

Configuring Exempt Rulebase Rules (NSM Procedure)

The exempt rulebase contains rules that prevent rules in the Intrusion Detection and Prevention (IDP) rulebase from matching specific source or destination pairs for specific attack objects.

The exempt rulebase works in conjunction with the IDP rulebase. Before you can create exempt rules, you must first create rules in the IDP rulebase. If traffic matches a rule in the IDP rulebase, the IDP sensor attempts to match the traffic against the exempt rulebase before performing the specified action or creating a log record for the event.



NOTE: The exempt rulebase is a non-terminal rulebase. The IDP device checks all rules in the exempt rulebase and executes all matches.

To configure an exempt rulebase rule:

1. In the NSM navigation tree, select **Policy Manager > Security Policies**.
2. Select and double-click the security policy for which you want to add an exempt rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add Exempt 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: Exempt 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 > From Zone	Specifies the zone from where the source sends traffic.	Select one or more zones for the source zone, or you can specify any for all source zones. NOTE: The selected zone must be available on the security device specified in the Install On column.

Table 1: Exempt Rulebase Rule Properties (continued)

Option	Function	Your Action
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 > To Zone	Specifies the destination zone.	Select the destination zone.
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.
Attacks	Specifies the attack(s) you want the IDP to exempt for the specified source or destination addresses.	Select the attack objects or groups. NOTE: You must include at least one attack object in an exempt rule.
VLAN Tag	Specifies that you can configure a rule to only apply to messages in certain VLANs.	Set a value by selecting any of the following options: <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.
Install On	Specifies the security devices or templates that receive and use this rule.	Select the target security device. NOTE: You can also select multiple security devices on which to install the rule.
Comments	Specifies any miscellaneous comment about the rule's purpose.	Enter any additional comments about the rule.

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

- Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview
 - Creating a New Security Policy (NSM Procedure)

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

Published: 2009-08-20