

# intrusion detection

# V intrusion prevention



Intrusion Detection Systems are the burglar alarms of the network security world, while Intrusion Prevention Systems can additionally be programmed to respond to an attack. This article describes the concepts behind both IDS and IPS technologies, and compares and contrasts their different approaches.

## Introduction

Firewalls have long been the mainstay of network security. Their role is to control access to network components or services in accordance with the policy defined by the system owner. They achieve this by examining the headers of IP packets and making decisions accordingly. However, this does leave the host system potentially vulnerable to attacks against its permitted services - such as exploits against a publicly-accessible web server - because in general no account is taken of the content of the packet, only that it corresponds to a permitted service.

Intrusion Detection systems (*IDS*) are the 'burglar alarms' of network security, designed to go off when activated by a particular trigger. In common with burglar alarms, the response then often depends on past experience - if your neighbour's house alarm has gone off by mistake five times in the last week, do

you recognise the significance on the sixth occasion or just ignore it? Alternatively, the response may depend on the availability of someone with the right experience to analyse the event and take appropriate action.

Intrusion Prevention systems (*IPS*) also aim to detect indications of an attack in progress, but they can respond automatically and in a predefined manner to prevent an attack from impacting the target system. This ability to respond means an IPS offers the potential to enable a system to remain on-line despite being under attack.

## Intrusion Detection Systems

This article only summarises the principles of IDS, but interested reader may wish to refer for further information to the NISCC Technical Note 05/02: *Understanding Intrusion Detection Systems*, which is available on our web site (<http://www.uniras.gov.uk>).

IDSs come in two main flavours, Network-based IDS (or *NIDS*) and Host-based IDS (or *HIDS*). As their names imply, NIDS systems examine data on the Network link being monitored for signs of attack, whilst HIDS reside on a Host machine (for example a file server or a web server) and examine transactions with that particular Host for signs of malicious activity (this may be achieved using data passed to the application or logs generated by the application or server). IDSs are generally 'passive' - they observe and report on potentially malicious activity rather than actively responding to stop an attack.

There are three main mechanisms by which IDSs attempt to identify attacks:

- **Rule based:** in this architecture the IDS contains a library of '*signatures*' that correspond to known attack vectors. For example, a signature for detecting the actions of the *Code Red* worm may involve detecting a request for 'default.ida' over HTTP. Each data item - for example, a packet that passes 'on the wire' (i.e. in transit on the network) or data that arrives at a particular host - is compared to the signature library and an alert or log entry is generated as appropriate.
- **Anomaly detection:** this category of IDS attempts to determine the presence of an attack based on the

presence of data items or activities that fall outside the 'normal' pattern of behaviour. For these to be effective, the system needs **'training'** to learn what constitutes normal behaviour.

- **Protocol Analysis:** attempts to detect protocol elements that do not conform to the appropriate standard, anomalies that may indicate an attempted attack.

Of these differing modes of operation, the signature based approach to IDS is the more mature technology, and most commercially available IDS systems fall into this category.

**NIDS systems** are usually deployed where they can view the most traffic, or at least the traffic on those segments that are considered most important. On a segmented network, they can be connected to a monitoring port on a switch, although data aggregation can result in problems for the IDS. HIDS would normally be deployed on the more important servers within a network. Figure 1a shows an example of a deployment architecture, the idea being that IDSs are transparent to the end user and do not add any processing overhead to the data passing between the end points of a transaction.

**Signature based IDS systems** are very good at detecting known attacks, but they are not so at detecting 'new' attacks due to the time delay between a new vulnerability or attack being discovered, and a vendor releasing a signature to detect it. Ideally, the IDS should provide an interface by which administrators can define their own signatures relevant to local conditions.

When discussing IDS, it is impossible to avoid considering 'false positives', which are alerts generated by an IDS due to benign activity. Signature based IDSs are prone to generating false positives, though a good understanding of the network being monitored and a period of 'training' should ensure that these are minimised.

**Anomaly detection engines** are designed to detect attacks through comparison with a baseline of the normal system behaviour. This approach will always be more prone to 'false positives' because a statistical metric is used to determine 'good' and 'bad'; thus benign traffic from an application that wasn't in the 'training set' of the IDS could be flagged as anomalous and raise an alert.

### Intrusion Prevention Systems

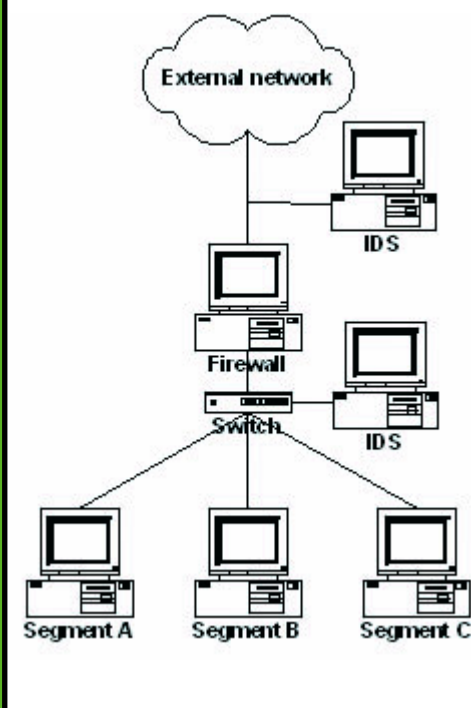
IPSS, which are relatively new to the market, respond in a proactive manner when they detect a potential attack. The response may take a number of different forms, such as:

- logging the event (like a standard IDS);
- blocking the transit of the data;
- resetting the connection between source and destination;
- limiting the rate of connection between source and destination;
- re-writing firewall rules for particular conditions.

