flow-based inspection (IPS, application control etc.) pattern matching acceleration with over 10Gbps throughput
- IPS pre-scan
- IPS signature correlation
- Full match processors
- High performance VPN bulk data engine
- IPsec and SSL/TLS protocol processor
- DES/3DES/AES128/192/256 in accordance with FIPS46-3/FIPS81/FIPS197
- MD5/SHA-1/SHA256/384/512-96/128/192/256 with RFC1321 and FIPS180
- HMAC in accordance with RFC2104/2403/2404 and FIPS198
- ESN mode
- GCM support for NSA "Suite B" (RFC6379/RFC6460) including GCM-128/256; GMAC-128/256
- Key Exchange Processor that supports high performance IKE and RSA computation
- Public key exponentiation engine with hardware CRT support

- Primary checking for RSA key generation
- Handshake accelerator with automatic key material generation
- True Random Number generator
- Elliptic Curve support for NSA "Suite B"
- Sub public key engine (PKCE) to support up to 4096 bit operation directly (4k for DH and 8k for RSA with CRT)
- DLP fingerprint support
- TTTD (Two-Thresholds-Two-Divisors) content chunking
- Two thresholds and two divisors are configurable

Kernel

Traffic is now in the process of exiting the FortiGate. 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.

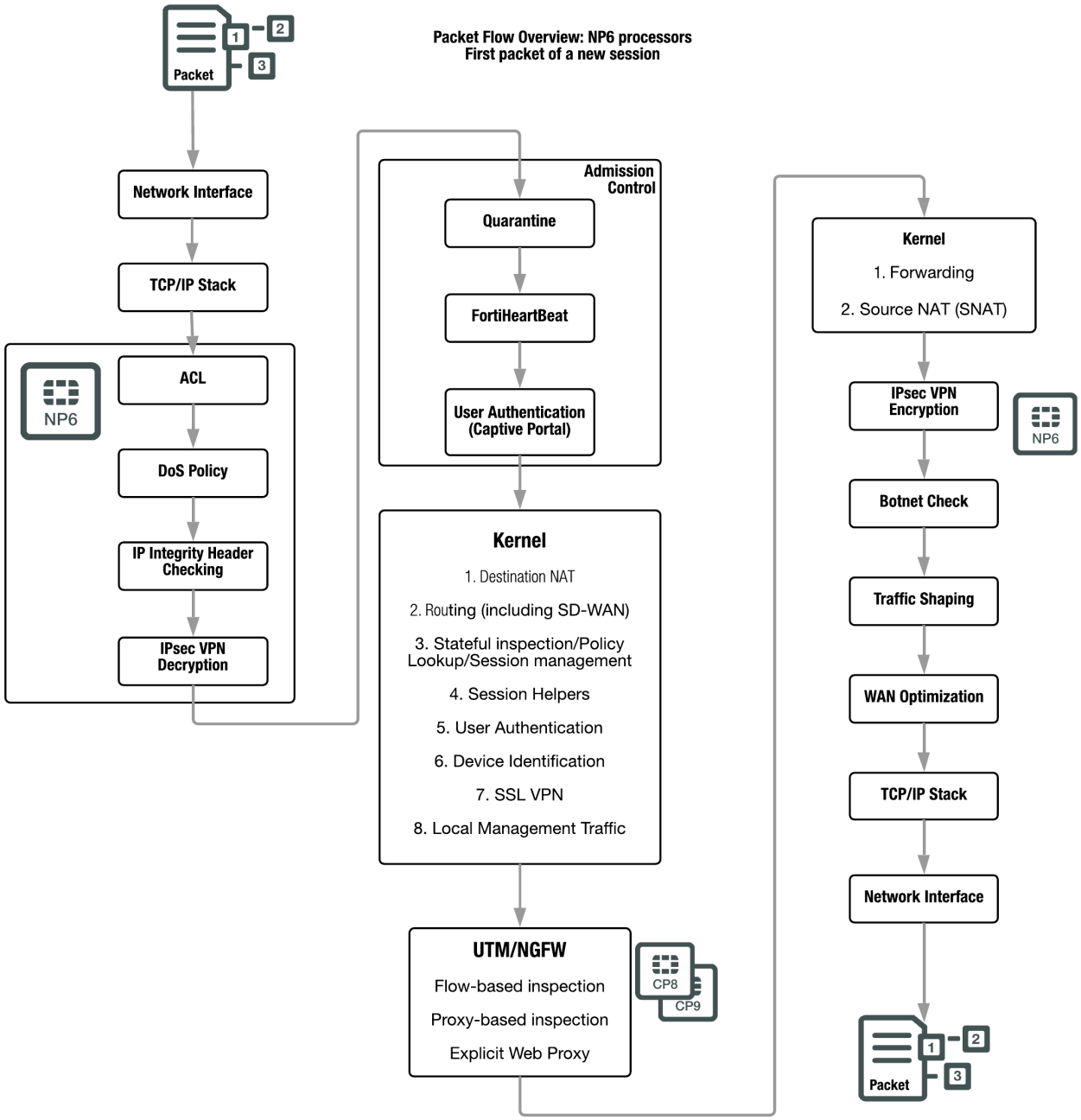
Egress

Before exiting the FortiGate, outgoing packets that are entering an IPsec VPN tunnel are encrypted and encapsulated. IPsec VPN encryption is offloaded to and accelerated by CP8 or CP9 processors. Packets are then subject to botnet checking to make sure they are not destined for known botnet addresses.

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.

Packet flow: NP6 and NP6lite sessions

On FortiGates with NP6 or NP6lite processors, the first packet of a session determines if the session can be offloaded. As long as there is no proxy-based UTM/NGFW, if your FortiGate includes NP6 processors, most sessions can be offloaded to them.

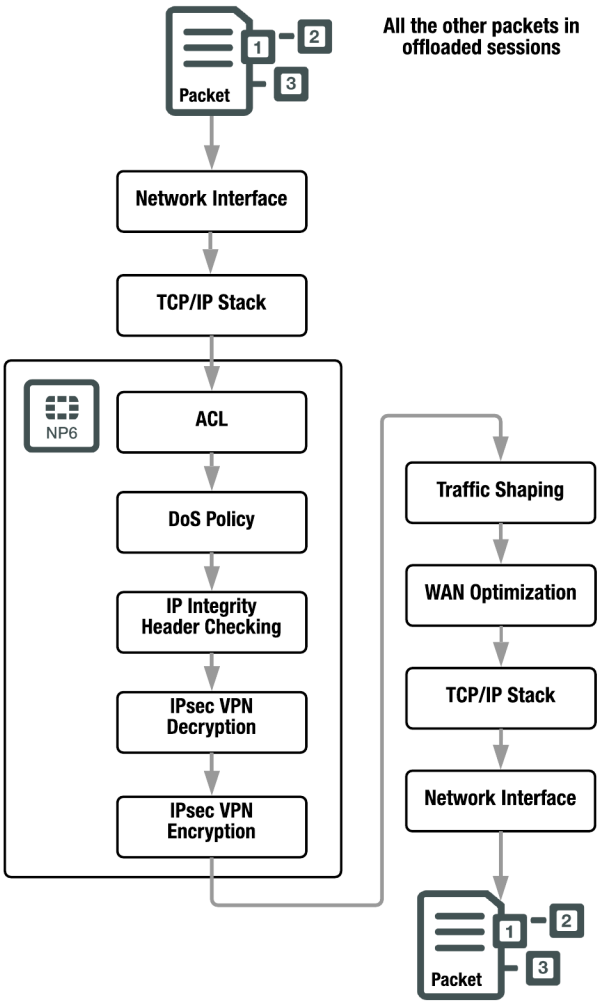


Access control list (ACL)

Access Control Lists (ACLs) use NP6 offloading to drop IPv4 or IPv6 packets at the physical network interface before the packets are analyzed by the CPU. The ACL feature is available only on FortiGates with NP6-accelerated interfaces. ACL checking is one of the first things that happens to the packet and checking is done by the NP6 processor. The result is very efficient protection that does not use CPU or memory resources.

