

Parallel Path Processing

FortiOS 7.6.0



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



January 16, 2026

FortiOS 7.6.0 Parallel Path Processing

01-760-619132-20260116

TABLE OF CONTENTS

Change Log	4
Introduction	5
How this guide is organized	5
Parallel Path Processing	6
Ingress	6
Admission control	7
Kernel	7
Destination NAT	7
Routing (including SD-WAN)	7
Stateful inspection	8
Policy lookup	8
Session management	8
Session helpers	8
User authentication	9
Device identification	9
Agentless VPN	9
Local management traffic	9
UTM and NGFW Profile or Policy mode	9
CP9 and CP10 content processors	10
Kernel	10
Egress	10
Packet flow: NGFW Profile mode with no NP offloading	11
Packet flow: NGFW Profile mode with flow-based inspection	12
Packet flow: NGFW Policy mode	14
NGFW policy types	14
Packet flow: first packet of an NP session	16
Packet flow: NP-offloaded session	17
Access control list (ACL)	18
Packet flow: NTurbo	18
NP7 Host Protection Engine (HPE)	20

Change Log

Date	Change Description
January 16, 2026	Initial release.

Introduction

A FortiGate inspects network traffic from the IP layer up through the application layer of the TCP/IP stack and uses security policies to do this inspection. Inspection steps depend on the FortiGate hardware such as whether the FortiGate has network processors like the NP7 and content processors like the CP9 and CP10. Inspection steps also depend on the Unified Threat Management (UTM)/Next Generation Firewall (NGFW) inspection mode (flow-based or proxy-based). Inspection steps are also different when the FortiGate is operating in NGFW Policy mode.

This guide describes what happens to a packet as it travels through a FortiGate running FortiOS 7.6 and higher.

The FortiGate performs the following 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.

How this guide is organized

This guide contains the following sections:

- [Parallel Path Processing](#) introduces the concept of Parallel Path Processing.
- [Packet flow: NGFW Profile mode with no NP offloading](#) describes packet flow through a FortiGate or a FortiGate VDOM in NGFW Profile mode with no NP offloading.
- [Packet flow: NGFW Profile mode with flow-based inspection](#) describes flow-based packet flow in NGFW Profile mode with no NP offloading.
- [Packet flow: NGFW Policy mode](#) describes packet flow in NGFW Policy mode with no NP offloading.
- [Packet flow: first packet of an NP session](#) the first packet in a new session that can be offloaded is processed in much the same way as on a FortiGate with no network processors.
- [Packet flow: NP-offloaded session](#) describes the much simpler packet flow for a packet from an offloaded session.

Parallel Path Processing

Parallel Path Processing (PPP) uses NGFW mode (Profile or Policy) and 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 such as HTTP, email, and so on that may contain security threats. Many UTM/NGFW processes are offloaded and accelerated by CP9 or CP10 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 NP7) much of the traffic that does not require UTM/NGFW processing can be offloaded to the NP7 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 CP9 and CP10 content processors, see [NTurbo and IPSA](#) in the [Hardware Acceleration Guide](#).

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 CP9 or CP10 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. 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 where the actual destination address is. 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 uses a type of policy routing that performs route selection, load balancing, and failover among two or more routes. SD-WAN can consider various ingress criteria such as the source and destination address, user group, application type, and type of internet service before matching an SD-WAN rule and making a routing decision. In particular when the ingress criteria involves application type, SD-WAN uses the Internet Services Database (ISDB) and Application Control to select a route in the following way:

- SD-WAN uses Application Control to compare 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

Stateful inspection occurs in Layer 3 and Layer 4 to determine whether a packet's source and destination address, source and destination port and the protocol state matches what the firewall expects on an interface. For example, when a TCP SYN packet arrives, the FortiGate understands this packet is the first packet of a TCP connection, and that a policy lookup is required to determine whether the traffic can pass. On the other hand, when a TCP ACK packet arrives, the FortiGate must verify whether this matches any known session in the session table based on the state of the session. 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.

Policy lookup

When a packet arrives that is determined to be the first packet of a session, the FortiGate must perform a policy lookup to match a firewall policy that fits the criteria. By now, the FortiGate has information about the packet source address and interface, destination address and interface, source and destination ports. This information can be used to match the kernel iproute table (policy table) to determine if this packet matches a policy. Subsequently, the action specified in the policy table can be taken on the packet.

If the packet matches and the action is allow, a new session is created and stateful information about the session is also added to the session table. The session is also tagged with the UTM/NGFW profiles that must be applied and session offloading that might be available.

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).

