

Understanding the SYN Protector Rulebase

The SYN Protector rulebase protects your network from malicious SYN flood attacks.

A *SYN flood attack* is a type of denial-of-service (DoS) attack, where the attacker attempts to flood your server with TCP requests to overwhelm your resources.

Attackers send a SYN message from a host with a spoofed, unreachable IP address to foil the TCP three-way handshake:

- A client host sends a SYN packet to a specific port on the server.
- Next, the server sends a SYN/ACK packet to the client host. The potential connection is now in a SYN_RECV state.
- Because the system is unreachable, the server never receives an ACK or RST packet back from the client host. The potential connection remains in the SYN_RECV state, and is placed into a connection queue while it waits for an ACK or RST packet. This “half-opened” connection remains in the queue until the connection-establishment timer expires (when it will be deleted).

To exploit this vulnerability, attackers use attack programs that generate thousands of bogus SYN messages, resulting in denial of service.

When the SYN Protector rulebase is enabled, the IDP engine detects traffic that exceeds the traffic thresholds you set as runtime parameters. Figure 1 shows the SYN protector detection settings in the NSM Device Manager configuration editor.

Figure 1: NSM Device Manager: Sensor Settings > Run-Time Parameters

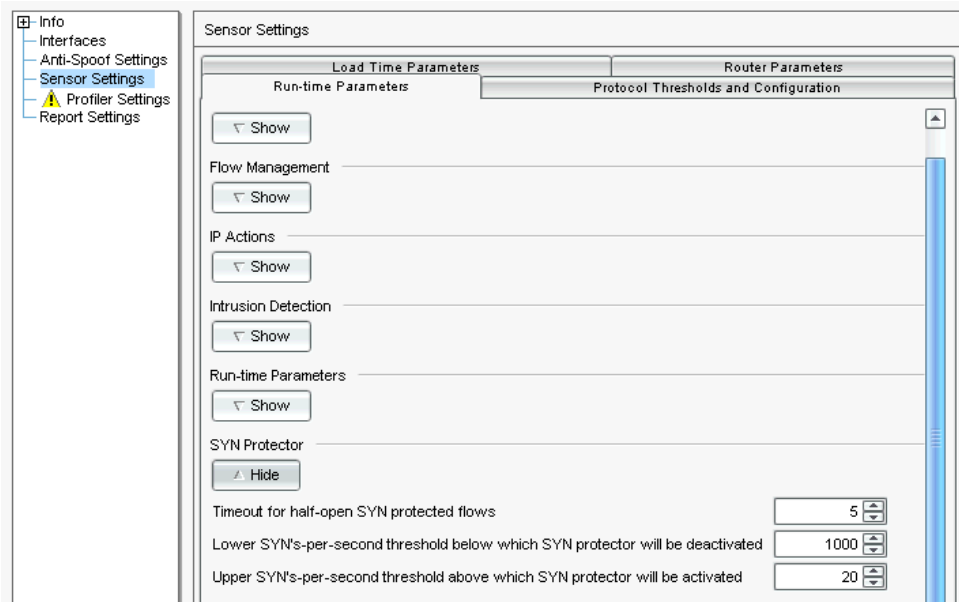


Table 1 describes the SYN Protector thresholds.

Table 1: SYN Protector Thresholds

| Setting | Description |
|---|---|
| Timeout for half-open SYN protected flows | <p>Used when SYN Protector is configured in passive mode.</p> <p>A half-open SYN flow occurs during the TCP three-way handshake, after the client has sent a SYN/ACK packet to the server. The half-open connection is now in the SYN_RECV state, and is placed into a connection queue while it waits for an ACK or RST packet. The connection remains in the queue until the connection-establishment timeout expires and the half-open connection is deleted.</p> <p>In passive mode, the IDP appliance monitors session startup. If the client does not send an ACK within the specified timeout, the IDP appliance sends a TCP reset. This setting controls the connection establishment timer, which determines the number of seconds that the IDP engine maintains a half-open SYN protected flow. The default is 5 seconds.</p> |
| Lower SYNs-per-second threshold below which SYN Protector will be deactivated | <p>Used to activate the SYN Protector in passive or relay mode.</p> <p>In passive mode, the SYN Protector rulebase is activated when the number of SYN packets per second is greater than the sum of the lower SYNs-per-second threshold and the upper SYNs-per-second threshold. The defaults are 1000 and 20. Using the defaults, the SYN Protector is activated when SYNs-per-second reach 1020. The SYN Protector rulebase is deactivated when the number of SYN packets per second falls below the lower SYNs-per-second threshold.</p> |
| Upper SYNs-per-second threshold above which SYN Protector will be activated | <p>In relay mode, the SYN Protector rulebase is activated when the number of SYN packets per second exceeds the lower SYNs-per-second threshold. The upper threshold is not used.</p> |

When you create rules for the SYN Protector rulebase, you specify:

- A source/destination/service match condition
- A response mode: passive or relay
- Notification options

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

- Understanding SYN Protector Rulebase Match Settings
- Understanding SYN Protector Rulebase Modes
- Understanding SYN Protector Rulebase Notification Options
- Understanding the Components of an IDP Security Policy

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

- Configuring SYN Protector Rulebase Rules (NSM Procedure)

Published: 2010-01-12