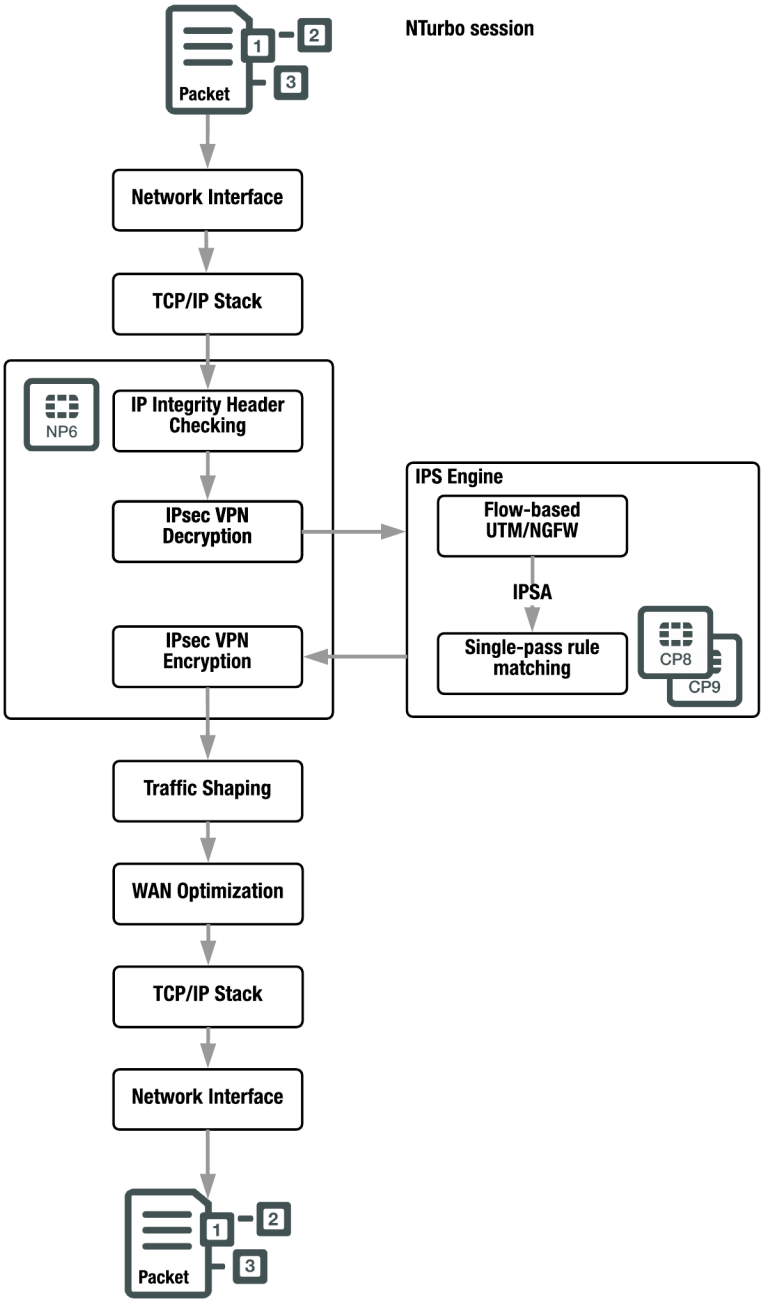
Packet flow: NP6 and NP6lite offloaded session

After the first packet, subsequent packets in an offloaded session skip routing, UTM/NGFW, and kernel processors and are just forwarded out the egress interface by the NP6 processor. As well, security measures such as DoS policies and so on are accelerated by the NP6 processor.



Packet flow: NTurbo

If your FortiGate supports NTurbo, many flow-based UTM/NGFW sessions can be offloaded to NP6 processors.



After the first packet, subsequent packets in an offloaded flow-based UTM/NGFW session skip routing, and kernel processors. Flow-based UTM/NGFW operations are still handled by the CPU with IPSA offloading pattern matching to CP8 or CP9 processors.