Session management

While a session is open, packets arriving and matching the session will be inspected and offloaded as established for the session. When the FortiGate processes the final packet in the session, 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.

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 | • MMS |
| • H323 | • PMAP |
| • RAS | • SIP |
| • TNS | • DNS-UDP |
| • TFTP | • RSH |

- | | |
|--|---|
| <ul style="list-style-type: none">• RTSP• FTP | <ul style="list-style-type: none">• DCERPC• MGCP |
|--|---|

User authentication

User authentication applied at the security policy level takes place after policy lookup. Users must be authenticated, then authorized by a policy that allows the user or user group. If allowed, a packet from this source IP is allowed to establish a session through the security policy.

Device identification

If device detection is enabled on the source interface, device identification is applied to devices connecting from the source interface.

Agentless VPN

Agentless VPN traffic is treated like special management traffic that arrives on the FortiGate interface on the Agentless VPN destination port. Users reaching the Agentless VPN portal are required to authenticate before entering the authorized portal page. Additionally, policy lookup must take place before users are allowed to access the protected resources.

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, authentication, SNMP queries, and so on. Management traffic can also be implicitly allowed or blocked based on whether the service is active and enabled. For instance, if SNMP queries are enabled, the FortiGate will listen on the SNMP port. Otherwise, the port is disabled. You can also configure custom ports and their access permission on the Local In Policy list.

UTM and NGFW Profile or Policy mode

UTM can apply NGFW in Profile or Policy mode.

- In **NGFW Profile mode**, the kernel handles stateful inspection and policy matching before passing traffic to either the flow engine (IPS process) or the proxy engine (wad process) for UTM/NGFW inspection. By the time the flow or proxy engine receives the packet, it is clear which policy is the best match and which security profiles should be applied to the policy. If there are any changes to the matched policy, it is caused by the session being flagged for re-evaluation due to changes to the configuration (e.g. policy changes), or changes to network conditions (e.g. routing changes).

- In **NGFW Policy mode**, UTM inspection is applied through security policies that take into account the application and the URL category as policy matching criteria. The kernel performs matching of the SSL inspection and authentication policy, before passing the traffic to the IPS Engine for application and URL category detection, and security policy matching.

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 security policy: Flow-based (single pass architecture) or proxy-based. Some UTM/NGFW processes can be offloaded and accelerated by CP9 or CP10 processors.

Single pass flow-based UTM/NGFW inspection identifies and blocks security threats in real time as they are identified using single-pass filtering and pattern matching to identify possible attacks or threats. Packets going through flow-based inspection are passed to the flow engine (aka IPS Engine) for processing.

Proxy-based UTM/NGFW inspection is handled by proxying the connecting between the client and the server. As a proxy, FortiGate establishes a connection to the server on behalf of the client in order to inspect the complete traffic. Though stream-based approaches are also employed on the AV engine to produce quicker results and to handle larger files. Packets going through proxy-based inspection are passed to the wad proxy for processing.

CP9 and CP10 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 CP10, CP9, CP9X Lite, and CP9 Lite processors.

For more information about content processors and their capabilities, refer to [Content Processors](#) in the [Hardware Acceleration Guide](#).

