

Modifying IDP Rulebase Rules (NSM Procedure)

This procedure assumes you have used the New Policy wizard to create a basic policy that you can modify.

The primary IDP security policy rulebase is the IDP rulebase. The IDP rulebase enables the IDP process engine to inspect matching traffic for signs of an attack.

For background on and examples of IDP rulebase rules, see the *IDP Concepts & Examples Guide*.

To modify IDP rulebase rules:

1. In the NSM navigation tree, select **Configure > Policy Manager > Security Policies**.
2. Select the security policy you want to edit.
3. In the security policy pane, select **IDP** tab to display the IDP rulebase table.
4. To add, delete, copy, or reorder rules, right-click the table cell for the rule number and make your selection.
5. To modify the property of a rule, right-click the table cell for the property and make your selection. Table 1 lists the rule properties you can modify and provides references documentation for these properties.

Table 1: IDP Rulebase Rule Properties

Property	Reference
ID	Identification number of the IDP rules that you add.
Match	You can select the zone from which the source sends traffic to the destination zone.
Look For	You can select the attacks that you want add IDP to match in the monitored traffic.
Action	Specifies the action you want IDP to perform against the current connection.
IP Action	Specifies the action you want IDP to perform against future connections that use the same IP address.
Notification	You can choose none, or enable logging and select the logging options that are appropriate for your network.
VLAN Tag	Specifies the VLAN tags you want to match in applying the rule.
Severity	You can use the default severity settings of the selected attack objects, or you can choose a specific severity for your rule.
Install On	Specifies the selected source and destination zone that are available on the security device.
Optional Fields	Specifies the optional fields that you can configure in the rule.

Table 1: IDP Rulebase Rule Properties (continued)

Property	Reference
Comments	Describes any additional comments about the rule.

Following are the updates that you can perform on an IDP rulebase rule:

- Specifying Rule Match Conditions on page 2
- Specifying IDP Rulebase Attack Objects on page 3
- Specifying Rule Session Action on page 4
- Specifying Rule IP Action on page 6
- Specifying Rule Notification Options on page 7
- Specifying Rule VLAN Matches on page 7
- Specifying Rule Targets on page 8
- Specifying Rule Severity on page 8
- Specifying Rule Optional Fields on page 9
- Specifying Rule Comments on page 9

Specifying Rule Match Conditions

To specify rule match conditions, right-click the table cell and select your setting.

Table 2 describes match condition columns for IDP rulebase rules.

Table 2: IDP Rulebase Match Condition Settings

Column	Description
From zone / To zone	Not applicable for standalone IDP devices.
Source	<p>Select Address—Display the Select Address dialog box where you can select address objects for traffic sources.</p> <hr/> <p>Any—Matches any source of traffic. To guard against incoming attacks, you typically specify Any.</p> <hr/> <p>Negate—Matches any except those specified.</p> <p>To use address negation:</p> <ol style="list-style-type: none"> 1. Add the address object. 2. Right-click the address object and select Negate.

Table 2: IDP Rulebase Match Condition Settings (continued)

Column	Description
User Role	<p>Select User Role—Displays the Select User Role dialog box where you can select or configure user role matches.</p> <p>If a value for User Role matches, the Source parameter is not consulted.</p> <p>User role-based rules are evaluated before IP source rules. If a user role matches, and if the other match criteria are met, the rule is applied and IP address-based rules are not consulted.</p> <p>NOTE: Matching based on user role depends on integration with Juniper Networks Infranet Controllers.</p>
Destination	<p>Select Address—Display the Select Address dialog box where you can select address objects for destination servers.</p>
	<p>Any—Matches any destination address.</p>
	<p>Negate—Specifies any except those specified.</p> <p>To use address negation:</p> <ol style="list-style-type: none"> 1. Add the address object. 2. Right-click the address object and select Negate.
Service	<p>Default—Matches the service(s) specified in the rule attack object(s).</p> <p>If you have enabled the Application Identification (AI) feature, the IDP process engine identifies services even if they are running on nonstandard ports.</p> <p>If you have not enabled AI and specify Default, the IDP process engine assumes that standard ports are used for the service.</p> <p>NOTE: If you do not enable AI and your service uses nonstandard ports, you must create a custom service objects.</p>
	<p>Any—Matches any service.</p>
	<p>Select Service—Display the Select Service dialog box where you can select predefined or custom service objects.</p>
Terminate	<p>Enable or Disable—Marks the rule a terminal rule (or clears the mark). If a session matches a terminal rule, the IDP process engine does not load any subsequent rules. It takes action, if any, according to the terminal rule.</p>

Specifying IDP Rulebase Attack Objects

To add attack objects:

1. Right-click the table cell for attacks and select **Select Attacks**.
2. In the All Attacks/Groups box, expand **Attack Groups**.

