



Juniper Networks ISG 2000

Getting Started Using IDP on the ISG 2000

Use the instructions in this Getting Started Guide to help you understand the basics of configuring Intrusion Detection and Prevention (IDP) functionality on your ISG 2000 device. You must use *Juniper Networks NetScreen-Security Manager 2004 FP3-IDPr1* to configure and manage IDP on the ISG 2000 device. Refer to the *NetScreen-Security Manager 2004 FP3-IDPr1 Administrator's Guide* for more information.

BEFORE YOU BEGIN...

Before you begin to configure and manage your ISG 2000 device, you must install and run the NetScreen-Security Manager management system and User Interface (UI). Refer to the *NetScreen-Security Manager 2004 FP3 Installer's Guide* for installation details for the NetScreen-Security Manager management system and UI.

After you have installed NetScreen-Security Manager, launch the UI and add the ISG 2000 device to the system. You also need to install an Advanced and IDP license key on the ISG 2000 device.

Note: To configure IDP on the ISG 2000 device, the device must be running ScreenOS 5.0 IDP and contain at least one Security module with IDP.

ADDING THE DEVICE

Use the Add Device wizard in the NetScreen-Security Manager UI to add the ISG 2000 device in the system, then configure some basic objects to represent the network components you want to protect.

Step 1

Launch the NetScreen-Security Manager User Interface (UI).

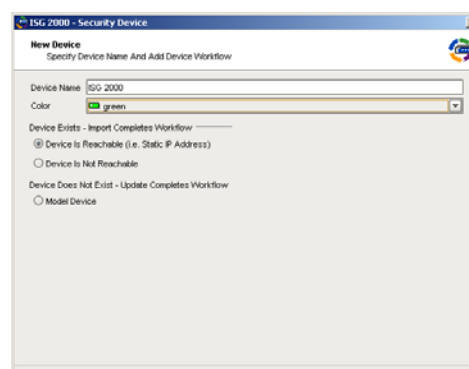
Step 2

In the main navigation tree, select **Device Manager > Security Devices**. Click the **Add** icon and select **Device**.



Step 3

The Add Device wizard appears. Follow the wizard instructions to successfully add the ISG 2000.



After you have added the device, use the **Device Monitor** to verify that the device is up and running.

Step 4

Use the **Object Manager** to add network components you want to protect. These components can be routers, servers, workstations, subnetworks, or any other object connected to your network.

Note: When you install an IDP license key on the ISG 2000 security device, DI is disabled.



CONFIGURING A SECURITY POLICY WITH IDP RULES

Configure a Security Policy with IDP rules, then install the policy on the ISG 2000 device.

Note: You must enable IDP in your firewall rules before creating your IDP rules. When using the ISG 2000 device as a dedicated IDP system, configure a simple firewall rule to direct all traffic to the Security module with IDP. For example, you would configure a simple, single firewall rule "ANY | ANY | PERMIT All" to direct all traffic to the Security module.

Step 1

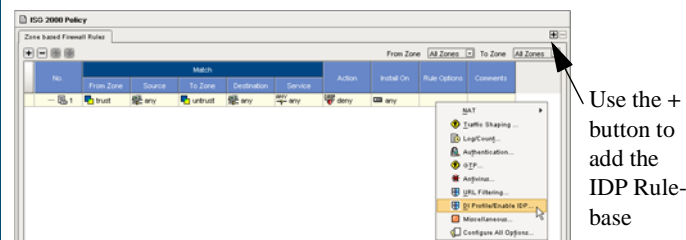
In the main navigation tree, select **Security Policies**, then select one of the following:

- To create a Security Policy from a template (recommended), click the **Add** icon. Select **Use IDP Template**, and choose the type of template you want from the pull-down menu.
Note: If you are using an IDP Template, you may bypass steps 2-6.
- To create a new custom Security Policy, in the main display area, click the **Add** icon. Configure the policy settings, then click **OK**.
- To edit an existing Security Policy, double-click the policy.

The Zone based Firewall rulebase appears, displaying the intrazone firewall rules for the Security Policy.

Step 2

Right-click in the **Rule Options** column of a rule and select **DI Profile/Enable IDP**.



The **DI Profile/Enable IDP** dialog box appears.

Note: The Attack Profile Settings apply only to the Deep Inspection (DI) feature on security devices. When you install the IDP license key on the ISG 2000 security device, DI is disabled.

Step 3

In the **IDP Option** area, select **Enabled** (option is disabled by default), then select one of the following IDP modes:

- Inline Mode.** In inline mode, the device passes network traffic that matches the selected rule directly to the Security module, enabling IDP to detect and prevent attacks.
- Tap Mode.** In inline tap mode, the device forwards the original traffic on the network, **and** sends a copy of every packet that matches the select rule to the Security module, enabling IDP to examine the traffic and flag potential problems.

Step 4

Right-click the **Install On** column and select the ISG 2000 device.

Step 5

From the menu bar, select **Edit > Add Rulebase > Add IDP Rulebase** to add the IDP rulebase, in which you can create IDP rules. You can also use the + button on the top right hand corner of the Security Policy window.

