

Understanding the Number of Available and Installed Policies

In NSM, you can create and save an unlimited number of security policies, and these policies are available to be installed on IDP appliances.

You can install the same security policy on an unlimited number of IDP appliances.

You can install one security policy on an IDP appliance. However, when you push a security policy update, you might observe more than one policy in place for a period after the update.

By default, IDP resets the flow table when you install a new policy. When the flow table is reset, existing sessions are passed through uninspected. For IDP75 and IDP200, you cannot override the default.

For high-end appliances, you can unset this default to avoid passing through sessions uninspected. Go to NSM Device Manager > Run-time Parameters and unselect **Reset flow table with policy load/unload**. If you unset this default, when you load a new policy, the IDP flow table will maintain sessions belonging to the previously installed policy as well as the newly installed policy. The IDP process engine will continue to use the previously installed security policy to inspect previous sessions; and use the newly installed security policy to inspect new sessions. When the previously installed policy is no longer in use, it is unloaded and all traffic is inspected using the newly installed policy. For IDP8200 and IDP250, the IDP engine can maintain flows for as many as two security policies. For IDP1100, IDP800, and IDP600, the IDP engine can maintain flows for as many as four security policies.

Related Topics The following related topic is included in the *IDP Concepts and Examples Guide*:

- Understanding the Components of an IDP Security Policy

The following related topic is included in the *IDP Administration Guide*:

- Developing Security Policies Task Summary
- Modifying the IDP Device Configuration

Published: 2010-01-12