

## Sniffer Mode Overview

You deploy an IDP virtual router in sniffer mode if you want to learn about security threats in your network but not disrupt connections.

In sniffer mode, the IDP appliance is not directly involved with packet flow. Based on your security policy, the device detects and logs threats in Layer 3 and Layer 2 traffic. For some attacks, the IDP appliance can send TCP resets. However, this action does not guarantee protection, as attacks might have already happened before the reset or the attacker might persist.

For a sniffer mode deployment, you connect an IDP traffic interface to a port mirror or Switched Port Analyzer (SPAN) port.

Figure 1 illustrates a sniffer mode deployment.

**Figure 1: Network Diagram: Sniffer Mode**

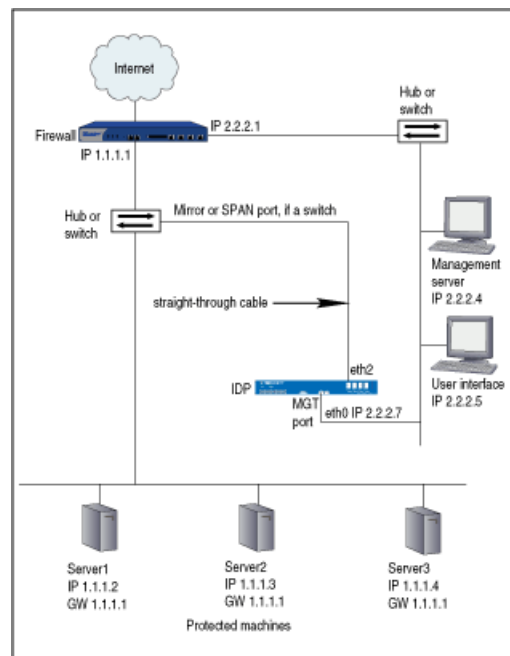


Table 1 lists the features and the limitations of sniffer mode.

**Table 1: Sniffer Mode: Features and Limitations**

Features	Limitations
<ul style="list-style-type: none"><li>■ Replaces the current intrusion detection with minimal effort</li><li>■ Does not create an additional point-of-failure gateway</li><li>■ Detects attacks according to your security policy rules</li><li>■ Performs the following security policy actions:<ul style="list-style-type: none"><li>■ Close Client and Server</li><li>■ Close Client</li><li>■ Close Server</li><li>■ IP Close</li><li>■ IP Notify</li></ul></li></ul>	<ul style="list-style-type: none"><li>■ Requires a hub or the SPAN port of a network switch</li><li>■ Cannot perform the following security policy actions:<ul style="list-style-type: none"><li>■ Drop Packet</li><li>■ Drop Connection</li><li>■ Mark Diffserv</li><li>■ IP Block</li></ul></li><li>■ Cannot perform drop actions</li><li>■ Does not inspect HTTPS traffic that requires the interdiction feature</li><li>■ Does not support SYN Protector rulebase in relay mode</li><li>■ Does not support Network Honeypot rulebase</li></ul>

**Related Topics** The following related topics are included in the *IDP Concepts and Examples Guide*:

- Transparent Mode Overview
- Mixed Deployment Mode Overview

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

- Configuring Virtual Routers (ACM Procedure)

---

Published: 2010-01-12