# Intrusion Protection System (IPS)

FortiOS IPS employs pre-defined and custom signature-based defences to protect networks from outside attacks

Protecting your network from outside attacks

A complex network may be running many different applications and operating systems. At any one time, any number of these systems may have open network vulnerabilities. Keeping the entire system on diverse network up-to-date and fully protected can be time consuming and prone to errors. When you use FortiOS Intrusion Protection System (IPS), protecting your network provides a much easier and quicker way to stop attacks that could otherwise take advantage of vulnerabilities before a patch or fix can be applied. An intrusion protection system, also known as an intrusion prevention system or intrusion detection and prevention systems, helps to stop or block malicious activity, as well as monitor such activity.
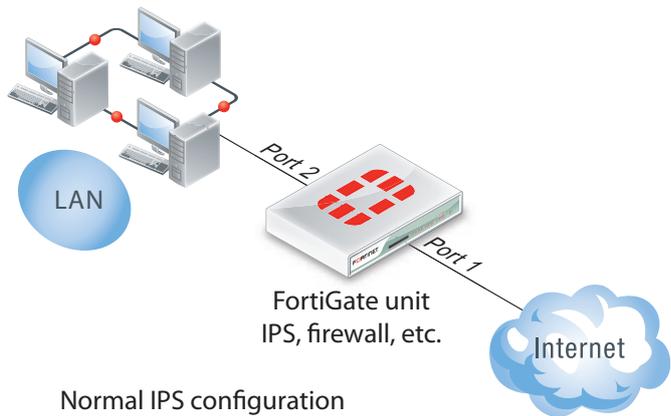
Normal IPS configuration
(FortiGate unit processes
all network traffic)

FortiOS IPS
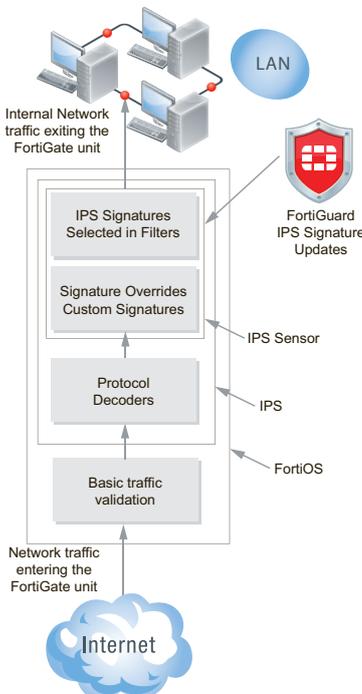
FortiOS IPS offers a wide range of tools so that you can monitor and block malicious activity. These tools are predefined signatures, out-of-band mode (or one-arm IPS mode), protocol decoders, custom signature entries, packet logging, and IPS sensors. IPS sensors provide an organized, central location of the IPS tools so that FortiOS can efficiently and quickly block or allow traffic, depending on what is stated in the IPS sensor.

Fortinet Security Processing (SP) modules such as the CE4, XE2, and FE8 provide multi-gigabit throughput increases for IPS by offloading IPS signature scanning from the FortiGate host system while maintaining all the benefits of a unified security platform. System administrators can fine tune the SP module configuration to devote more resources to IPS; which can be useful in hostile high-traffic environments.

Predefined signatures

Predefined signatures are provided to FortiOS through the FortiGuard network. These signatures are used to detect attacks and FortiOS supports more than 4000 attack signatures that can detect everything from attacks against unpatched operating system vulnerabilities to invalid checksums in UDP packets.

The FortiGuard IPS vulnerability database keeps FortiOS up-to-date with protection for new attacks as they are found. Updates can be delivered to FortiOS the moment they are released to the FortiGuard network. For more information about the FortiGuard IPS vulnerability database see the FortiGuard Center web site. A list of the latest vulnerabilities that are currently prevalent is available as well as access to the FortiGuard encyclopedia, to get more information about individual vulnerabilities in the IPS vulnerability database.

Custom signature entries

custom signature entries can be created to extend IPS protection to instances that may not be protected by standard, predefined IPS signatures. For example, IPS signatures may not be available to protect unusual or specialized applications, or uncommon platforms from known attacks. Custom signatures can be constructed to detect these otherwise unknown attacks. custom signature entries can also be used as temporary solutions to block new attacks that Fortinet has not created signatures for.

Finally, custom signature entries can be used for specialized network traffic analysis and pattern matching. For example, if a network is experiencing unusual or unwanted traffic, system administrators can use packet sniffers to monitor the traffic and understand its pattern. A custom signature can then be written to match the pattern and the custom signature can be added to an IPS sensor and set to block the unwanted traffic. Custom signatures can be very specific, for example a custom signature can be created to detect and block high rates of DNS requests to non-existing domains. This custom signature would include parameters that match the traffic as well as a rate setting to start blocking traffic only when the rate is exceeded.

