

## Understanding SYN Protector Rulebase Modes

Table 1 summarizes SYN Protector rulebase modes.

**Table 1: SYN Protector Rulebase Modes**

Mode	Description
None	The IDP appliance takes no action and does not participate in the three-way handshake.
Passive	In passive mode, the IDP appliance monitors session startup. If the client does not send an ACK within a timeout period, the IDP appliance sends a TCP reset.
Relay	<p>In relay mode, the IDP appliance acts as a relay for the connection establishment, performing the three-way handshake with the client on behalf of the server. When the IDP appliance receives the initial SYN packet, it returns a SYN/ACK packet with a SYN cookie. A SYN cookie is a 32-bit number that is put into the TCP sequence number field of a packet. If the client replies with an ACK packet with the appropriate cookie, the IDP appliance completes the three-way handshake and allows the session to become established. If the IDP appliance does not receive an appropriate ACK packet from the client, as is the case in a SYN flood attack, the IDP appliance does not establish the connection. Relay mode guarantees that the server allocates resources only to connections that are already in an established state. The relay is transparent to both the client and server.</p> <p>Relay mode has the following limitations:</p> <ul style="list-style-type: none"><li>■ When the ACK packet from the client is lost, it can potentially lead to an unsynchronized state between client and server.</li><li>■ Because the IDP appliance does not save TCP options found in SYN packets, TCP extensions used for efficient transaction-oriented service (T/TCP) and Selective Acknowledgment (SACK), or applications such as BGP, have a problem when SYN flooding is detected and the IDP appliance initiates the proxy TCP handshake.</li><li>■ Relay mode can be susceptible to ACK flooding because the IDP appliance must check for the validity of a cookie in the ACK messages.</li></ul> <p><b>NOTE:</b> Relay mode might not work as expected for MPLS traffic. When the IDP engine processes MPLS traffic, it stores the MPLS label information for traffic in each direction. In the case of traffic that matches SYN Protector rules in relay mode, the IDP appliance is programmed to send a SYN-ACK before the traffic has reached the server. In these cases, the IDP engine does not have server-to-client MPLS label information. Therefore, the SYN-ACK packet does not include an MPLS label. Some MPLS routers can add packets without a label to an existing MPLS tunnel; others drop such packets.</p>



**TIP:** You can use two rules to protect a large number of servers. Configure rule 1 to match servers you do not need to protect, and set Mode to **None**. Configure rule 2 to match any traffic and set Mode to **Passive** or **Relay**, as you prefer.

**Related Topics** The following related topic is included in the *IDP Concepts and Examples Guide*:

- Understanding the SYN Protector Rulebase

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

- Configuring SYN Protector Rulebase Rules (NSM Procedure)

---

Published: 2010-01-12