

Configuring Antispoof Settings in Intrusion Detection and Prevention Devices (NSM Procedure)

Antispoof settings are valid for standalone IDP sensors only. You can assign address objects to specific interfaces on your sensor. You can set the sensor to log or drop any connections that do not match the permitted address objects for that interface.

In addition, you can set the sensor to check incoming IP addresses against the permitted address objects for other interfaces. If the sensor detects an IP address entering the wrong interface, it can log or drop that connection.

To configure antispoof settings:

1. In NSM Device Manager, double-click the IDP device you want to configure antispoof settings. The device configuration editor appears.
2. Click **Anti-Spoof Settings**.
3. Click **New** to display the Anti-Spoof Settings dialog box.
4. Configure antispoof settings using Table 1.
5. Click **OK**.

Table 1: IDP Device Configuration: Anti-Spoof Settings

Setting	Description
Interface Name	Select a forwarding interface to configure.
Logging	Enable logging for spoofed IP address.
Alarm	Enable alerts for spoofed IP addresses.
Check Other Interfaces	Indicate whether the device should check the status of other interfaces when determining spoofing.
Action	Specify the action for the IDP device to take: None or Drop Packet .
Network Objects	Browse and select the address objects you associate with the selected interface.

- Related Topics**
- [Configuring Additional Intrusion Detection and Prevention Features Overview](#)
 - [Adding Intrusion Detection and Prevention Devices in NSM Overview](#)
 - [NSM and Intrusion Detection and Prevention Device Management Overview](#)

Published: 2009-08-20