NetScreen-Security Manager 2004
Migration Guide

Release FP3
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>2</td>
</tr>
<tr>
<td>Conventions</td>
<td>3</td>
</tr>
<tr>
<td>User Interface Conventions</td>
<td>4</td>
</tr>
<tr>
<td>Illustration Conventions</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>NetScreen-Security Manager 2004 FP3 Migration Guide Overview</td>
<td>6</td>
</tr>
<tr>
<td>Related NetScreen-Security Manager Documentation</td>
<td>7</td>
</tr>
<tr>
<td>Web Access</td>
<td>8</td>
</tr>
<tr>
<td>Comments About the Documentation</td>
<td>8</td>
</tr>
<tr>
<td>Contacting Customer Support</td>
<td>9</td>
</tr>
<tr>
<td><strong>Chapter 1</strong></td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>11</td>
</tr>
<tr>
<td>Migration and Installation Process</td>
<td>12</td>
</tr>
<tr>
<td>Management System Install Process</td>
<td>12</td>
</tr>
<tr>
<td>Migration Path</td>
<td>12</td>
</tr>
<tr>
<td>Data Export Process (Optional)</td>
<td>13</td>
</tr>
<tr>
<td>NetScreen-Global PRO Data Export Utility</td>
<td>13</td>
</tr>
<tr>
<td>Using the NetScreen-Global PRO Data Export Utility</td>
<td>14</td>
</tr>
<tr>
<td>Transferring Export Files</td>
<td>14</td>
</tr>
<tr>
<td>User Interface Install Process</td>
<td>14</td>
</tr>
<tr>
<td>Data Import Process (Optional)</td>
<td>14</td>
</tr>
<tr>
<td>Upgrade to NetScreen-Security Manager 2004 FP3</td>
<td>15</td>
</tr>
<tr>
<td>Installation Package</td>
<td>16</td>
</tr>
<tr>
<td>Minimum System Requirements</td>
<td>17</td>
</tr>
<tr>
<td>System Requirements - Management System</td>
<td>17</td>
</tr>
<tr>
<td>System Requirements - User Interface</td>
<td>18</td>
</tr>
<tr>
<td>Configuration Options</td>
<td>19</td>
</tr>
<tr>
<td>Typical Configuration</td>
<td>19</td>
</tr>
<tr>
<td>Extended Configuration</td>
<td>20</td>
</tr>
<tr>
<td>NetScreen-Statistical Report Server Interoperability</td>
<td>20</td>
</tr>
<tr>
<td>Local/Remote Database Backup</td>
<td>21</td>
</tr>
<tr>
<td>High Availability Configuration</td>
<td>21</td>
</tr>
<tr>
<td>HA Requirements</td>
<td>22</td>
</tr>
<tr>
<td>Data Replication</td>
<td>23</td>
</tr>
<tr>
<td>Failover Process</td>
<td>23</td>
</tr>
<tr>
<td>Restoring Connections</td>
<td>24</td>
</tr>
<tr>
<td>Capacity Planning For Additional Redundancy</td>
<td>24</td>
</tr>
<tr>
<td>Next Steps</td>
<td>25</td>
</tr>
<tr>
<td><strong>Chapter 2</strong></td>
<td></td>
</tr>
<tr>
<td>Migrating From Global PRO Express</td>
<td>27</td>
</tr>
<tr>
<td>Migration and Installation Scenarios</td>
<td>28</td>
</tr>
<tr>
<td>Installing NetScreen-Security Manager Using Existing Hardware</td>
<td>28</td>
</tr>
<tr>
<td>Installing NetScreen-Security Manager Using New Hardware</td>
<td>29</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Installing NetScreen-Security Manager Using Both Existing and New</td>
<td>29</td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
</tr>
<tr>
<td>Migration Scenarios Not Supported</td>
<td>30</td>
</tr>
<tr>
<td>Migration Path</td>
<td>30</td>
</tr>
<tr>
<td>Supported Devices</td>
<td>31</td>
</tr>
<tr>
<td>Pre-Migration Steps</td>
<td>32</td>
</tr>
<tr>
<td>Defining System Parameters</td>