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

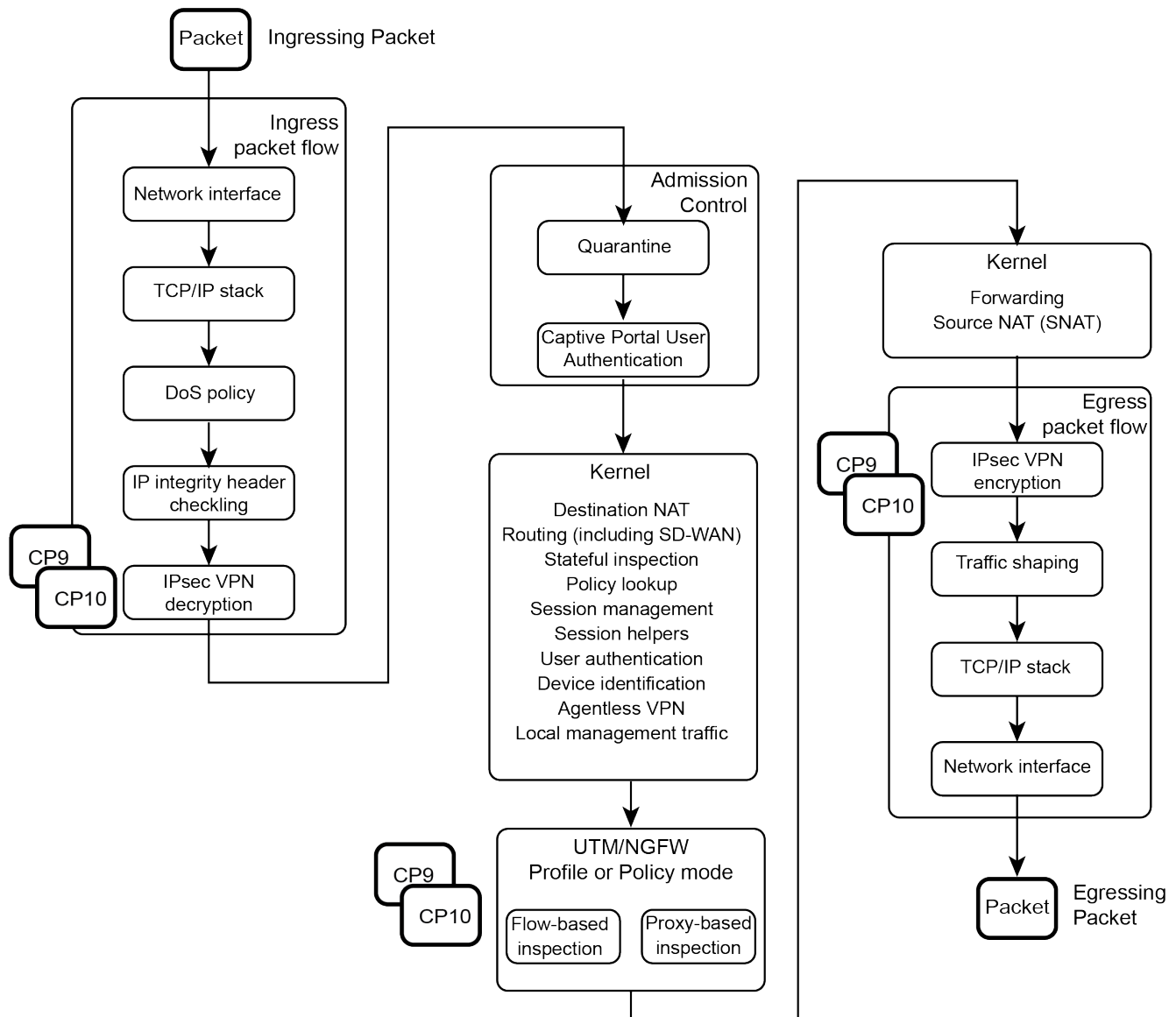
Before exiting the FortiGate, outgoing packets that are entering an IPsec VPN tunnel are encrypted and encapsulated. IPsec VPN encryption is offloaded to and accelerated by CP9 or CP10 processors.

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

Packet flow: NGFW Profile mode with no NP offloading

For a FortiGate operating in NGFW Profile mode, this section describes the steps a packet that is not offloaded by NP processors goes through as it enters, passes through, and exits from a FortiGate.

In NGFW Profile mode, the kernel handles stateful inspection and policy matching before passing traffic to either the flow engine (IPS process) or the proxy engine (wad process) for UTM/NGFW inspection. By the time the flow or proxy engine receives the packet, it is clear which policy is the best match and which security profiles should be applied to the policy. If there are any changes to the matched policy, it is caused by the session being flagged for re-evaluation due to changes to the configuration (e.g. policy changes), or changes to network conditions (e.g. routing changes).



Packet flow: NGFW Profile mode with flow-based inspection

For a FortiGate operating in NGFW Profile mode, flow-based inspection identifies and blocks security threats in real time using single-pass filtering and pattern matching.

If a firewall policy is configured for flow-based inspection, most security profiles can be applied except for Video filtering, Inline CASB, Web Application Firewall and SSH filtering. Flow-based inspection is performed by the IPS processes, which load the IPS engines and the AV Engines to perform inspection. As you would expect, no proxying is involved.