Note: To use the full functionality of IDP, you can create rules in three IDP-related rulebases: **IDP**, **Exempt**, and **Backdoor Detection**. For details on creating rules in all IDP-related rulebases, refer to the *NetScreen-Security Manager 2004 FP3-IDP1 Administrator's Guide*

Step 6

In the main display area, click the **Add** icon to add a default IDP rule. Right-click in each column to configure the following:

- Edit the Match columns, the **Action** column, and the **Attacks** columns of the rule as needed.
- In the **Notification** column, enable logging and set other notification preferences, if desired.
- In the **Install On** column, select the ISG 2000 device.

Create additional rules, as desired.

Step 7

From the menu bar, select **File > Assign Policy**. In the device list, select the ISG 2000 device, then click **OK**.

Step 8

From the menu bar, select **Devices > Configuration > Update Device Config**. In the device list, select the ISG 2000 device, then click **OK**.

Note: The first time you update the device may take several minutes to complete.



VIEWING IDP LOGS

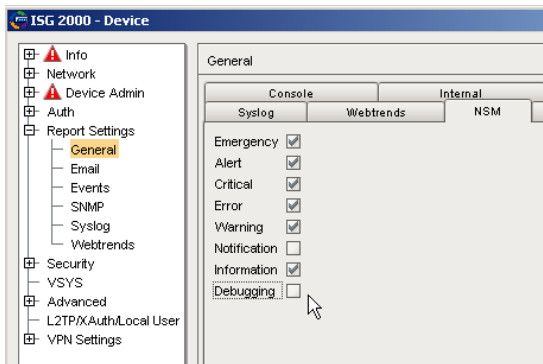
Enable the ISG 2000 device to send log entries to NetScreen-Security Manager, then update the device configuration on the device and begin viewing IDP logs.

Step 1

In the main navigation tree, select **Device Manager > Security Devices**, then double-click the ISG 2000 security device.

Step 2

In the device navigation tree, select **Report Settings > General > NSM**. The default reporting settings appear.



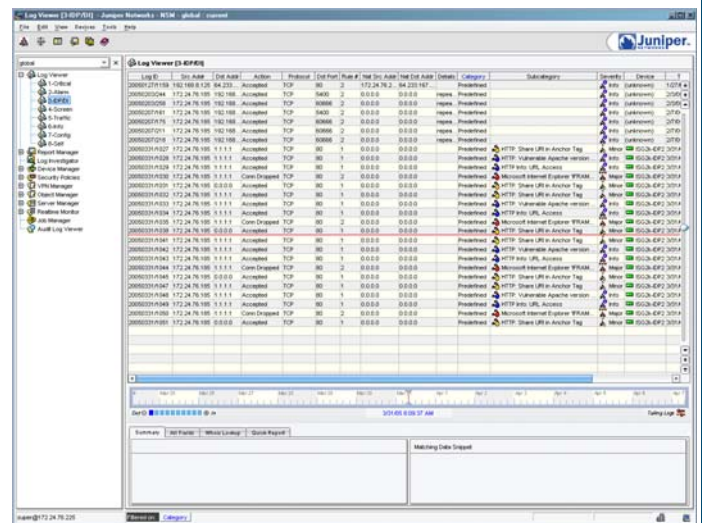
Step 3

Select the severity settings for all log entries that you want the device to forward to the NetScreen-Security Manager system, then click **OK**.

Remember to update your device configuration from **Devices > Configuration > Update Device Config**. In the device list, select the ISG 2000 device, then click **OK**.

Step 4

In the main navigation tree, select **Log Viewer > IDP/DI**. NetScreen-Security Manager displays logs in the order they are received from the device.



Step 5

You can add or remove columns from the Log Viewer depending on the type of information that you want to view. You can do this by selecting **View > Choose Columns**. Change your settings in the Column Settings window.

Step 6

To view all log entries (firewall and IDP) for all security devices in the domain, select the main Log Viewer view.

Note: Right-click on a host object within a log to display the option to create an Exempt rule.



MAINTAINING THE ATTACK OBJECT DATABASE

Perform frequent updates to the attack object database to ensure that you are protected against the latest attacks.

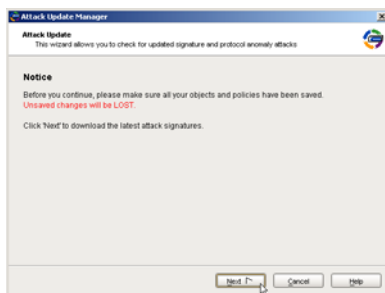
Step 1

Verify that the GUI Server has Internet access and DNS host resolution before proceeding to Step 2.

Step 2

From the menu bar, select **Tools > Update NSM Attack Database**.

The Update NSM Attack Database dialog box appears.

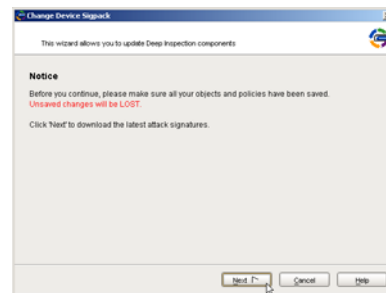


Follow the instructions in the **Attack Update Manager** to download new attack objects to the NetScreen-Security Manager GUI Server.

Step 3

From the menu bar, select **Devices > Deep Inspection > Update Device Attack Database**.

The Change Device Sigpack dialog box appears.



Step 4

Follow the directions in the **Change Device Sigpack** wizard to update the attack object database.

Remember to update your device configuration from **Devices > Configuration > Update Device Config** to apply the new signatures to your device(s).