<td>33</td>
</tr>
<tr>
<td>Typical Configuration Parameters</td>
<td>33</td>
</tr>
<tr>
<td>Extended Configuration Parameters</td>
<td>34</td>
</tr>
<tr>
<td>HA Configuration Parameters</td>
<td>35</td>
</tr>
<tr>
<td>Shared Disk Parameters</td>
<td>35</td>
</tr>
<tr>
<td>Prerequisite Steps</td>
<td>37</td>
</tr>
<tr>
<td>Other Recommended Actions</td>
<td>37</td>
</tr>
<tr>
<td>Running the System Update Utility</td>
<td>38</td>
</tr>
<tr>
<td>Patching the Sun Solaris SSH Daemon</td>
<td>39</td>
</tr>
<tr>
<td>Establishing a Trust Relationship</td>
<td>40</td>
</tr>
<tr>
<td>Installing the Management System Software</td>
<td>41</td>
</tr>
<tr>
<td>Viewing the Management System Installation Log</td>
<td>48</td>
</tr>
<tr>
<td>Starting Server Processes Manually</td>
<td>48</td>
</tr>
<tr>
<td>Validating Management System Status</td>
<td>49</td>
</tr>
<tr>
<td>Exporting Data From NetScreen-Global PRO Express</td>
<td>50</td>
</tr>
<tr>
<td>Transferring the Export Data Files</td>
<td>50</td>
</tr>
<tr>
<td>Installing the User Interface</td>
<td>51</td>
</tr>
<tr>
<td>Viewing the User Interface Installation Log</td>
<td>54</td>
</tr>
<tr>
<td>Running the User Interface</td>
<td>54</td>
</tr>
<tr>
<td>Validating the Installation</td>
<td>55</td>
</tr>
<tr>
<td>Running the UI in Demo Mode</td>
<td>56</td>
</tr>
<tr>
<td>Importing Data Into NetScreen-Security Manager</td>
<td>57</td>
</tr>
<tr>
<td>Import Process</td>
<td>57</td>
</tr>
<tr>
<td>Resolving Domain Name Conflicts</td>
<td>57</td>
</tr>
<tr>
<td>Importing Migration Data</td>
<td>58</td>
</tr>
<tr>
<td>Rolling Back a Failed Migration</td>
<td>59</td>
</tr>
<tr>
<td>Validating a Successful Migration</td>
<td>59</td>
</tr>
<tr>
<td>Post Migration Steps</td>
<td>60</td>
</tr>
<tr>
<td>Manually Configuring Protected Resources</td>
<td>60</td>
</tr>
<tr>
<td>Manually Configuring Authentication Servers</td>
<td>60</td>
</tr>
<tr>
<td>Manually Configuring VPNs</td>
<td>60</td>
</tr>
<tr>
<td>Transferring Certificate Files</td>
<td>60</td>
</tr>
<tr>
<td>Upgrading to NetScreen-Security Manager 2004 FP3</td>
<td>61</td>
</tr>
<tr>
<td>Next Steps</td>
<td>62</td>
</tr>
</tbody>
</table>

**Chapter 3  Migrating From Global PRO**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Scenarios</td>
<td>64</td>
</tr>
<tr>
<td>Installing Management System Using New Hardware</td>
<td>64</td>
</tr>
<tr>
<td>Installing Management System Using Existing Hardware</td>
<td>65</td>
</tr>
<tr>
<td>Considerations If You Are Running Multiple Arbitrators</td>
<td>66</td>
</tr>
<tr>
<td>Considerations If You Are Running Multiple Data Collectors</td>
<td>68</td>
</tr>
<tr>
<td>Maintaining Historical Reporting Functionality</td>
<td>68</td>
</tr>
<tr>
<td>Migration Scenarios Not Supported</td>
<td>68</td>
</tr>
<tr>
<td>Migration Path</td>
<td>68</td>
</tr>
<tr>
<td>Supported Devices</td>
<td>69</td>
</tr>
<tr>
<td>Pre-Migration Steps</td>
<td>70</td>
</tr>
<tr>
<td>Defining System Parameters</td>
<td>71</td>
</tr>
<tr>
<td>Typical Configuration Parameters</td>
<td>71</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Extended Configuration Parameters</td>
<td>72</td>