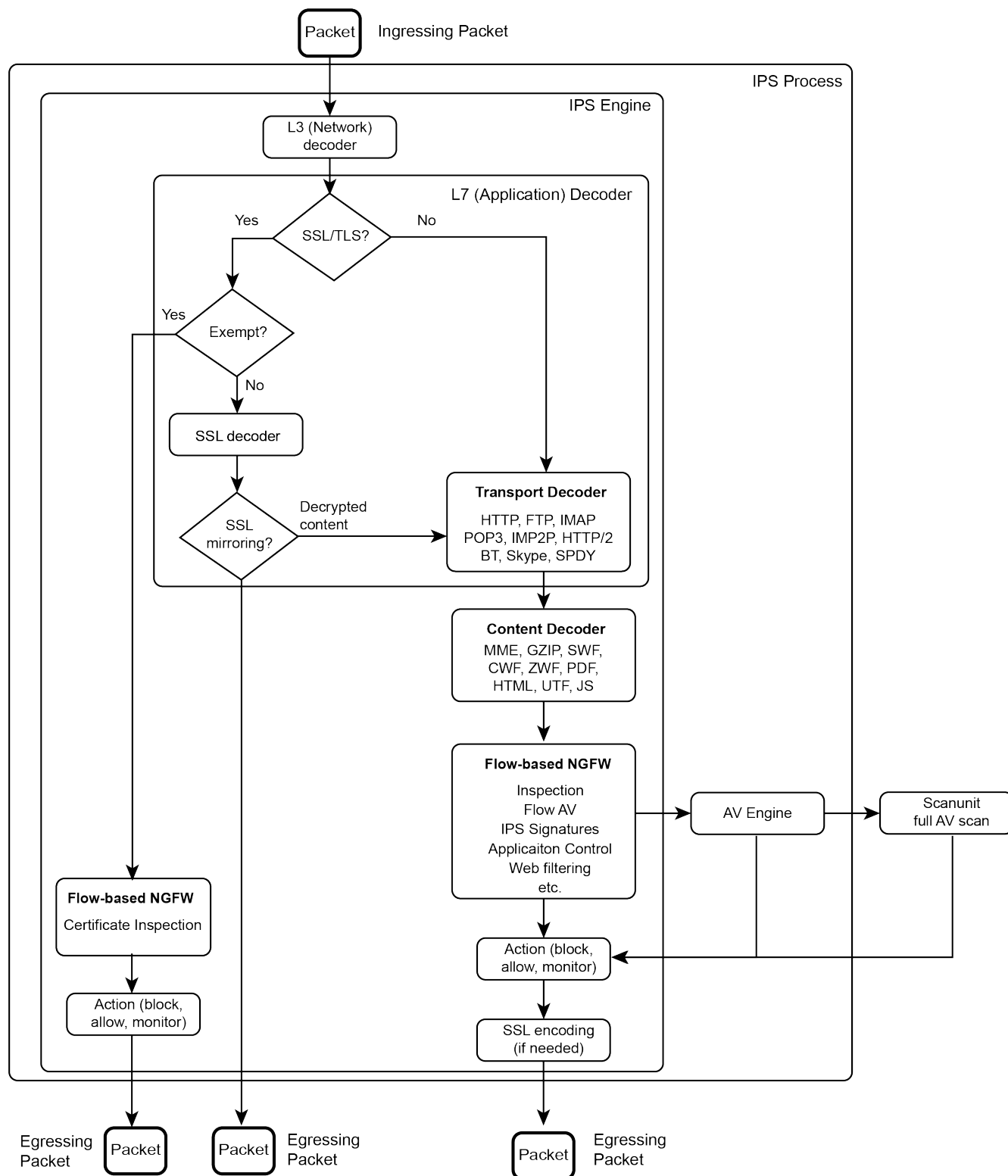


Sniffer-policy and interface-policy are supported only in flow-based inspection.

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. If SSL inspection is configured, the IPS engine also decrypts SSL packets.

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 CP9 or CP10 processors. IPS, Application Control, Local URL Filtering, Botnet checking, and flow-based DLP filtering happen together. Flow-based antivirus happens on the AV Engine loaded by the IPS process to perform stream-based scanning of the content. If a file requires advanced scanning or when the protocol is not supported, the IPS process forwards the file to the `scanunit` process for a more advanced scan.



Packet flow: NGFW Policy mode

In NGFW Policy mode, UTM inspection is applied through security policies that take into account the application and the URL category as policy matching criteria. The kernel performs matching of the SSL inspection and authentication policy, before passing the traffic to the IPS Engine for application and URL category detection, and security policy matching.

Depending on the configuration and traffic, security policy matching in NGFW policy mode may be completed on the first packet, or may require multiple packets while the IPS Engine attempts to determine the application and/or URL filter category. The IPS Engine may allow traffic to pass through and SSL decoding to occur (if applicable) when additional packets are needed to determine a security policy match. As new information is gathered about the traffic, non-matching policies are removed from the list of candidate policies. Traffic continues to flow as long as not all “allow” policies have been ruled out. This process runs iteratively until a final verdict can be found: either a single best matching policy is identified, or none are found.

