

What is Intrusion Prevention?

An intrusion prevention system is any device which exercises access control to protect computers from exploitation. "Intrusion prevention" technology is considered by some to be an extension of intrusion detection (IDS) technology, but it is actually another form of access control, like an application layer firewall.

Intrusion prevention systems (IPS) were invented to resolve ambiguities in passive network monitoring by placing detection systems in-line. A considerable improvement upon firewall technologies, IPS make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done. As IPS systems were originally a literal extension of intrusion detection systems, they continue to be related.

Intrusion prevention systems may also serve secondarily at the host level to deny potentially malicious activity. There are advantages and disadvantages to host-based IPS compared with network-based IPS. In many cases, the technologies are thought to be complementary. An Intrusion Prevention system must also be a very good Intrusion Detection system to enable a low rate of false positives. Some IPS systems can also prevent yet to be discovered attacks, such as those caused by a Buffer overflow.

Due to the fact that a high amount of new security vulnerabilities are discovered on a daily basis it can be a hassle for the end user to keep all their servers up to date with the latest patches. In many cases the patches to rectify the security holes can be delayed days, weeks or even months. In some critical environments the installation of patches can break functionality and this can result in a direct loss for the customer if their production systems are not performing optimal due to a dysfunctional patch.

How does Intrusion Prevention work?

Intrusion Prevention is an advanced intelligent way of scanning the different layers for vulnerabilities. It consists of many techniques to ensure the optimal and most advanced security level.

This includes:

- Database updated multiple times daily for the latest signature definitions.
- Traffic abnormalities are being identified and if consisting of dangerous content will be blocked.
- Port Scans. Most likely when a port scan is being performed an attack will follow in a matter of minutes afterwards.
- Denial of Service attacks protection – A successful Denial of Service attacks can cause your system to crash or be permanently crashed.
- Protection for known Buffer overflow attacks and or other exploits being launched.
- Zero Day Protection – This module protects for zero day known and unknown vulnerabilities
- Wide protection for Web,Mail,Ftp, Windows, Linux, BSD, UNIX, Routers, Firewalls, Databases such as DB2, Oracle, MySQL, MSsql, Postgresql and more.