FortiWiFi unit

FortiOS IPS
(Internet and
Wireless LAN Traffic)
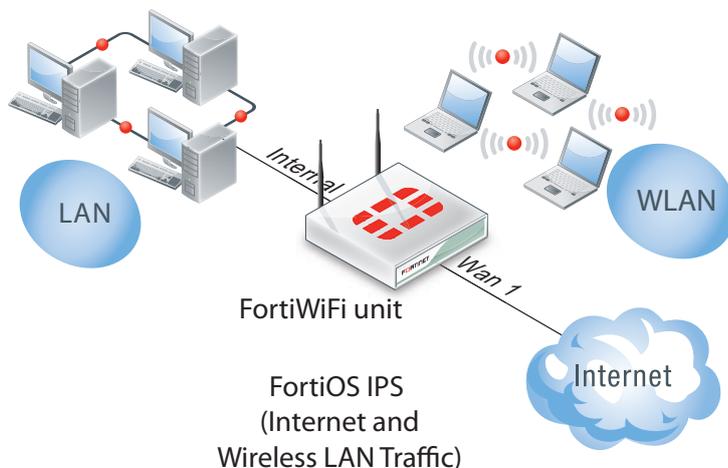
Protocol decoders

Protocol decoders help to identify abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTP packets that do not meet the HTTP protocol standard.

FortiOS displays the port or ports that are monitored by each decoder, and many decoders are able to recognize traffic by type, rather than port. FortiOS contains protocol decoders that have "auto" as their monitored port, which indicates that these types of protocol decoders can detect traffic on any port so there is no need to specify individual ports.

IPS packet logging and quarantining attackers

IPS packet logging, enabled in an IPS sensor, can be used to save packets matched by one or more IPS signatures. The packets are saved as log messages and packet contents can be viewed and analyzed using log message analysis tools. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.

IPS also provides a way to quarantine attackers and display those attackers on the Banned User List. This list displays all the users that tried to attack and that were quarantined. These attackers can be quarantined using their IP address, their IP address and the victim's IP address, or which interface the incoming attack was detected on. The attackers can also be banned for an infinite amount of time, or for only hours, minutes, or days.

IPS out-of-band sniffer mode

IPS can also be deployed out-of-band in sniffer mode, also called one-arm IPS mode. In this mode, the FortiOS IPS is operating as an Intrusion Detection System (IDS) detecting attacks and reporting them, but not taking any action against them. In sniffer mode, the FortiGate unit does not process network traffic. Instead a FortiGate interface operates in sniffer mode and is connected to a spanning or mirrored port of a switch that processes all of the traffic to be analyzed.

Out of Band IPS configuration
(also called IDS or one-arm IPS)
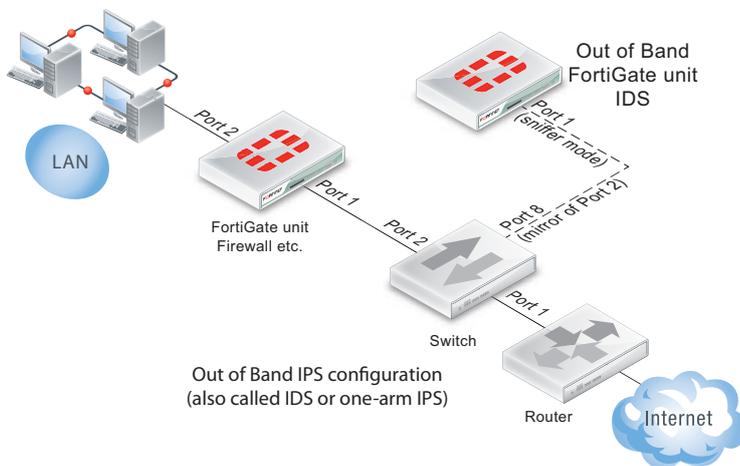
The spanning or mirrored switch port sends a copy of the switch traffic to the FortiGate interface operating in sniffer mode where it is analyzed. If the IDS detects an attack, FortiOS records log messages and sends alerts to system administrators. Since its out-of-band, IDS scanning does not affect network performance and network traffic is not affected if the IDS fails or goes offline.

IPS sensors

IPS sensors can be configured to apply specific signatures to selected traffic. The traffic to be scanned can be selected by adding specific firewall policies. The signatures to scan the traffic accepted by a firewall policy are added to an IPS sensor and the sensor is added to the policy. The sensor selects the signatures used to test traffic accepted by a firewall policy and control the actions that the IPS performs for each signature. Actions can block, pass, or reset traffic found to be an attack. IPS sensors are also used to enable logging and packet logging for each signature and to exempt addresses from scanning.

IPS sensors can also apply quarantining to prevents attacks from spreading by blocking all traffic originating from an attack source, sent to an attack destination, or received by the FortiGate interface that on which the attack was detected.

IPS sensors are populated with filters and custom signature entries. In each filter, the attributes of the signatures are selected, which include severity, target (client/server), OS, protocol, application, and tags. Specifying more or fewer attributes widens or narrows the focus of the sensor to suit individual needs. Custom signature entries can also be used to include or exclude signatures on an individual basis. These overrides can also include an action the FortiOS should take when a match is detected, logging, packet logging and filtering, quarantine attackers, and exempt address settings unique for individual signatures.