If a security threat is found the session is dropped. Otherwise, packets that are not blocked by UTM/NGFW are forwarded out of the egress interfaces by the NP6 processor.

NTurbo is not compatible with DoS policies, session helpers, or and most types of tunneling. If any of these features are present, flow-based UTM/NGFW sessions are not offloaded by NTurbo.

UTM/NGFW packet flow: flow-based inspection

Flow-based UTM/NGFW inspection identifies and blocks security threats in real time as they are identified using single-pass architecture that involves Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats.

If a FortiGate or a VDOM is configured for flow-based inspection, depending on the options selected in the firewall policy that accepted the session, flow-based inspection can apply **IPS**, **Application Control**, **Web Filtering**, **DLP**, and **AntiVirus**. Flow-based inspection is all done by the IPS engine and as you would expect, no proxying is involved.

Flow-based DLP is supported but not recommended. Flow-based DLP is not available from the GUI, but can be configured from the CLI.

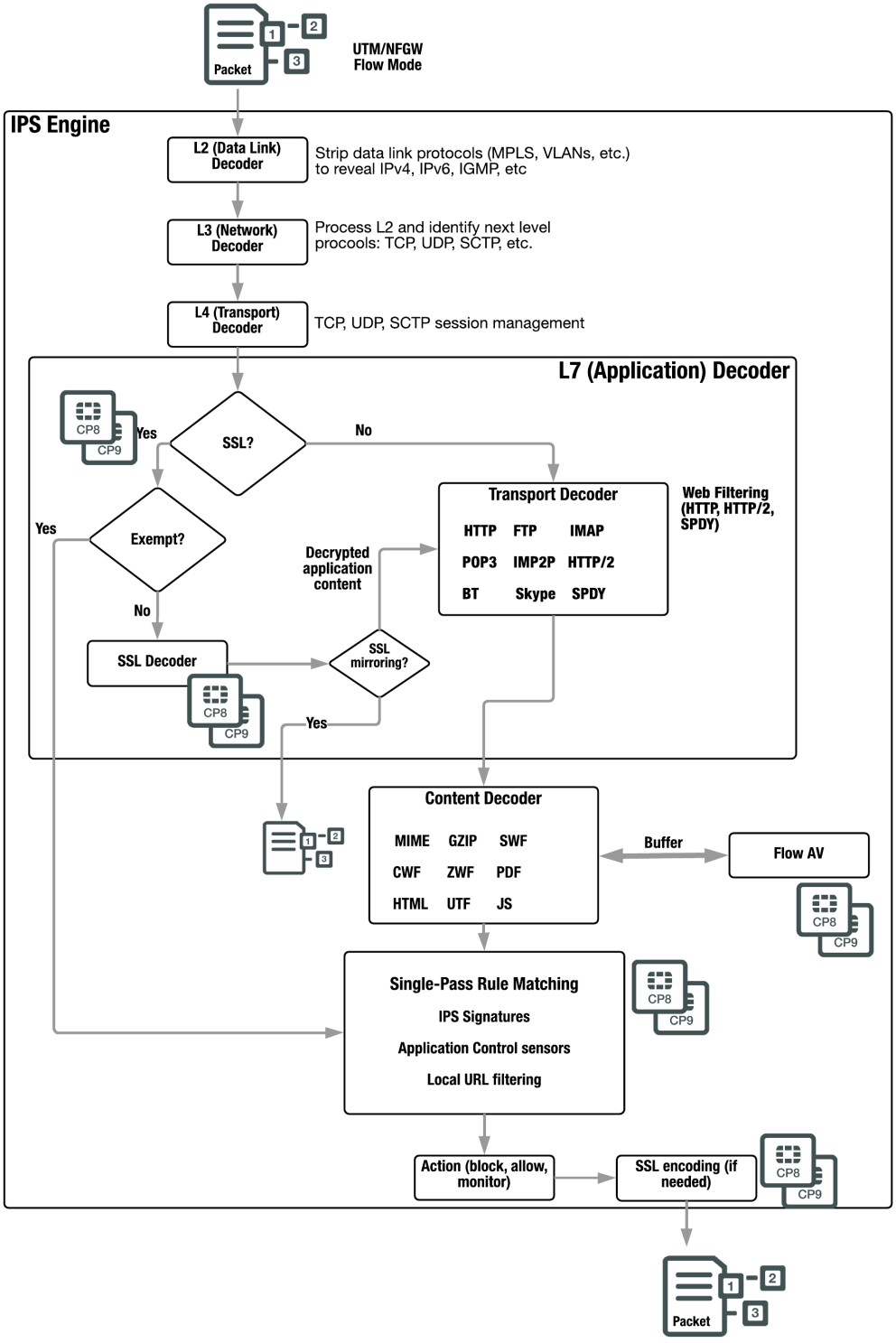
Before flow-based inspection can be applied the IPS engine uses a series of decoders to determine the appropriate security modules to be applied depending on the protocol of the packet and on policy settings. In addition, if SSL inspection is configured, the IPS engine also decrypts SSL packets. SSL decryption is offloaded and accelerated by CP8 or CP9 processors.

