

Loading J-Security-Center Updates (NSM Procedure)

The Juniper Networks Security Center (J-Security Center) routinely makes important updates available to IDP security policy components, including updates to the IDP detector engine and NSM attack database.

The IDP detector engine is a dynamic protocol decoder that includes support for decoding more than 60 protocols and more than 500 service contexts. You should update IDP detector engine when you first install the IDP device, whenever you upgrade, and whenever alerted to do so by Juniper Networks.

The NSM attack database stores data definitions for the attack objects that are key components of IDP security policies. Updates can include new attack objects, revised severity settings, or removed attack objects. You should schedule daily updates to the NSM attack database.

After you have completed the update, any new attack objects are available in the security policy editor. If you use dynamic groups to your IDP rulebase rules and a new attack object belongs to the dynamic group, the rule automatically inherits the new attacks.

Table 1 provides procedures for updating IDP detector engine and the NSM attack database.

Table 1: IDP Detector Engine and NSM Attack Database Update Procedures

Task	Procedure
To download IDP detector engine and NSM attack database updates to the NSM GUI server	<p>From the NSM main menu, select Tools > View/Update NSM attack database and complete the wizard steps.</p> <p>NOTE: The default URL from which to obtain updates is https://services.netscreen.com/restricted/sigupdates/nsm-updates/NSM-SecurityUpdateInfo.dat. If you encounter connection errors, ensure this setting has not been inadvertently changed.</p> <ol style="list-style-type: none">1. From the NSM main menu, select Tools > Preferences.2. Click Attack Object.3. Click Restore Defaults. <p>NSM restores the URL in the Download URL for ScreenOS Devices text box.</p> <ol style="list-style-type: none">4. Click OK.
To push an IDP detector engine update from the NSM GUI server to IDP devices	<p>From the NSM main menu, select Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS and complete the wizard steps.</p> <p>NOTE: Updating the IDP detector engine on a device does not require a reboot of the device.</p>

Table 1: IDP Detector Engine and NSM Attack Database Update Procedures (continued)

Task	Procedure
To push predefined attack object updates from the NSM GUI server to IDP devices	<ol style="list-style-type: none"> 1. From the NSM main menu, select Devices > Configuration > Update Device Config. 2. Select the devices that you want to push configuration updates to and to set update job options on. 3. Click OK. <p>NOTE: Only the attack objects that are used in IDP rules for the device are pushed from the GUI server to the device.</p>
To schedule regular updates	<ol style="list-style-type: none"> 1. Log in to the NSM GUI server command line. 2. Change directory to <code>/usr/netscreen/GuiSvr/utlils</code>. 3. Create a shell script called <code>attackupdates.sh</code> with the following contents: <ul style="list-style-type: none"> ■ Set the <code>NSMUSER</code> environment variable with an NSM domain/user pair. The command for setting environment variables depends on your OS. Example: <pre style="margin-left: 40px;">export NSMUSER=domain/user</pre> ■ Set the <code>NSMPASSWD</code> environment variable with an NSM password. The command for setting environment variables depends on your OS and shell. Example: <pre style="margin-left: 40px;">export NSMPASSWD=password</pre> ■ Specify a <code>guiSvrCli</code> command string. Example: <pre style="margin-left: 40px;">/usr/netscreen/GuiSvr/utlils/guiSvrCli.sh -update-attacks -post-action -update-devices -skip</pre> 4. Make the script executable by the user associated with the cron job: <pre style="margin-left: 40px;">chmod 700 attackupdates.sh</pre> 5. Run the crontab editor: <pre style="margin-left: 40px;">crontab -e</pre> 6. Add an entry for the shell script: <pre style="margin-left: 40px;">minutes_after_hour hour * * * /usr/netscreen/GuiSvr/utlils/attackupdates.sh</pre> <p>During the update, the <code>guiSvrCli</code> utility updates the attack object database, then performs the post actions. After updating and executing actions, the system generates an exit status code of 0 (no errors) or 1 (errors).</p>

- Related Topics**
- Attack Objects in Intrusion Detection and Prevention Security Policies Overview
 - Viewing Predefined Attack Objects (NSM Procedure)

- Working with Attack Groups (NSM Procedure)

Published: 2009-08-20