

IP Spoof Attack Prevention Overview

Every IP packet includes the destination address (where the packet is going) and the source address (where the packet came from). The routers that provide Internet communication between distant computers determine the best route for the IP packet using only the destination address and typically ignore the source address.

Attackers, who typically do not want you to know where an attack is coming from, can fake the source address of a malicious IP packet (by modifying the packet headers) so that the packet appears to come from a trusted system. The use of a fake IP address is called *IP spoofing*. You can configure the IDP system to detect these irregularities.

To detect attacks that attempt to spoof the addresses of hosts in your protected network, you can associate IDP traffic interfaces with the addresses of hosts in your protected network. IDP then detects an IP spoof attack if:

- An incoming packet uses an IP address that belongs to a network object on your internal network.
- An outgoing packet uses an IP address that does not belong to a network object on your internal network.

You can configure whether IDP drops or logs the session with a spoofed IP address.

Related Topics The following related topic is included in the *IDP Administration Guide*:

- Modifying the IDP Device Configuration

Published: 2010-01-12