If your configuration includes SSL mirroring, the IPS engine copies decrypted application content, wraps it inside a TCP packet (with IP and ethernet headers), and sends it to the configured mirror interface. The TCP connection tuple is carried over from the original SSL connection. For the Ethernet frame, destination address is broadcast (FF:FF:FF:FF:FF:FF) and source address is all zeros.

All of the applicable flow-based security modules are applied simultaneously in one single pass, and pattern matching is offloaded and accelerated by CP8 or CP9 processors. IPS, Application Control, flow-based Web Filtering and flow-based DLP filtering happen together. Flow-based antivirus caches files during protocol decoding and submits cached files for virus scanning while the other matching is carried out.

Flow-based inspection typically requires less processing resources than proxy-based inspection and since its not a proxy, flow-based inspection does not change packets (unless a threat is found and packets are blocked). Flow-based inspection cannot apply as many features as proxy inspection (for example, flow-based inspection does not support client comforting and some aspects of replacement messages).

IPS and Application Control are only applied using flow-based inspection. Web Filtering, DLP and Antivirus can also be applied using proxy-based inspection.


Packet
UTM/NFGW
Flow Mode
IPS Engine
L2 (Data Link) Decoder
Strip data link protocols (MPLS, VLANs, etc.) to reveal IPv4, IPv6, IGMP, etc
L3 (Network) Decoder
Process L2 and identify next level procools: TCP, UDP, SCTP, etc.
L4 (Transport) Decoder
TCP, UDP, SCTP session management
L7 (Application) Decoder
CP8
CP9
SSL?
Yes
No
Exempt?
Yes
No
Transport Decoder
HTTP FTP IMAP
POP3 IMP2P HTTP/2
BT Skype SPDY
Web Filtering (HTTP, HTTP/2, SPDY)
Decrypted application content
SSL Decoder
SSL mirroring?
Yes
Content Decoder
MIME GZIP SWF
CWF ZWF PDF
HTML UTF JS
Buffer
Flow AV
Single-Pass Rule Matching
IPS Signatures
Application Control sensors
Local URL filtering
Action (block, allow, monitor)
SSL encoding (if needed)
Packet

UTM/NGFW packet flow: proxy-based inspection

If a FortiGate or VDOM is configured for proxy-based inspection then a mixture of flow-based and proxy-based inspection occurs. Packets initially encounter the IPS engine, which uses the same steps described in UTM/NGFW packet flow: flow-based inspection on page 19 to apply single-pass IPS and Application Control if configured in the firewall policy accepting the traffic.

The packets are then sent to the FortiOS 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.

If your configuration includes SSL mirroring, the IPS engine copies decrypted application content, wraps it inside a TCP packet (with IP and ethernet headers), and sends it to the configured mirror interface. The TCP connection tuple is carried over from the original SSL connection. For the Ethernet frame, destination address is broadcast (FF:FF:FF:FF:FF:FF) and source address is all zeros.

