For the troubleshooting of any firewall, it's very important to understand the packet flow. In the FortiGate Firewall packet flow, a packet enters the FortiGate unit towards its destination on the internal network. The incoming packet arrives at the external interface. Similar steps occur for outbound traffic.

This scenario shows all of the steps a packet goes through a FortiGate without network processor (NP6) offloading.

At any point in the path, if the packet is going through what would be considered a filtering process and if it fails, the packet is dropped and does not continue any further down the path.

Fortigate firewall packet flow consists of the following modules:

Step#1 Ingress packet flow

- Interface TCP/IP stack
- DoS Sensor
- Interface policy
- IP integrity header checking
- IPsec VPN
- Destination NAT (DNAT)
- Routing

Step#2 Stateful inspection

- Local Management Traffic
- Policy Lookup
- Session Tracking
- Session helpers
- SSL VPN
- User Authentication
- Traffic Shaping

Step#3 Security Features

Flow-based inspection

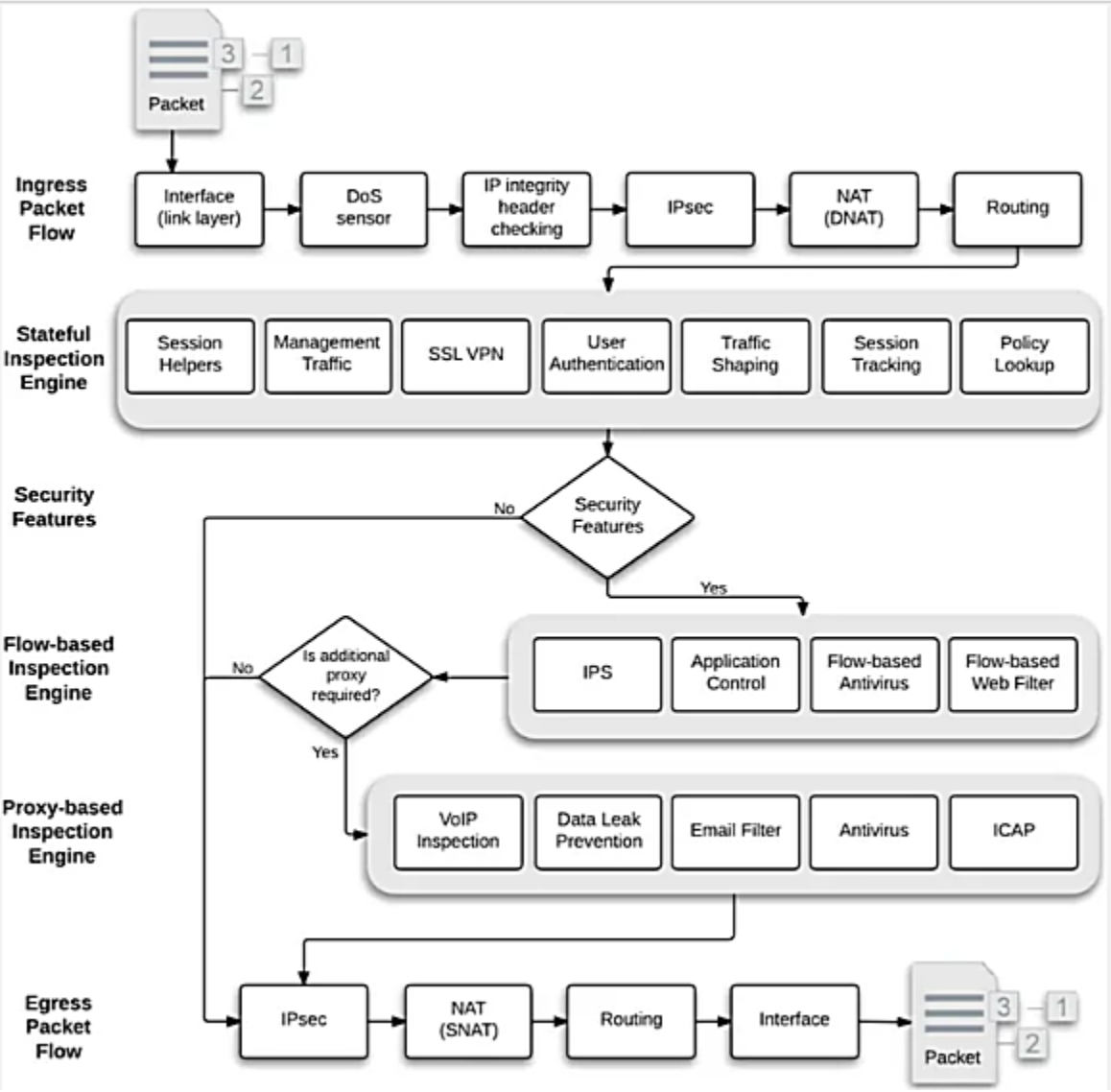
- IPS
- Application Control
- Web Filter
- DLP
- Antivirus