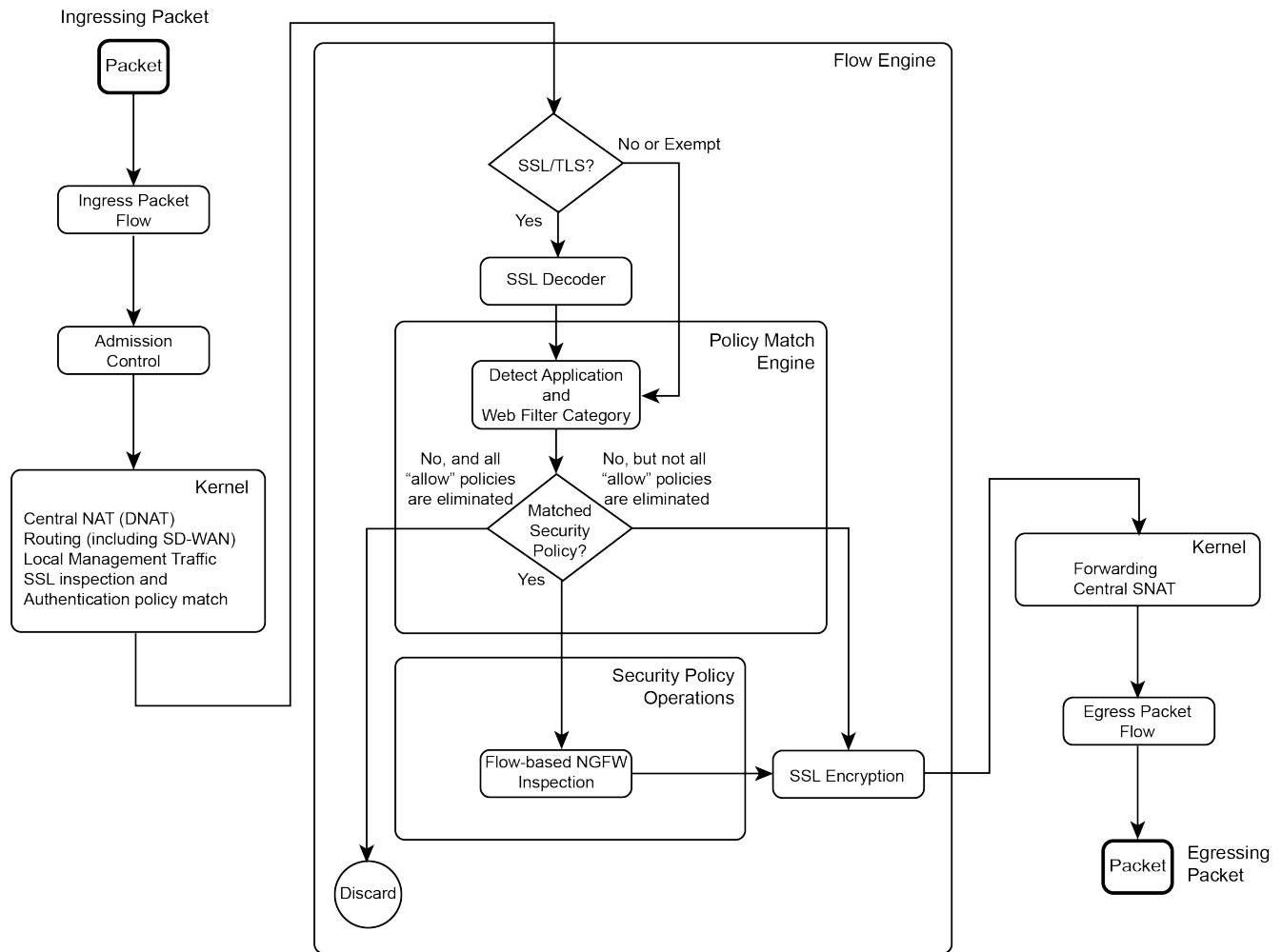
Once a security policy is identified, the configured action and applicable UTM profiles are applied to the traffic matched to that policy. Upon the completion of inspection, traffic is encrypted back (if applicable) and processed by the kernel for egress.

NGFW policy types

The following types of policies combine to make up the flow of the packet.

