



Intrusion Prevention System (IPS)

Introduction

The Intrusion Protection Systems (IPS) is a proactive defence tool against active attacks on computers and networks. This network device monitors a network or system activities to find malicious or unwanted behaviour and can react to block those activities.

Evolution of IDS to IPS

Originally, intrusion attempts were detected after-the-fact by Intrusion Detection System (IDS). The early systems were reactive systems and attacks could penetrate the network and cause damage without timely analyst intervention.

To provide a proactive approach to intrusion attempts, vendors created the Intrusion Prevention System (IPS).

Generally, IPS devices are placed directly in line between a workstation and the internet. The IPS is then able to inspect the traffic as it goes to and from the internet and make a decision whether to allow or block it. An IPS can therefore identify and halt a malicious threat before it has an opportunity to breach the network.

An IPS can itself be vulnerable to attack, if it is not correctly configured and maintained. An IPS is effectively a computer system running an operating system and applications specific to the identification function. Departments are recommended to ensure the updates and patches for IPS' are current and applied regularly. A compromised IPS may allow malicious traffic through that would potentially introduce risk to the network.

Benefits and Limitations of an IPS

Benefits

An IPS can include any product or method used to keep attackers from gaining access to a network, such as firewalls and anti-virus software.

Limitations

An IPS can signal false-alarms due to the similarity between valid information and malicious attacks. This potentially lowers the credibility of the IPS' reporting security control mechanism.