Proxy-based inspection

- VoIP Inspection
- DLP
- Email Filter
- Web Filter
- Antivirus
- ICAP

Step#4 Egress packet flow

- IPsec VPN
- Source NAT (SNAT)
- Routing
- Interface TCP/IP stack



FortiGate firewall packet flow

Step#1 Ingress packet flow (FortiGate firewall packet flow)

When a packet is received by an interface and enters a FortiGate, the following steps occur:

Interface TCP/IP stack
The packet enters the system, and the interface network device driver passes the packet to the Denial of Service (DoS) sensors, if enabled, to determine whether this is a valid information request or not.

DoS sensor
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 and other packets are allowed.

IP integrity header checking
The FortiGate unit 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.

IPsec VPN
If the packet is an IPsec packet, the IPsec engine attempts to decrypt it. Non-IPsec traffic passes on to the next step without being affected.

Interface policy
Interface policies apply flow-based inspection to packets received at an interface before the packets are accepted by firewall policy. Using interface policies, you can apply IPS sensors, application control and flow-based web filtering and virus scanning to traffic before it is accepted by a firewall policy. Packets can be dropped or allowed depending on the sensor or profile settings. Interface policies can also be applied to decrypted IPsec VPN traffic.

Destination NAT (DNAT)
The FortiGate unit 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 exists.

DNAT must take place before routing so that the FortiGate unit can route packets to the correct destination.

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

Step#2 Stateful inspection (Fortigate firewall packet flow)

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 identify the start and end of a session, the source/destination IP, source/destination port, and protocol.

When the first packet is 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 Wikipedia article (https://en.wikipedia.org/wiki/Stateful_firewall) for description of stateful inspection.

Local management traffic

Local management traffic terminates at a FortiGate interface. This can be any FortiGate interface including dedicated management interfaces.

In multiple VDOM modes 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. 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 that administrative traffic and can thus be detected and handled differently.

Policy lookup

The first stateful inspection step is a policy lookup that matches the packet with a firewall policy based on standard firewall matching criteria (source and destination interfaces, source and destination IP addresses, and port numbers). If the policy denies the packet it is discarded. An accepted packet continues to the next step.

Many FortiOS features are applied to traffic depending on the settings in the policy that matches the traffic as determined by the policy lookup. This includes authentication, security features, and so on.

Session tracking
Sessions are tracked in a session table after policy lookup has identified a new session.

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 session helpers: H323, RAS, TFTP, RTSP, FTP, MMS, PMAP, SIP, RSH, MGCP etc.

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.

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.

Traffic Shaping
If the policy that matches the packet includes traffic shaping it is applied as the last stateful inspection step.

Step#3 Security Features

Flow-based inspection

This identifies and blocks security threats in real-time as they are identified.

Flow-based inspection samples packets in a session and uses single-pass Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats. 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.**

All the applicable flow-based security modules are applied simultaneously in one pass. IPS, Application Control, Web Filtering and 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 inspection typically requires less processing resources than proxy inspection and since its not a proxy, the flow-based inspection does not change packets (unless a threat is found, and packets are blocked). This inspection cannot apply as many features as proxy inspection (for example, the 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.

Proxy-based inspection
Proxy-based inspection uses a proxy to inspect content traffic (VoIP, HTTP, HTTPS, FTP, email, and others) for threats. The proxy extracts and caches content, such as files and web pages, from a content session and inspects the cached content for threats. Content inspection happens in the following order: **VoIP inspection, DLP, Email Filtering, 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 content 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 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 FortiGate unit determines the action that should be taken with these ICAP responses and requests.

Read the article: https://en.wikipedia.org/wiki/Deep_content_inspection

Step#4 Egress packet flow (Fortigate firewall packet flow)

After stateful inspection and flow or proxy-based inspection the packet goes through the following steps before exiting.

IPsec VPN
If the packet is to be sent out an IPsec tunnel, it is at this stage the encryption and required encapsulation is performed.

Source NAT (SNAT)
The FortiGate unit 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.

DNAT must take place before routing so that the FortiGate unit can route the packet to the correct destination.

Routing

The final routing step determines the next hop router to send the packet to after it exits the FortiGate unit.

Interface TCP/IP Stack

Egress packets are received by the interface network device driver which forwards the packet out the interface an onto the network.

Example for Client/server connection: