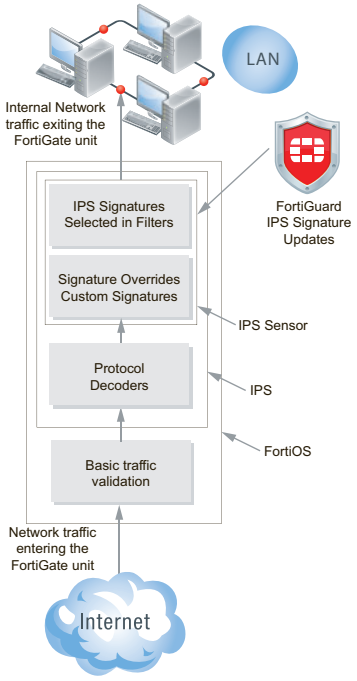
Intrusion Prevention System (IPS)

Fortinet's IPS technology protects networks from known and unknown threats by blocking attacks that attempt to take advantage of network vulnerabilities.

Protecting your network from outside attacks

Networks often support many different applications, protocols and operating systems at the same time. These diverse infrastructures can be time consuming to keep up-to-date and fully protected, causing the risk of external attack to be high.



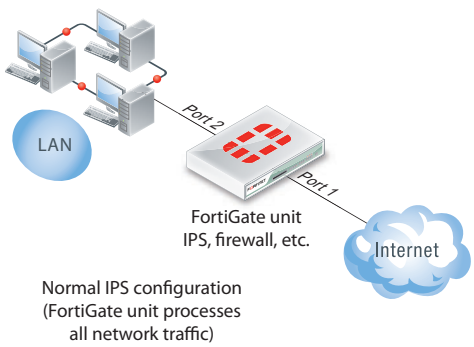
FortiOS IPS

FortiOS's Intrusion Prevention System (IPS) technology protects your network against attacks by looking for and blocking network-level threats before they can reach your potentially vulnerable network devices. FortiOS offers a wide range of tools to monitor, block and analyze malicious activity, including: IPS signatures, filters and sensors, quarantines, packet logging, out of band sniffer mode and options for hardware acceleration.

FortiOS IPS supports both IPv4 and IPv6 traffic, as well as SSL inspection of encrypted traffic.

IPS signatures

IPS signatures are the foundation FortiOS IPS. The FortiGuard Intrusion Prevention Service provides Fortinet customers with the latest defenses against stealthy threats over the network. FortiGuard uses a constantly updated database that can identify more than 6000 known threats and also provides behavior-based heuristics that enable your FortiGate to recognize threats for which no signature has yet been developed.

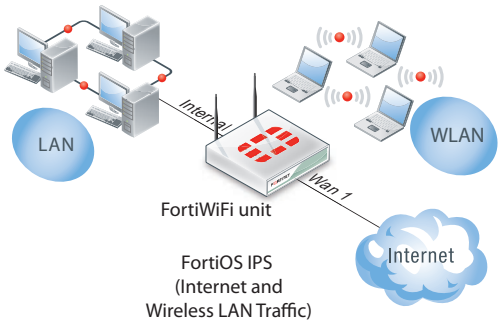


Normal IPS configuration (FortiGate unit processes all network traffic)

Customers can construct their own custom signatures to detect and protect against attacks for which Fortinet has not yet created signatures, providing temporary protection until a FortiGuard signature is created. Custom signatures can also be used for specialized network traffic analysis and pattern matching if a network is experiencing unusual or unwanted traffic.

IPS filters and sensors

IPS filters can be customized to provide different levels of protection by grouping signatures together. Sensors are then used to group filters and apply them directly to network traffic. Advanced IPS filter creation tools make it easy to sort through the thousands of IPS signatures to find the ones you want to add to a sensor.

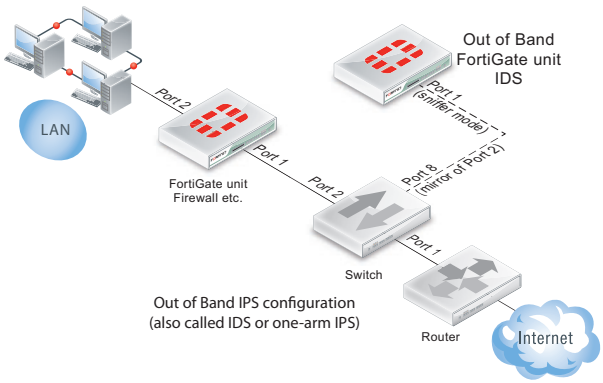


Quarantine

The IPS quarantine function extends protection by quarantining all activity from an identified attacker for an extended period of time, or even permanently. Quarantining prevents future attacks from known attackers and can be used to protect potentially vulnerable servers until a more permanent defense can be put in place. You can also use the quarantine function to protect a vulnerable server or to block all traffic received by an interface on which the IPS has detected attacks.

Packet logging

IPS packet logging saves packets for detailed analysis when an IPS signature is matched. Saved packets can be viewed and analyzed on the FortiGate unit or by using third-party analysis tools.



Out of band sniffer mode

In out of band sniffer mode (or one-arm IPS mode), IPS operates 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 and instead is connected to a spanning or mirrored switch port, or a network tap. If an attack is detected, log messages can be recorded and alerts sent to system administrators.

Because sniffer mode does not process traffic on the original port, IDS scanning does not affect network performance and network traffic is not affected if the IDS goes offline.

Hardware acceleration

IPS functions can be offloaded from the FortiGate's general purpose CPU to content processors (CP7 and CP8), network processors (NP4 and NP6) and Security Processors (SP3). All FortiGate units can accelerate IPS processing with content processors. Exceptional IPS hardware acceleration is available from FortiGate units with NP processors (such as the FortiGate-3700D) and those with security processors (such as the FortiGate-5101C).

The FortiGuard Center

The FortiGuard Center shows information on all the most recent FortiGuard news, including information concerning zero-day research and hot intrusion detections. Research papers are also available, concerning a variety of current security issues.

To view recent FortiGuard Intrusion Prevention Service developments, go to http://www.fortiguard.com/static/intrusionprevention.html.