

Troubleshooting Security Policy Validation Errors (NSM Procedure)

Problem If NSM identifies a problem in the policy during policy validation, it displays information about the problem at the bottom of the selected rulebase. For example, if you included a non-IDP capable security device in the Install On column of an IDP rule, policy validation displays an error message. You can validate those errors and troubleshoot them.

Table 1 describes security policy validation errors and how to resolve them.

Table 1: Troubleshooting: Security Policy Validation Errors

Error	Description
Rule Duplication	Rule appears more than once. To resolve this problem, delete the duplicate.
Rule Shadowing	Rule shadowing occurs when two rules are designed to detect the same attack, and the first rule is either a terminal match rule or contains a more severe action than the second rule. In these cases, the second rule will never be applied. To resolve this problem, modify or delete one of the rules.
Protocol Mismatches	Protocol mismatches occur when a service object that is specified in the Service column of the security policy uses a different protocol from that specified by the default service binding of the attack object for that rule. Remember that the service binding specifies the service and port that the attack uses. Because two different protocols are specified, IDP cannot match attacks for the attack object. To resolve this problem, set Service to Default .
Any-Any-None Rules	Any-Any-None rules are rules that specify any for the source and destination and none for attacks. Because IDP must log all packets for all connections, this rule can cause severe IDP performance penalties. To resolve this problem, specify network objects for the destination and attack objects for the attacks.
Any-Any-One Rules	Any-Any-One rules are rules that specify any for the source and destination and a single attack object for attacks. Because IDP must look at all network traffic, this rule can cause severe IDP performance penalties. To resolve this problem, specify network objects for the destination.
Unsupported Options	Rule contains options that are not supported on the target device. To resolve this problem, upgrade the target device or remove the option from the rule.

- Related Topics**
- Intrusion Detection and Prevention Devices and Security Policies Overview
 - Assigning a Security Policy in an Intrusion Detection and Prevention Device (NSM Procedure)

- Validating a Security Policy (NSM Procedure)

Published: 2009-08-20