3. To add attack objects recommended by Juniper Networks Security Center (J-Security Center), expand **Recommended Attacks**, browse groups, and select groups or individual attack objects.
4. To add other predefined attack objects, expand **All Attacks**, browse groups, and select groups or individual attack objects.
5. To add attack objects that belong to custom groups, expand the node for the custom group, browse subgroups, and select groups or individual attack objects.
6. To add custom attack objects that do not belong to groups, expand **Attack List** and select from custom attack objects.
7. Click **OK**.

Table 3 describes the attack object group hierarchy for recommended and predefined attack objects provided by J-Security Center.

Table 3: Attack Object Group Hierarchy

Group	Contents
Attack Type	Contains two subgroups: anomaly and signature. Within each subgroup, attack objects are grouped by severity.
Category	Contains subgroups based on category. Within each category, attack objects are grouped by severity.
Operating System	Contains the following subgroups: BSD, Linux, Solaris, and Windows. Within each operating system, attack objects are grouped by services and severity.
Severity	Contains the following subgroups: Critical, Major, Minor, Warning, Info. Within each severity, attack objects are grouped by category. NOTE: Our severity rating is not based on CVSS (Common Vulnerability Scoring System). We do include data from Bugtraq (Symantec) and CVE (Common Vulnerabilities and Exposures).
Web Services	Contains subgroups based on Web services. Within services, attacked objects are grouped by severity.
Miscellaneous	Contains attack objects that have a significant affect on IDP performance.

Specifying Rule Session Action

Actions are responses to sessions that match the source/destination condition and attack object pattern. Actions protects your network from attacks.

If a packet triggers multiple rule actions, the IDP device takes the most severe action. For example, if the rules dictate that a packet will receive a DiffServ marking and be dropped, and then the packet will be dropped.

To specify a rule action, right-click the table cell and select your setting.

Table 4 describes the actions you can set for IDP rulebase rules.

Table 4: IDP Rulebase Actions

Action	Description
Recommended	Predefined attack objects include a recommended action. The recommended action is related to severity. Table 5 lists the recommended actions by severity.
None	IDP inspects for attacks but takes no action against the connection if an attack is found.
Ignore	IDP does not inspect for attacks and ignores the connection.
Diffserv Marking	IDP assigns the indicated service-differentiation value to the packet, and then passes it on normally. Set the service-differentiation value in the dialog box that appears when you select this action in the rulebase. NOTE: The marking has no effect in sniffer mode.
Drop Packet	IDP drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a DoS that prevents you from receiving traffic from a legitimate source address.
Drop Connection	IDP drops the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.
Close Client and Server	IDP closes the connection and sends an RST packet to both the client and the server. If IDP is in sniffer mode, IDP sends an RST packet to both the client and server but does not close the connection.
Close Client	IDP closes the connection to the client but not to the server.
Close Server	IDP closes the connection to the server but not to the client.

Table 5 describes the logic applied to the value Recommended, a setting coded in predefined attack objects provided by Juniper Networks Security Center.

Table 5: IDP Rulebase Actions: Recommended Actions by Severity

Severity	Description	Recommended Action
Critical	Attacks attempt to evade an IPS, crash a machine, or gain system-level privileges.	Drop Packet, Drop Connection
Major	Attacks attempt to crash a service, perform a denial of service, install or use a Trojan, or gain user-level access to a host.	Drop Packet, Drop Connection
Minor	Attacks attempt to obtain critical information through directory traversal or information leaks.	None
Warning	Attacks attempt to obtain noncritical information or scan the network. They can also be obsolete attacks (but probably harmless) traffic.	None

Table 5: IDP Rulebase Actions: Recommended Actions by Severity (continued)

Severity	Description	Recommended Action
Info	Attacks are normal, harmless traffic containing URLs, DNS lookup failures, and SNMP public community strings. You can use informational attack objects to obtain information about your network.	None



NOTE: Our severity rating is not based on CVSS (Common Vulnerability Scoring System). We do include data from Bugtraq (Symantec) and CVE (Common Vulnerabilities and Exposures).

Specifying Rule IP Action

If the IDP device matches an attack, it can take action not only against the current session but also against future network traffic that uses the same IP address. Such actions are called *IP actions*. By default, the specified IP action is permanent (timeout = 0). If you prefer, you can set a timeout.

To specify an IP action, right-click the table cell and configure options.

Table 6 describes IDP rulebase IP actions.