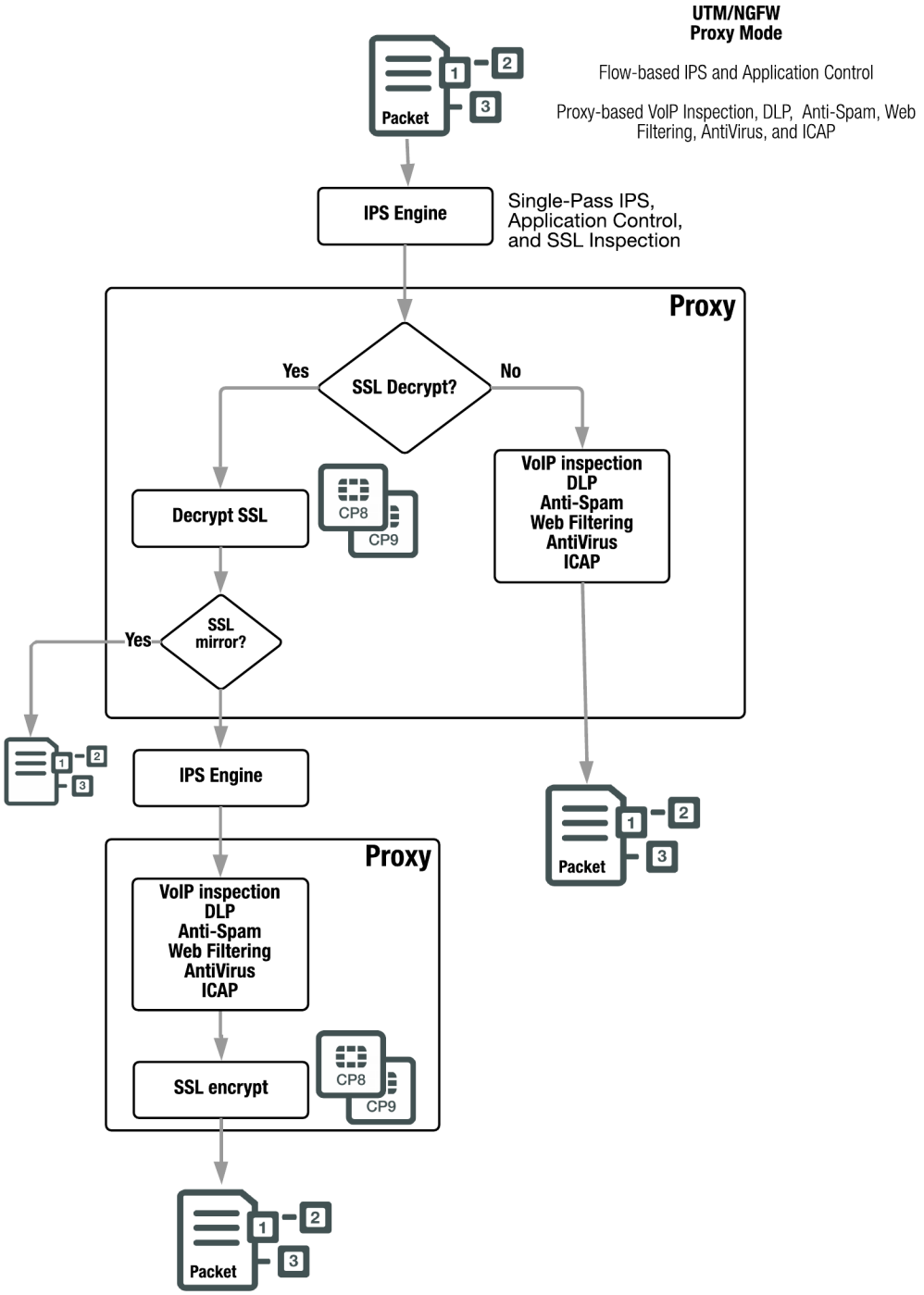
Proxy-based inspection extracts and caches content, such as files and web pages, from content sessions and inspects the cached content for threats. Content inspection happens in the following order: **VoIP inspection**, **DLP**, **Ant-Spam**, **Web Filtering**, **AntiVirus**, and **ICAP**.