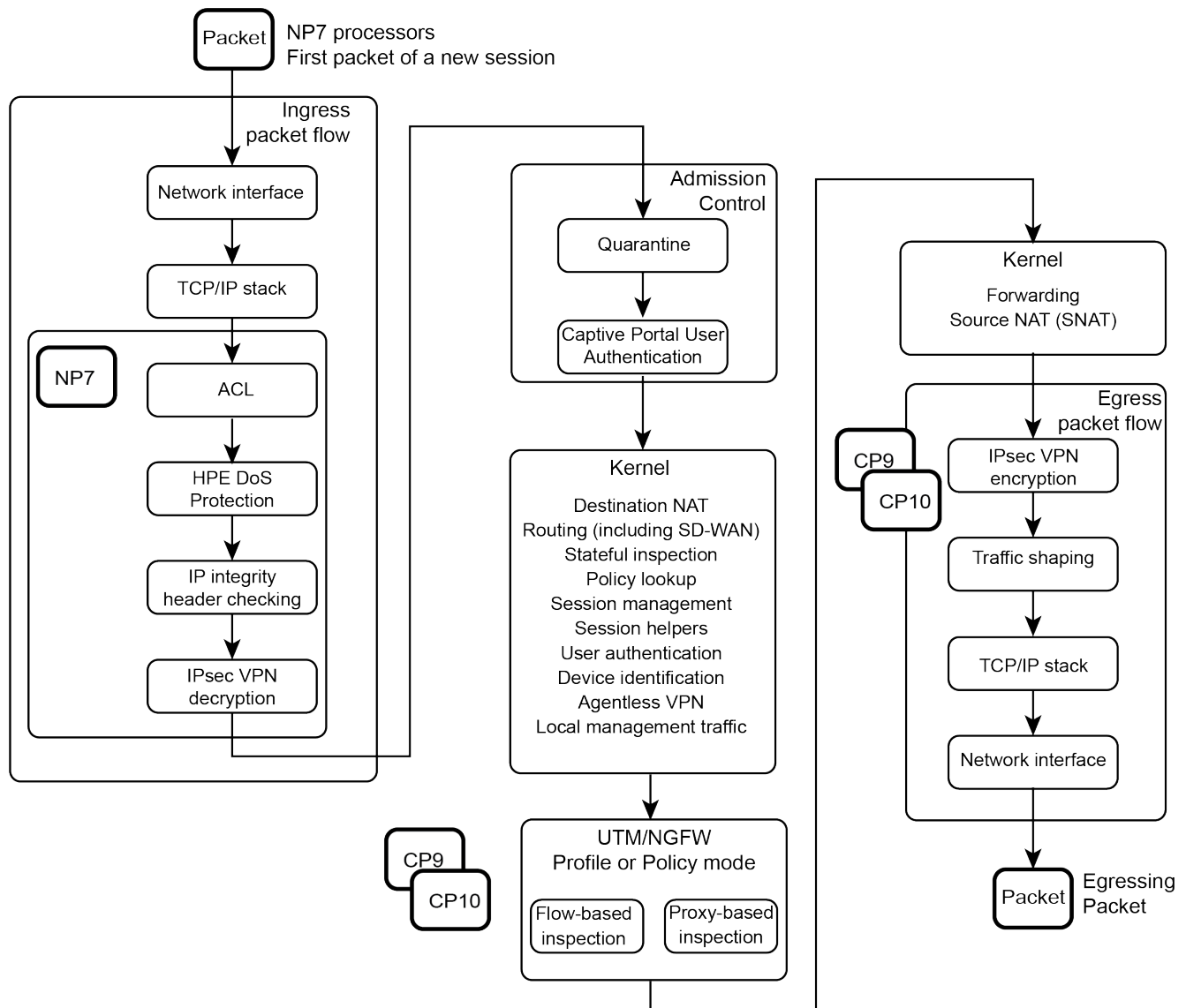
- The **SSL Inspection & Authentication policy** (`config firewall policy`) is responsible for determining the type of SSL inspection that would occur (Deep Packet Inspection, Certificate inspection, or None) as well as applying authentication to traffic matching the policy. This policy is matched and applied at the kernel level. User authentication must be configured at this policy level, as the identity of the user will be authenticated at this point. The user identity may be used by the security policy later for authorization.
- The **Security policy** (`config firewall security-policy`) is where UTM is configured for traffic based on matching criteria. In NGFW policy mode, application and web filter categories may be used as matching criteria. Furthermore, if a user or user group is configured here, authorization will take place. The user identity previously authenticated by the `authd` daemon is used to match against the user or user group here. Once a security policy is matched, UTM inspection is applied as configured in the policy.

For more information, see [NGFW policy](#).



