

Configuring Traffic Anomalies Rulebase Rules (NSM Procedure)

The traffic anomalies rulebase employs a traffic flow analysis method to detect attacks that occur over multiple connections and sessions (such as scans).

To configure a traffic anomalies 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 traffic anomalies rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add Traffic Anomalies 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: Traffic Anomalies 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: Traffic Anomalies Rulebase Rule Properties (continued)

Option	Function	Your Action
Traffic Anomaly	Specifies how IDP is to treat the matching traffic.	<p>Select any of the following options:</p> <ul style="list-style-type: none"> ■ Ignore—IDP ignores this traffic. This option excludes traffic from trusted sources that might be falsely construed as a scan. ■ Detect—IDP matches this traffic and takes the IP action that you have set. <p>When you select this option, the Traffic Anomalies dialog box appears. Select the scans or sweep you want to detect and enter values for Port Count and Time Threshold (in seconds) or Session Count.</p>
IP Action	Allows you to log, drop, or close the current connection for each attack that matches a rule.	<p>Select Configure to do any one of the following actions:</p> <ul style="list-style-type: none"> ■ Enabled—Enables IP actions. ■ Action—Specifies the action you want the IDP to take. ■ Block—Specifies which parameters IDP will use to close or block further connections from the drop down list. ■ Logging—Specifies the log action for a matching event. ■ Timeout (sec)—Specifies the number of seconds that this action remains in effect on IDP after a traffic match.
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.

Table 1: Traffic Anomalies Rulebase Rule Properties (continued)

Option	Function	Your Action
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—Specifies which VLAN tags the rule applies to.
Severity	Specifies if you can override the inherent attack severity on a per-rule basis within the IDP rulebase.	Set the severity to Default, Info, Warning, Minor, or Critical . NOTE: This column only appears when you view the Security Policy in Expanded Mode.
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
 - Modifying IDP Rulebase Rules (NSM Procedure)
 - Configuring Network Honeypot Rulebase Rules (NSM Procedure)
 - Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)

Published: 2009-08-20