CHAPTER 26

Protecting the Router from DoS Attacks

Internet service providers (ISPs) and other Cisco customers face increasing Denial of Service (DoS) attacks associated with IP options set in the IP header of packets. Cisco IOS routers use the Route Processor (RP) to process IP options packets, which can become problematic during a DoS attack. To protect the router, the Cisco 10000 series router supports the dropping of packets with IP options.

This chapter discusses the following topics:

IP Options Selective Drop

The IP Options Selective Drop feature enables you to protect your network routers in the event of a denial of service (DoS) attack. Hackers who initiate such attacks commonly send large streams of packets with IP options. By dropping the packets with IP options, you can reduce the load of IP options packets on the router. The end result is a reduction in the effects of the DoS attack on the router and on downstream routers.

Internet service providers (ISPs) and other Cisco customers face increasing DoS attacks associated with IP options set in the IP header. Cisco IOS routers are susceptible to DoS attacks because of the way in which the routers process IP options. The hardware-based forwarding engine of Cisco IOS routers cannot handle IP options; therefore, the forwarding engine forwards the IP options packets to the route processor (RP). Similarly, most of the line cards forward IP option packets to the RP. The software-based RP processes the packets and performs the extra processing that the IP options packets require.

Processing IP options packets in the RP can become problematic. Software-switching of IP options packets can lead to a serious security problem if a Cisco IOS router comes under a DoS attack by a hacker sending large streams of packets with IP options. The RP can easily become overloaded and drop high priority or routing protocol packets. Switching packets in software slows down the switching speed of the router and increases the router's vulnerability to resource saturation. Some types of IP options, such as the Router Alert option, can be especially harmful to the router when forwarded to the RP.

By default, Cisco IOS software processes packets with IP options, as required by RFC 1812, *Requirements for IP Version 4 Routers*. The IP Options Selective Drop feature provides the ability to drop packets with IP options in the forwarding engine so that they are not forwarded to the RP. This result in a minimized load on the RP and reduced RP processing requirements.

Feature History for IP Options Selective Drop

Cisco IOS Release	Description
12.0(23)S	This feature was introduced.
12.2(2)T	This feature was integrated in Cisco IOS Release 12.2(2)T.
12.2(25)S	This feature was integrated in Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This feature was integrated in Cisco IOS Release 12.2(27)SBC.
12.3(19)	This feature was integrated in Cisco IOS Release 12.3(19).
12.2(31)SB2	This feature was integrated in Cisco IOS Release 12.2(31)SB2 and introduced on the Cisco 10000 series router for the PRE2 and PRE3.

Restrictions for IP Options Selective Drop

Resource Reservation Protocol (RSVP), Multiprotocol Label Switching-Traffic Engineering (MPLS-TE), Internet Group Management Protocol Version 2 (IGMPV2), and other protocols that use IP options packets may not function in drop mode if this feature is configured.

How to Configure IP Options Selective Drop

You can configure the router to drop all the inbound IPv4 packets with IP options or all the RP-forwarded IP options packets.

To configure IP Options Selective Drop and protect the RP during a DoS attack, perform the following configuration tasks:

- Dropping Packets with IP Options, page 26-2
- Verifying IP Options Packets, page 26-3

Dropping Packets with IP Options

Use the following procedure to configure the forwarding engine to drop packets with IP options before sending them to the RP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip options drop**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip options drop** **Example:** `Router(config)# ip options drop`	Turns IP options processing off. The router drops all the packets received with IP options. **Note** To resume normal options processing, use the **no** form of the command: **no ip options**.

Verifying IP Options Packets

Use the **show ip traffic** command to verify that the router drops all the packets received with IP options.

Configuration Examples for IP Options Selective Drop

This section provides the following configuration examples:

- Dropping IP Options Packets: Example, page 26-3
- Verifying IP Options Handling: Example, page 26-4

Dropping IP Options Packets: Example

The following sample configuration shows how to configure the router (and downstream routers) to drop all the packets with IP options that enter the network:

```
Router(config)# ip options drop

% Warning:RSVP and other protocols that use IP Options packets may not function in drop or
ignore modes.
end
```

Verifying IP Options Handling: Example

The following sample output from the **show ip traffic** command indicates that the router received 2905 packets with IP options set. Because the **ip options drop** command is configured, the router drops all the packets with IP options, as indicated by the options denied counter.

```
Router# show ip traffic

IP statistics:
  Rcvd:  2905 total, 13 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 1 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 12 received, 3 sent
  Mcast: 0 received, 0 sent
  Sent:  3 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop, 0 unsupported-addr
         3000 options denied, 0 source IP address zero
```

Related Documentation

This section provides additional Cisco documentation for the features discussed in this chapter. To display the documentation, click the document title or a section of the document highlighted in blue. When appropriate, paths to applicable sections are listed below the documentation title.

Feature	Related Documentation
Denial of service (DoS) attacks	*Characterizing and Tracing Packet Floods Using Cisco Routers technical note*