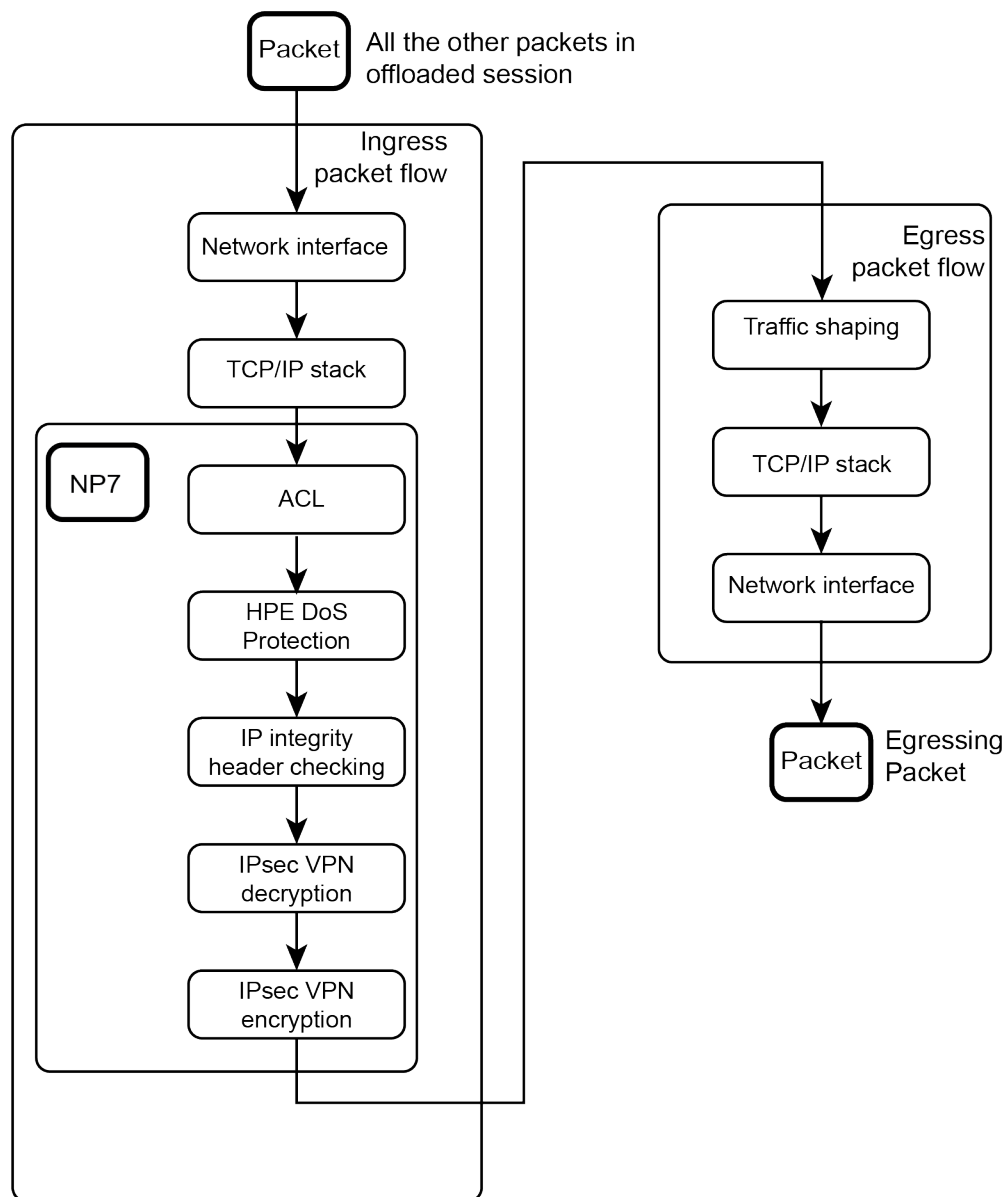
Packet flow: first packet of an NP session

On FortiGates with NP7 or NP7lite 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 NP7 processors, most sessions can be offloaded to them.



Packet flow: NP-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 NP7 processor. As well, security measures such as DoS policies, ACL, and so on are accelerated by the NP7 processor.