</tr>
<tr>
<td>HA Configuration Parameters</td>
<td>73</td>
</tr>
<tr>
<td>Shared Disk Parameters</td>
<td>73</td>
</tr>
<tr>
<td>Prerequisite Steps</td>
<td>75</td>
</tr>
<tr>
<td>Other Recommended Actions</td>
<td>75</td>
</tr>
<tr>
<td>Running the System Update Utility</td>
<td>76</td>
</tr>
<tr>
<td>Patching the Sun Solaris SSH Daemon</td>
<td>77</td>
</tr>
<tr>
<td>Installing the Management System Software</td>
<td>79</td>
</tr>
<tr>
<td>Viewing the Management System Installation Log</td>
<td>85</td>
</tr>
<tr>
<td>Starting Server Processes Manually</td>
<td>85</td>
</tr>
<tr>
<td>Validating Management System Status</td>
<td>86</td>
</tr>
<tr>
<td>Exporting Data From NetScreen-Global PRO</td>
<td>87</td>
</tr>
<tr>
<td>Policy Manager Export Data</td>
<td>87</td>
</tr>
<tr>
<td>Report Manager Export Data</td>
<td>87</td>
</tr>
<tr>
<td>Transferring the Export Data Files</td>
<td>87</td>
</tr>
<tr>
<td>Installing the User Interface</td>
<td>88</td>
</tr>
<tr>
<td>Viewing the Management System Installation Log</td>
<td>91</td>
</tr>
<tr>
<td>Running the User Interface</td>
<td>91</td>
</tr>
<tr>
<td>Validating the Installation</td>
<td>92</td>
</tr>
<tr>
<td>Running the UI in Demo Mode</td>
<td>93</td>
</tr>
<tr>
<td>Importing Data Into NetScreen-Security Manager</td>
<td>95</td>
</tr>
<tr>
<td>Import Process</td>
<td>95</td>
</tr>
<tr>
<td>Resolving Domain Name Conflicts</td>
<td>95</td>
</tr>
<tr>
<td>Import Migration Data</td>
<td>95</td>
</tr>
<tr>
<td>Rolling Back a Failed Migration</td>
<td>97</td>
</tr>
<tr>
<td>Validating a Successful Migration</td>
<td>97</td>
</tr>
<tr>
<td>Post Migration Processes</td>
<td>98</td>
</tr>
<tr>
<td>Historical Reporting</td>
<td>98</td>
</tr>
<tr>
<td>Manually Configuring Protected Resources</td>
<td>98</td>
</tr>
<tr>
<td>Manually Configuring Authentication Servers</td>
<td>98</td>
</tr>
<tr>
<td>Manually Configuring VPNs</td>
<td>98</td>
</tr>
<tr>
<td>Transferring Certificate Files</td>
<td>98</td>
</tr>
<tr>
<td>Disabling the Realtime Monitor Console</td>
<td>99</td>
</tr>
<tr>
<td>Disabling Historical Reporting</td>
<td>99</td>
</tr>
<tr>
<td>Upgrading to NetScreen-Security Manager 2004 FP3</td>
<td>100</td>
</tr>
<tr>
<td>Next Steps</td>
<td>101</td>
</tr>
<tr>
<td>Chapter 4 Maintaining NetScreen-Security Manager</td>
<td>103</td>
</tr>
<tr>
<td>Controlling the Management System</td>
<td>104</td>
</tr>
<tr>
<td>Viewing Management System Commands</td>
<td>104</td>
</tr>
<tr>
<td>Common Management System Commands</td>
<td>104</td>
</tr>
<tr>
<td>Starting All Server Processes Using the HA Server</td>
<td>105</td>
</tr>
<tr>
<td>Starting GUI Server and Device Server Processes Manually</td>
<td>105</td>
</tr>
<tr>
<td>Stopping Server Processes</td>
<td>106</td>
</tr>
<tr>
<td>Maintaining the Management System</td>
<td>107</td>
</tr>
<tr>
<td>Changing the Management System IP Address</td>
<td>107</td>
</tr>
<tr>
<td>Changing the Device Server IP Address</td>
<td>107</td>
</tr>
<tr>
<td>Configuring the Device Server Manually</td>
<td>108</td>
</tr>
<tr>
<td>Changing the GUI Server IP Address</td>
<td>108</td>
</tr>
<tr>
<td>Changing Permissions To a Normal User</td>