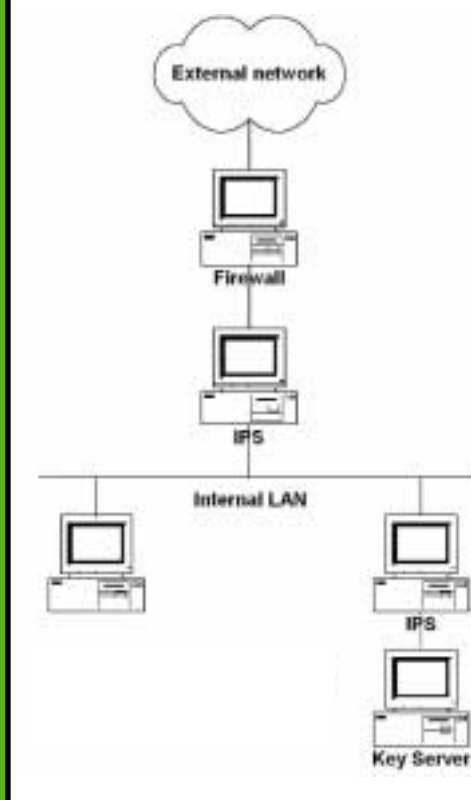
IPSS are designed to sit 'in-line' with the target system (see figure 1b), effectively acting as a 'bridge' between the internal systems requiring protection and the rest of the network. In this architecture all traffic must pass through the IPS device, which inspects all the data for signs of attack (against the signatures it has been configured to use).

An immediate issue with this type of architecture is the potential consequence of the IPS crashing, which may effectively cut off the target system from the rest of the network. Depending on the nature of the business, it may be preferable for the system to fail 'open' thereby providing continued availability of the network services at the cost of removing the additional layer of security provided by the IPS.

**Fig 1a** Possible deployment architecture for NIDS



**Fig 1b** Possible deployment architecture for IPS



IPS systems do have the potential to form a valuable tool for network security, and they provide a means for reducing the amount of attack traffic reaching vital systems within a network.

The different types of IPS system that are available commercially include:

- **Network (or Gateway IPS):** sit in the network line, monitoring all network traffic for malicious activity, and are able to block packets that are designated as attacks;
- **Web server shields:** sit on the web server, effectively 'wrapping' the server software. Attacks are detected by monitoring the activity undertaken by the web server account;
- **Web application firewalls:** sit in the network path and inspect the contents of packets destined for any web server or web application for signs of attack.

Trusted operating systems can also be considered to be a form of IPS because they implement access control functionality and enforce user privilege restrictions.

Attack detection within the IPS can be achieved in several ways, including:

- **Signature Detection:** the IPS holds a library of signatures (similar to IDS) corresponding to known attacks that it compares with data on the wire. Ideally, the administrator should have the capacity to define additional signatures relevant to local conditions.
- **Protocol Analysis:** here the IPS compares the elements of the data on the wire with protocol definitions that it understands. Any deviations from the accepted protocol

definition may indicate an attack, the IPS then responding in the manner in which it has been configured.

- **Anomaly Detection:** similar to IDS, uses techniques to determine anomalous traffic and then respond.

Issues with detection of attacks within IPSs are similar to those within IDSs - the time delay between new attacks and signature availability, false positive rates, etc. However, in this instance the consequences of 'false positives' may be more serious, especially if the IPS is configured to block traffic from a source in the event of an 'attack' being detected.

IPS systems have the potential to form a valuable tool for network security, and for providing a means of reducing the amount of attack traffic reaching vital systems within a network. Their use to filter out traffic corresponding to known worms (such as *CodeRed* and *Nimda*) may, for example, greatly reduce the load on a web server. However, this must be offset against the risk of misidentification of attacks on service 'availability'. In common with an IDS, implementing an IPS is not a 'set and forget' task. Careful performance monitoring is necessary both to ensure that an IPS is meeting its objectives, and that the administrators remain aware of what is happening in their networks.

## Summary

IDSs and IPSs are useful tools in the system administrator's armoury for helping to ensure the security of their networks. The choice of which system to deploy will depend on a number of local considerations, such as:

- cost;
- which parts of the network are to be protected by the deployed system;
- availability of resource to administer the system;
- requirement for alerts or a system making proactive defence responses;
- availability of resource to investigate the causes of alerts generated by IDS systems;
- applicability of detection techniques to local network services; and.....
- the degree of tolerance to loss of service.

Neither type of system can be considered to be 'set and forget'. Each requires monitoring to ensure that it meets its objectives; that signature libraries remain up to date and accurate; and that administrators are aware of what is happening in their networks. Where an IPS is used to respond to an attack proactively, administrators must be aware of any configuration changes made by the IPS (such as addition/modification of firewall rules) to their network.

**N.I.S.C.C.** (<http://www.niscc.gov.uk>)