

Configuring Backdoor Rulebase Rules (NSM Procedure)

The backdoor rulebase detects if there exists any interactive traffic introduced during backdoor attacks.

To configure a backdoor 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 backdoor rulebase rule.
3. Click **New** in the upper right corner of the policy viewer and select **Add Backdoor 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: Backdoor 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 following options: <ul style="list-style-type: none"> ■ Any—Sets any service. ■ Default—Accepts the service specified by the attack object. ■ Select Service—Chooses specific services from the list of defined service objects.

Table 1: Backdoor Rulebase Rule Properties (continued)

Option	Function	Your Action
Operation	Specifies whether to detect or ignore the backdoor traffic.	Select either Detect or Ignore .
Action	Specifies an action of the IDP to detect any interactive traffic.	Select any type of action.
Notification	Allows you to create log records with attack information that you can view real-time in the Log Viewer.	Select Configure to create log records.
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.
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, Major, 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 SYN Protector Rulebase Rules (NSM Procedure)
- Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)

Published: 2009-08-20