# IDS Example



To help you better understand the configuration of the Cisco IOS Firewall IDS feature, take a look at an example. Use the perimeter router in Figure 16-1 as an example. In Example 16-3, alarms should be generated for informational signature matches and alarms, drops, and resets for attacks.

### Example 16-3. Simple IDS Configuration Example

```
Router(config)# ip audit notify log

Router(config)# ip audit name IDSRULZ info action alarm

Router(config)# ip audit name IDSRULZ attack action alarm drop
reset

Router(config)# ip audit signature 2000 disable

Router(config)# ip audit signature 2001 disable

Router(config)# ip audit signature 2002 disable

Router(config)# ip audit signature 2004 disable

Router(config)# ip audit signature 2005 disable

Router(config)# ip audit signature 6051 disable

Router(config)# interface ethernet1

Router(config-if)# ip audit IDSRULZ in
```

In this example, one rule is created (IDSRULZ) that enables the information signatures with a match option of alarm and attack signatures, with actions of alarm, drop, and reset. The following signatures have been disabled:

- 2000 (echo reply)
- 2001 (host unreachable)
- 2002 (source quench)
- 2004 (echo request)
- 2005 (time exceeded)
- 6051 (DNS zone transfers).

These are normal actions and generate a lot of IDS logging records, making it more difficult to see other, more important information.

CAUTION

A common misconfiguration/misunderstanding that I see when administrators enable the Cisco IOS IDS is that they are not aware that portions of the CBAC engine also are enabled. The Cisco internal development team states that enabling components of CBAC is necessary to track half-open sessions for certain signatures. The biggest problem that this creates is that the CBAC inspection process for the max-incomplete low/high and 1-minute low/high parameters are set to their default values (these parameters are discussed in Chapter 17, "DoS Protection"). The main problem with the default setting of these parameters is that they are set low for most environments, especially in environments where the router is processing a lot of traffic. Therefore, you need to tune these parameters to appropriate values based on your network's traffic patterns. See Chapter 17 for more information on this topic.