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 re-entering the proxy where actual proxy-based inspection is applied to the decrypted SSL traffic. Once 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.

The proxy can also block VoIP traffic that contains threats. VoIP inspection can also look inside VoIP packets and extract port and address information and open pinholes in the firewall to allow VoIP traffic through.

ICAP intercepts HTTP and HTTPS traffic and forwards it to an ICAP server. The FortiGate 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 FortiGate determines the action that should be taken with these ICAP responses and requests.


UTM/NGFW
Proxy Mode
Flow-based IPS and Application Control
Proxy-based VoIP Inspection, DLP, Anti-Spam, Web Filtering, AntiVirus, and ICAP
Packet
IPS Engine
Single-Pass IPS, Application Control, and SSL Inspection
Proxy
SSL Decrypt?
Yes
No
Decrypt SSL
CP8
CP9
VoIP inspection
DLP
Anti-Spam
Web Filtering
AntiVirus
ICAP
SSL mirror?
Yes
IPS Engine
Proxy
VoIP inspection
DLP
Anti-Spam
Web Filtering
AntiVirus
ICAP
SSL encrypt
CP8
CP9
Packet
Packet

UTM/NGFW packet flow: explicit web proxy

If the explicit web proxy is enabled on a FortiGate or VDOM, a mixture of flow-based and 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.

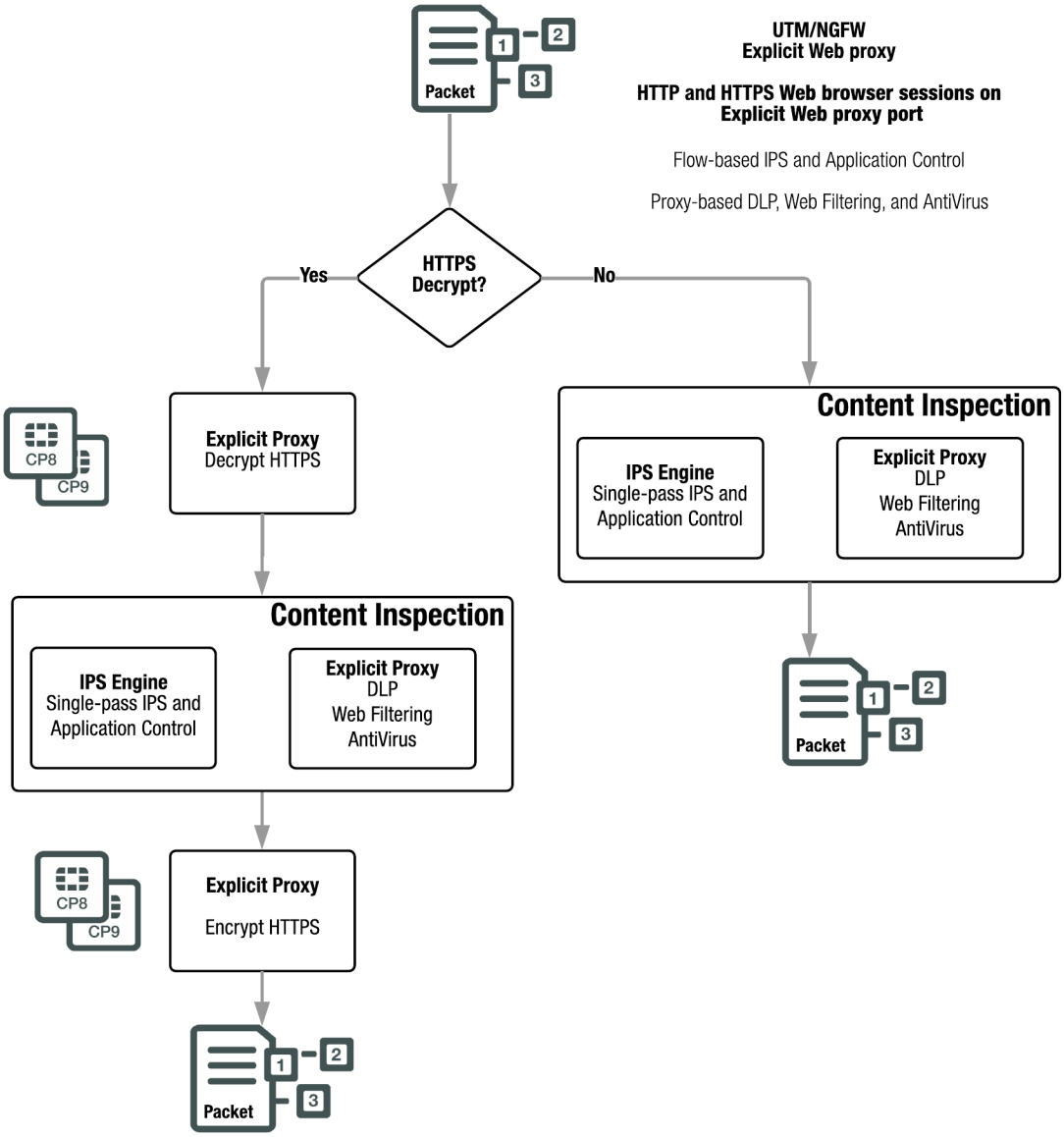
Plain text explicit web proxy HTTP traffic passes in parallel to both the IPS engine and the explicit web proxy for content scanning. The IPS engine applies IPS and application control content scanning. The explicit web proxy applies DLP, web filtering, and AntiVirus content scanning.

