

Understanding SYN Protector Rulebase Match Settings

The SYN Protector rulebase becomes active when IDP detects traffic that exceeds the thresholds you set as runtime parameters. Table 1 shows the defaults for SYN Protector rulebase detection runtime parameters. You can tune these parameters if safe traffic in your network triggers false positives.

Table 1: SYN Flood Detection Runtime Parameters

Parameter	Default
Timeout for half-open SYN protected flows	5
Lower SYN-per-second threshold below which SYN Protector will be deactivated	1000
Upper SYN-per-second threshold above which SYN Protector will be activated.	20

In other words, using the defaults, the SYN Protector rulebase is activated when the IDP appliance counts 1020 SYN packets per second and deactivates when it falls below 1000 SYN packets per second.

When the SYN Protector rulebase is active, the IDP process engine evaluates its rules, beginning with source, destination, and service matching.

Because all TCP-IP is susceptible to a SYN flood attack, we recommend the following settings:

- Source — Any
- Destination — Servers you want to protect
- Service — TCP Any



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.



TIP: In NSM, you can create address objects and service objects to facilitate configuration. One benefit of using objects is that you can configure them once and then use them in multiple rules. For details, see the NSM documentation.



NOTE: The SYN Protector rulebase is a terminal rulebase—that is, SYN Protector rules are inherently terminal rules. If a SYN Protector rule matches, IDP does not process subsequent rules.

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

- Understanding the Rule-Matching Algorithm
- Understanding the SYN Protector Rulebase

The following related topics are included in the *IDP Administration Guide*:

- Configuring SYN Protector Rulebase Rules (NSM Procedure)
- Modifying the IDP Device Configuration

Published: 2010-01-12