

Configuring SYN Protector Rulebase Rules (NSM Procedure)

The SYN protector rulebase protects your network from malicious SYN-flood attacks.

To configure a SYN protector rulebase rule:

1. In the NSM navigation tree, select **Policy Manager > Security Policies**.
2. Select and double-click the security policy to which you want to add the SYN protector rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add SYN Protector Rulebase**.
4. Click the **New** button within the rules viewer to add a rule.
5. Modify the property of the rule by right-clicking the table cell for the property and making your modifications.
6. Configure or modify the rule using the settings described in Table 1.

Table 1: SYN Protector Rulebase Rule Properties

Option	Function	Your Action
No	Specifies if you want to add, delete, copy, or reorder rules.	Right-click the table cell for the rule number and make your required modifications.
Match > Source	Specifies the address object that is the source of the traffic.	Select any to monitor network traffic originating from any IP address. NOTE: You can also negate one or more address objects to specify all sources except the excluded object.
Match > Destination	Specifies the address object that is the destination of the traffic, typically a server or other device on your network.	Select the destination object. NOTE: You can also negate one or more address objects to specify all destinations except the excluded object.
Match > Service	Specifies service objects in rules to service an attack to access your network.	Set a service by selecting any of the available options. NOTE: We recommend that you do not change the default value, TCP-ANY .

Table 1: SYN Protector Rulebase Rule Properties (continued)

Option	Function	Your Action
Mode	Specifies the mode that indicates how IDP handles TCP traffic.	<p>Select any of the following options:</p> <ul style="list-style-type: none"> ■ None—Specifies that IDP takes no action and does not participate in the three-way handshake. ■ Relay—Specifies that IDP acts as the middleman or relay, for the connection establishment, performing the three-way handshake with the client host on behalf of the server. <p>NOTE: 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> <ul style="list-style-type: none"> ■ Passive—Specifies that IDP handles the transfer of packets between the client host and the server, but does not actively prevent the connection from being established.

Table 1: SYN Protector Rulebase Rule Properties (continued)

Option	Function	Your Action
Notification	<p>Allows you to create log records with attack information that you can view real-time in the Log Viewer.</p> <p>NOTE: For more critical attacks, you can also set an alert flag to appear in the log record.</p>	<p>Select Configure to create log records.</p> <p>NOTE: The Configure menu option does not appear if the Mode column is set to None.</p> <ul style="list-style-type: none"> ■ Select Logging to have a log record created each time the rule is matched. ■ Select Alert to have an alert flag placed in the Alert column of the Log Viewer for the matching log record. ■ In the Log Actions tab, select desired log actions, if any.
VLAN Tag	<p>Specifies that you can configure a rule to only apply to messages in certain VLANs.</p>	<p>Set a value by selecting any of the following options:</p> <ul style="list-style-type: none"> ■ Any—This rule is applied to messages in any VLAN and to messages without a VLAN tag. ■ None—This rule is applied only to messages that do not have a VLAN tag. ■ Select VLAN Tags—This rule specifies which VLAN tags the rule applies to.
Severity	<p>Specifies if you can override the inherent attack severity on a per-rule basis within the IDP rulebase.</p>	<p>Set the severity to Default, Info, Warning, Minor, Major, or Critical.</p> <p>NOTE: This column only appears when you view the Security Policy in Expanded Mode.</p>
Install On	<p>Specifies the security devices or templates that receive and use this rule.</p>	<p>Select the target security device.</p> <p>NOTE: You can also select multiple security devices on which to install the rule.</p>
Comments	<p>Specifies any miscellaneous comment about the rule's purpose.</p>	<p>Enter any additional comments about the rule.</p>

For more information, see the *IDP Concepts & Examples guide*.

- Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview
 - Modifying IDP Rulebase Rules (NSM Procedure)

- Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)

Published: 2009-08-20