

Troubleshooting Configuration Push Errors (NSM Procedure)

Problem Table 1 provides tips for troubleshooting errors related to NSM configuration push jobs.

Table 1: Troubleshooting: Configuration Push Errors

Error	Description
Timeout	<p>The default timeout for IDP policy is 2400000 milliseconds (40 minutes).</p> <p>When you first push a policy to a newly deployed IDP device, NSM must send a lot of information (mostly attack definitions). In some cases, the update job can time out before it completes.</p> <p>To modify the timeout setting:</p> <ol style="list-style-type: none">1. On the NSM Device Server, open the following file in a text editor: <code>/usr/netscreen/DevSvr/var/devSvr.cfg</code>2. Modify the following setting: <code>devSvrDirectiveHandler.idpPolicyPush.timeout 2400000</code>
The following attacks/groups cannot be updated. Not supported for version.	<p>Different versions of IDP use different detector engines. Not all attack objects are valid for all versions of the detector engine. IDP indicates which attack objects in the security policy were not valid for the loaded detector engine and, therefore, not loaded.</p> <p>This message is for information purposes only and does not indicate a problem with the IDP device or the policy.</p>
No firewall rules can be updated for device in assigned policy policyName.	<p>You try to load a policy that contains a firewall rulebase onto a standalone IDP device.</p> <p>This message just means that IDP cannot process the firewall rulebase. The IDP rulebases are still processed normally, assuming no other errors.</p>
Rule #: Packet logging with any/any rule has serious performance implications.	<p>Setting the rule to log packets causes IDP to save packets until it is sure that they will not be needed for a log entry. A rule that has any in the Source IP column and any in the Destination IP column examines all traffic. So, IDP has to save a lot of packets all the time, which impacts performance.</p>
Policy has not changed and hence will not be updated.	<p>For performance reasons, IDP does not spend resources recompiling a security policy that has not changed.</p>
Failed to update device. Failed to compile policy.	<p>Something has gone wrong with the policy compilation. Other error messages may indicate why.</p>
No license for idp.	<p>The device does not have a valid license. Unlicensed devices do not accept policy uploads.</p>

Related Topics ■ NSM and Intrusion Detection and Prevention Device Management Overview

- Pushing Security Policy Updates to an IDP Device (NSM Procedure)

Published: 2009-08-20