

## **Example: Applying Antispoof to a Web Server and Database Server (NSM Procedure)**

---

To apply antispoof settings to a Web server and a database server:

1. Add your Web server and database server to the list of address objects.
2. Connect the Web server to the Sensor through eth2. Connect the database server to the Sensor through eth4.
3. Open the device in Device Manager.
4. Click **Anti-Spoof Settings**.
5. Click **New** to add a new entry to the antispoof table. In the dialog box that opens, configure the following settings:
  - a. Select **eth4** as the forwarding interface for the database server.
  - b. Check both the **Logging** and **Alert** check boxes because your database server is important.
  - c. Select **None** from the Action list.
  - d. Select your database server from the list of address objects.
  - e. Click **OK**.
  - f. Click **New** again to add your Web server.
  - g. Select **eth2** as the interface.
  - h. Select the **Logging** check box.
  - i. Select the **Check other interfaces** check box.

If this check box is selected, the sensor compares each IP address to the list of addresses known to be assigned to other interfaces. In other words, if the database server IP address appears at this interface, you want the sensor to let you know.
  - j. Select **None** from the Action list. You just want to log this event.
  - k. Select the Web server as the address object assigned to this interface.

- Related Topics**
- [Configuring Antispoof Settings in Intrusion Detection and Prevention Devices \(NSM Procedure\)](#)
  - [Intrusion Detection and Prevention Services and Device Configurations Supported in NSM](#)

---

Published: 2009-08-20