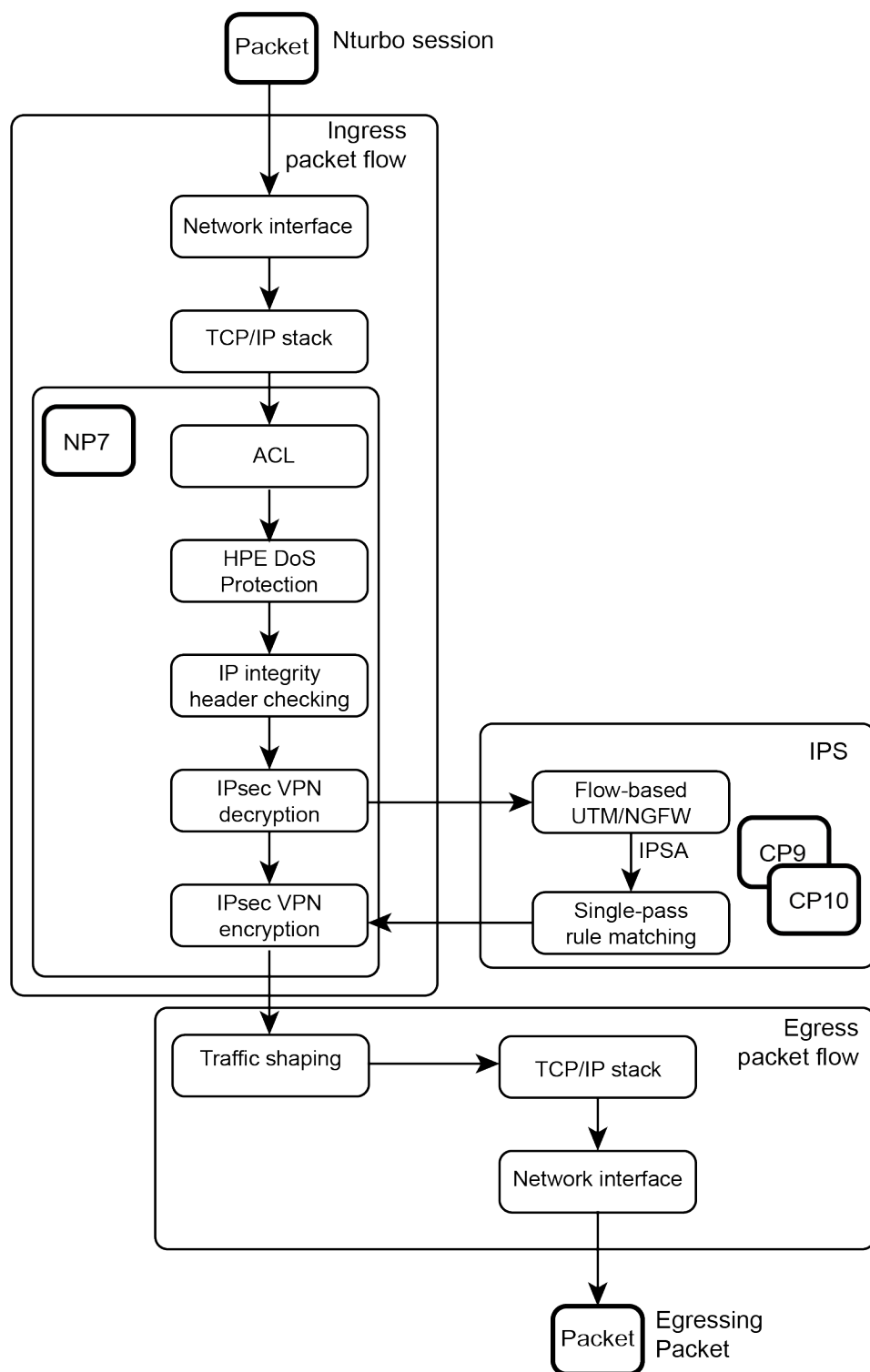


Access control list (ACL)

Access Control Lists (ACLs) use NP7 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 NP7-accelerated interfaces. ACL checking is one of the first things that happens to the packet and checking is done by the NP7 processor. The result is very efficient protection that does not use CPU or memory resources.

Packet flow: NTurbo

If your FortiGate supports NTurbo, many flow-based UTM/NGFW sessions can be offloaded to NP7 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 CP9 or CP10 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 NP7 processor.

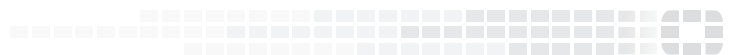
NTurbo is not compatible with DoS policies, session helpers, or and most types of tunneling. If any of these features are present, flow-based UTM/NGFW sessions are not offloaded by NTurbo.

NP7 Host Protection Engine (HPE)

The NP7 host protection engine (HPE) uses NP7 processors to protect the FortiGate CPU from excessive amounts of ingress traffic, which typically occurs during DDoS attacks or network problems (for example an ARP flood due to a network loop). You can use the HPE to prevent ingress traffic received on data interfaces connected to NP7 processors from overloading the FortiGate CPU. For more information, see [NP7 Host Protection Engine \(HPE\)](#).



FORTINET®



Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.