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

FortiOS uses routing to route explicit web proxy sessions through the FortiGate 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 FortiGate 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
1
2
3
UTM/NGFW
Explicit Web proxy
HTTP and HTTPS Web browser sessions on
Explicit Web proxy port
Flow-based IPS and Application Control
Proxy-based DLP, Web Filtering, and AntiVirus
HTTPS
Decrypt?
Yes
No
CP8
CP9
Explicit Proxy
Decrypt HTTPS
Content Inspection
IPS Engine
Single-pass IPS and
Application Control
Explicit Proxy
DLP
Web Filtering
AntiVirus
Content Inspection
IPS Engine
Single-pass IPS and
Application Control
Explicit Proxy
DLP
Web Filtering
AntiVirus
Packet
CP8
CP9
Explicit Proxy
Encrypt HTTPS
Packet

Comparison of inspection types

The tables in this section show how different security functions map to different inspection types.

Mapping security functions to inspection types

The table below lists FortiOS security functions and shows whether they are applied by the kernel, flow-based inspection or proxy-based inspection.

FortiOS security functions and inspection types

Security Function	Kernel (Stateful inspection)	Flow-based inspection	Proxy-based inspection
Firewall	yes		
IPsec VPN	yes		
Traffic Shaping	yes		
User Authentication	yes		
Management Traffic	yes		
SSL VPN	yes		
IPS		yes	
Antivirus		yes	yes
Application Control		yes	
Web filtering		yes	yes
DLP		yes	yes
Email Filtering			yes
VoIP inspection			yes
ICAP			yes

More information about inspection methods

The three inspection methods each have their own strengths and weaknesses. The following table looks at all three methods side-by-side.

Inspection methods comparison

Feature	Stateful	Flow	Proxy
Inspection unit per session	first packet	selected packets, single pass architecture, simultaneous application of configured inspection methods	complete content, configured inspection methods applied in order
Memory, CPU required	low	medium	high
Level of threat protection	good	better	best
Authentication	yes		
IPsec and SSL VPN	yes		
Antivirus protection		yes	yes
Web Filtering		yes	yes
Data Leak Protection (DLP)		yes	yes
Application control		yes	
IPS		yes	
Delay in traffic	minor	no	small
Reconstruct entire content		no	yes