

## Configuring Network Honeypot Rulebase Rules (NSM Procedure)

The network honeypot rulebase is a method to detect investigation activities.

To configure a network honeypot 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 network honeypot rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add Network Honeypot 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: Network Honeypot 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.
Source Address	Specifies the address object that is the source of the traffic.	Select any source address or group.
Impersonate > 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. <b>NOTE:</b> You can also negate one or more address objects to specify all destinations except the excluded object.
Impersonate > Service	Specifies the services running on your network.	Select the services you want to monitor.
Operation	Specifies whether or not IDP fakes open ports.	Select any of the following options: <ul style="list-style-type: none"> <li>■ <b>Ignore</b>—This option allows free passage on your network when creating rules for trusted traffic.</li> <li>■ <b>Impersonate</b>—IDP creates a fake port open to the public based on the destination IP addresses and service you selected.</li> </ul>

**Table 1: Network Honeypot Rulebase Rule Properties (continued)**

Option	Function	Your Action
IP Action	Allows you to log, drop, or close the current connection for each attack that matches a rule.	<p>Select <b>Configure</b> to do any one of the following actions:</p> <ul style="list-style-type: none"> <li>■ <b>Enabled</b>—Enable IP actions.</li> <li>■ <b>Action</b>—Specifies the action you want the IDP to take.</li> <li>■ <b>Block</b>—Specifies which parameters IDP will use to close or block further connections from the drop-down list.</li> <li>■ <b>Logging</b>—Specifies the log action for a matching event.</li> <li>■ <b>Timeout (sec)</b>—Specifies the number of seconds that this action remains in effect on IDP after a traffic match.</li> </ul>
Notification	<p>Allows you to create log records with attack information that you can view real-time in the Log Viewer.</p> <p><b>NOTE:</b> For more critical attacks, you can also set an alert flag to appear in the log record.</p>	<p>Select <b>Configure</b> to create log records.</p> <p><b>NOTE:</b> The Configure menu option does not appear if the Mode column is set to None.</p> <ul style="list-style-type: none"> <li>■ Select <b>Logging</b> to have a log record created each time the rule is matched.</li> <li>■ Select <b>Alert</b> to have an alert flag placed in the Alert column of the Log Viewer for the matching log record.</li> <li>■ In the Log Actions tab, select desired log actions, if any.</li> </ul>
VLAN Tag	Specifies that you can configure a rule to only apply to messages in certain VLANs.	<p>Set a value by selecting any of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Any</b>—This rule is applied to messages in any VLAN and to messages without a VLAN tag.</li> <li>■ <b>None</b>—This rule is applied only to messages that do not have a VLAN tag.</li> <li>■ <b>Select VLAN Tags</b>—This rule specifies which VLAN tags the rule applies to.</li> </ul>

**Table 1: Network Honeypot Rulebase Rule Properties** (continued)

Option	Function	Your Action
Severity	Specifies if you can override the inherent attack severity on a per-rule basis within the IDP rulebase.	Set the severity to <b>Default, Info, Warning, Minor, Major, or Critical</b> .  <b>NOTE:</b> 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.  <b>NOTE:</b> 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.



**NOTE:** The IDP drops MPLS traffic that matches a Network Honeypot rule. When the IDP engine processes MPLS traffic, it stores the MPLS label information. It stores separate labels for client-to-server and server-to-client communication. In the case of traffic that matches Network Honeypot rules, there is no genuine server-to-client communication, so the IDP engine does not have server-to-client MPLS label information. Therefore, the impersonation operation is not supported.

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)
  - Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)
  - Validating a Security Policy (NSM Procedure)

Published: 2009-08-20