Table 6: IDP Rulebase IP Actions

IP Action	Description
IP Block	IDP blocks the matching connection and future connections that match combinations of the following properties you specify: <ul style="list-style-type: none">■ Source IP address■ Source subnet■ Protocol■ Destination IP Address■ Destination Subnet■ Destination Port■ From Zone
IP Close	IDP closes the matching connection and future connections that match combinations of the following properties you specify: <ul style="list-style-type: none">■ Source IP address■ Source subnet■ Protocol■ Destination IP Address■ Destination Subnet■ Destination Port■ From Zone

Table 6: IDP Rulebase IP Actions (continued)

IP Action	Description
IP Notify	IDP does not take any action against future traffic but logs the event or sends an alert.

Specifying Rule Notification Options

Notification options determine how events that match the rule are logged.

To specify notification options, right-click the table cell and configure options.

Table 7 describes IDP rulebase notification options.

Table 7: IDP Rulebase Notification Options

Option	Description
Event logs and alerts	<p>You can enable the following delivery and handling options for logs:</p> <ul style="list-style-type: none">■ Send to NSM Log Viewer■ Send to NSM Log Viewer and flag as an alert■ Send to an e-mail address list■ Send to syslog■ Send to SNMP trap■ Save in XML format■ Save in CVS format■ Process with a script
Packet captures	<p>Viewing the packets used in an attack on your network can help you determine the extent of the attempted attack, its purpose, whether or not the attack was successful, and any possible damage to your network.</p> <p>If multiple rules with packet capture enabled match the same attack, IDP captures the maximum specified number of packets. For example, you configure rule 1 to capture 10 packets before and after the attack, and you configure rule 2 to capture 5 packets before and after the attack. If both rules match the same attack, IDP attempts to capture 10 packets before and after the attack.</p> <p>You can capture up to 256 packets before the event and 256 packets after the event.</p> <p>NOTE: If necessary, you can improve performance by logging only the packets received after the attack.</p>

Specifying Rule VLAN Matches

If you deploy an IDP device in a virtual local area network (VLAN), you can specify VLAN tags for traffic in IDP rulebase rules.

Normally, rules match source, destination, and service. If your rule specifies a VLAN tag, then the rule must also match the VLAN tag.

To specify that rules match a VLAN tag, right-click the table cell and configure your setting.

Table 8 describes VLAN tag settings.

Table 8: IDP Rulebase VLAN Tag Settings

Option	Description
None	Matches only traffic that has no VLAN tag.
Any	Matches traffic with any or no VLAN tag (default).
Select VLAN Tags	Displays the Select VLAN Tags dialog box where you can set a single VLAN tag or a range of VLAN tags.
Delete VLAN Tags	Displays a dialog box that prompts you to confirm you want to delete the VLAN tag match setting.

Specifying Rule Targets

By default, IDP security policy rules can be applied to any IDP device. If you desire, you can specify that the rule applies to only specified IDP devices.

To specify that the rule only applies to specified devices, right-click the table cell and select **Select Target** to display the Select Targeted Devices dialog box, where you can select the specify devices on which the rule is to be applied.

Specifying Rule Severity

Severity is a rating of the danger posed by the threat the rule is designed to prevent.

To specify a rule severity, right-click the table cell and select a severity.

Table 9 describes rule severity settings.

Table 9: IDP Rulebase Severity

Severity	Description
Default	Select Default to inherit severity from that specified in the attack object.
Critical	Attacks that attempt to evade an IPS, crash a machine, or gain system-level privileges. We recommend that you drop the packets or drop the connection for such attacks.
Major	Attacks that attempt to crash a service, perform a denial of service, install or use a Trojan, or gain user-level access to a host. We recommend that you drop the packets or drop the connection for such attacks.

Table 9: IDP Rulebase Severity (continued)

Severity	Description
Minor	Attacks that attempt to obtain critical information through directory traversal or information leaks. We recommend that you log such attacks.
Warning	Attacks that attempt to obtain noncritical information or scan the network. They can also be obsolete attacks (but probably harmless) traffic. We recommend that you log such attacks.
Info	Attacks that are normal, harmless traffic containing URLs, DNS lookup failures, and SNMP public community strings. You can use informational attack objects to obtain information about your network. We recommend that you log such attacks.



NOTE: Our severity rating is not based on CVSS (Common Vulnerability Scoring System). We do include data from Bugtraq (Symantec) and CVE (Common Vulnerabilities and Exposures).

Specifying Rule Optional Fields

Optional fields are user-defined name-value pairs you can configure if you want to be able to sort rules based on these fields. Optional fields do not affect the functionality of the security policy rule.

To specify optional fields, right-click the table cell and select **Edit Options** to display the Select Policy Custom Options dialog box, where you can configure name-value pairs.

Specifying Rule Comments

Comments are notations about the rule. Comments do not affect the functionality of the security policy rule.

To specify comments, right-click the table cell and select **Edit Comments** to display the Edit Comments dialog box, where you can enter a comment up to 1024 characters in length.

- Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview
 - Configuring Predefined Security Policies (NSM Procedure)

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

Published: 2009-08-20