Intrusion Prevention System (IPS)

https://campus.barracuda.com/doc/72516336/

To report and instantly block suspicious network traffic from passing the firewall, the Intrusion Prevention System (IPS) actively scans forwarded network traffic for malicious activities and known attack patterns. The IPS engine analyzes network traffic and continuously compares the bitstream with its internal signature database for known attack patterns. To increase security, the IPS system offers TCP stream reassembly to prevent IP datagram fragmentation before packets are scanned for vulnerabilities. The IPS engine can also inspect HTML requests passing the firewall.

IPS must be globally enabled on the firewall. However, you can enable or disable IPS for each firewall rule. Enabling IPS on a per-rule basis lets you select which network traffic is scanned for threats. For example, you can choose to enable IPS scanning only for network traffic that travels from and to the DMZ. When IPS is enabled in a firewall rule, the default IPS policy of Report Mode or Enforce Mode is used. In Report Mode, the firewall reports detected attacks instead of immediately blocking network traffic. This mode is recommended after the initial deployment of IPS to prevent traffic from being incorrectly blocked. However, you can prevent false positives when the IPS engine operates in Enforce Mode by creating IPS exceptions.

IPS Features

TCP Stream Reassembly

The firewall engine provides support for TCP Stream Reassembly (SRA). In general, TCP streams are broken into TCP segments that are encapsulated into IP packets. By manipulating how a TCP stream is segmented, it is possible to evade detection, for example by overwriting a portion of a previous segment within a stream with new data in a subsequent segment. This method allows the hacker to hide or obfuscate the network attack. The firewall engine receives the segments in a TCP conversation, buffers them, and reassembles the segments into a correct stream by, for example, checking for segment overlaps, interleaved duplicate segments, invalid TCP checksums, and so forth. Afterwards, the firewall engine passes the reassembled stream to the IPS engine for inspection.

URL Obfuscation

The IPS engine provides various countermeasures to avert possible network attacks based on the following URL encoding techniques:

- Escape encoding (% encoding)
- Microsoft %u encoding
- Path character transformations and expansions (/./ , //, \ )
- Premature URL ending
- Long URL

- Fake parameter
- TAB separation
- FTP evasion

The IPS engine is able to avert FTP exploits where the attacker is trying to evade the IPS by inserting additional spaces and Telnet control sequences in FTP commands.

TCP Split Handshake

The IPS engine provides an evasion countermeasure technique that is able to block the usage of TCP split handshakes attacks. Although the TCP split handshake is a legitimate way to start a TCP connection (RFC793), it can also be used by hackers to execute various network attacks by gaining access to the internal network by way of establishing a trusted IP connection, thus evading firewall and IPS policies.

Configuring and Managing IPS

For step-by-step instructions on how to configure and manage IPS, see the following articles:

- How to Check the IPS Security Subscription Status
- How to Configure IPS Policies
- How to Configure the Intrusion Prevention System (IPS)
- How to Manage Threats