

## Working with Attack Groups (NSM Procedure)

---

NSM groups are administrative objects that facilitate configuration and monitoring tasks. You can add attack groups or individual attack objects to IDP rulebase rules and Exempt rulebase rules.

- Creating Dynamic Groups on page 1
- Creating Static Groups on page 2

### Creating Dynamic Groups

A dynamic group contains attack objects that are automatically added or deleted based on specified criteria for the group. The NSM Object Manager includes predefined dynamic groups that work with recommended attack objects, predefined attack objects, the recommended security policy, and predefined policy templates.

When you run an NSM attack database update job, the process automatically performs the following tasks:

- For all new attack objects, compares the predefined attributes of each attack object to each dynamic group criteria and adds the attack objects that match.
- For all updated attack objects, removes attack objects that no longer meet their dynamic group criteria.
- Reviews updated attack objects to determine if they now meet any other dynamic group criteria, and adds them to those groups if necessary.
- For all deleted attack objects, removes the attack objects from their dynamic groups.

Use of dynamic groups eliminates the need to review each new signature to determine if you need to use it in your existing security policy.

A predefined or custom dynamic group can contain only attack objects and not attack groups. Dynamic group members can be either predefined or custom attack objects.

To create a custom dynamic group:

1. In Object Manager, select **Attack Objects > IDP Objects** to display the IDP Objects dialog box.
  2. Click the **Custom Attack Groups** tab, then click the + icon and select **Add Dynamic Group** to display the New Dynamic Group dialog box.
  3. Enter a name and description for the static group. Select a color for the group icon.
  4. In the Filters tab, click the + icon and add select filters that determine which attack objects should be in the group using Table 1.
2. Click the **Members** tab to view the attack objects now belonging to the group.
3. Click **OK** to save your settings.

**Table 1: Dynamic Attack Group Filters**

| Filter                   | Description  |
|--------------------------|--|
| Add Products Filter      | Filters attack objects based on the application that is vulnerable to the attack.  |
| Add Severity Filter      | Filters attack objects based on attack severity.<br><br><b>NOTE:</b> All predefined attack objects are assigned a severity level by Juniper Networks. However, you can edit this setting to match the needs of your network. |
| Add Category Filter      | Filters attack objects based on category.  |
| Add Last Modified Filter | Filters attack objects based on their last modification date.  |
| Add Recommended Filter   | Filters attack objects based on whether they have been marked Recommended.   |

## Creating Static Groups

A static group contains a specific, finite set of attack objects or groups. There are two types of static groups: predefined static groups and custom static groups.

A custom static group can include the same members as a predefined static group (predefined attack objects, predefined static groups, and predefined dynamic groups), plus the following members:

- Custom attack objects
- Custom dynamic groups
- Other custom static groups

Use static groups to define a specific set of attacks to which you know your network is vulnerable, or to group custom attack objects. For example, you might want to create a group for a specific set of informational attack objects that keep you aware of what is happening on your network.

Static groups require more maintenance than dynamic groups because you must manually add or remove attack objects in a static group to change the members. However, you can include a dynamic group within a static group to automatically update some attack objects. For example, the predefined attack object group Operating System is a static group that contains four predefined static groups: BSD, Linux, Solaris, and Windows. The BSD group contains the predefined dynamic group BSD-Services-Critical, to which attack objects can be added during an attack database update.

To create a custom static group:

1. In Object Manager, select **Attack Objects > IDP Objects** to display the IDP Objects dialog box.
2. Click the **Custom Attack Groups** tab, then click the + icon and select **Add Static Group** to display the New Static Group dialog box.

3. Enter a name and description for the static group.
4. Select a color for the group icon.
5. Select the attack or group from the Attacks/Group list and click **Add** .
6. Click **OK**.

- Related Topics**
- Attack Objects in Intrusion Detection and Prevention Security Policies Overview
  - Creating Custom Attack Objects (NSM Procedure)
  - Viewing Predefined Attack Objects (NSM Procedure)
  - Verifying the Attack Object Database Version (NSM Procedure)

---

Published: 2009-08-20