<td>109</td>
</tr>
<tr>
<td>Archiving and Restoring Logs and Configuration Data</td>
<td>110</td>
</tr>
<tr>
<td>Restoring Logs and Configuration Data</td>
<td>111</td>
</tr>
<tr>
<td>Configuring High Availability</td>
<td>112</td>
</tr>
<tr>
<td>Enabling and Disabling High Availability Processes</td>
<td>112</td>
</tr>
<tr>
<td>Chapter</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring High Availability Options</td>
<td>112</td>
</tr>
<tr>
<td>Running the Remote Replication Utility as a Non-Root User</td>
<td>113</td>
</tr>
<tr>
<td>Backing Up the Database Locally</td>
<td>113</td>
</tr>
<tr>
<td>Restoring the Database</td>
<td>113</td>
</tr>
<tr>
<td>Validating the Database Recovery Process</td>
<td>114</td>
</tr>
<tr>
<td>Relocating the Database</td>
<td>115</td>
</tr>
<tr>
<td>Archiving the GUI Server Database and Device Server Log Database</td>
<td>115</td>
</tr>
<tr>
<td>Installing NetScreen-Security Manager On a New System</td>
<td>116</td>
</tr>
<tr>
<td>Moving the Databases to the New System</td>
<td>116</td>
</tr>
<tr>
<td>Installing a tftp Server</td>
<td>118</td>
</tr>
<tr>
<td>Installing a tftp Server on Linux</td>
<td>118</td>
</tr>
<tr>
<td>Installing a tftp Server on Solaris</td>
<td>119</td>
</tr>
<tr>
<td>Downgrading from Feature Pack 3 to Feature Pack 2</td>
<td>120</td>
</tr>
<tr>
<td>Removing the Management System</td>
<td>121</td>
</tr>
<tr>
<td>Uninstalling the User Interface</td>
<td>122</td>
</tr>
<tr>
<td>Appendix A: Technical Overview</td>
<td>123</td>
</tr>
<tr>
<td>Technical Overview</td>
<td>124</td>
</tr>
<tr>
<td>About the Management System</td>
<td>124</td>
</tr>
<tr>
<td>GUI Server</td>
<td>125</td>
</tr>
<tr>
<td>Device Server</td>
<td>125</td>
</tr>
<tr>
<td>HA Server</td>
<td>125</td>
</tr>
<tr>
<td>About the NetScreen-Security Manager User Interface (UI)</td>
<td>126</td>
</tr>
<tr>
<td>About Managed FW/VPN Devices</td>
<td>126</td>
</tr>
<tr>
<td>Communications</td>
<td>127</td>
</tr>
<tr>
<td>Communication Ports and Protocols</td>
<td>127</td>
</tr>
<tr>
<td>Using the Secure Server Protocol (SSP)</td>
<td>129</td>
</tr>
<tr>
<td>Communications With Devices Running ScreenOS 5.0+</td>
<td>129</td>
</tr>
<tr>
<td>Communicating With Devices Running Screen 4.x and Earlier</td>
<td>150</td>
</tr>
<tr>
<td>Creating a Separate Management Network</td>
<td>151</td>
</tr>
<tr>
<td>Appendix B: Migration Details - Global PRO to NetScreen Security Manager</td>
<td>133</td>
</tr>
<tr>
<td>Domains</td>
<td>134</td>
</tr>
<tr>
<td>Domain Migration</td>
<td>154</td>
</tr>
<tr>
<td>Example</td>
<td>154</td>
</tr>
<tr>
<td>Devices and Device Groups</td>
<td>135</td>
</tr>
<tr>
<td>Policy Manager Device Migration</td>
<td>135</td>
</tr>
<tr>
<td>Report Manager/Realtime Monitor Device Migration</td>
<td>156</td>
</tr>
<tr>
<td>Example: Migrating Devices</td>
<td>156</td>
</tr>
<tr>
<td>Users and User Groups</td>
<td>138</td>
</tr>
<tr>
<td>Policy Manager User Migration</td>
<td>138</td>
</tr>
<tr>
<td>Report Manager/Realtime Monitor User Migration</td>
<td>139</td>
</tr>
<tr>
<td>Policy Manager User Group Migration</td>
<td>139</td>
</tr>
<tr>
<td>Report Manager/Realtime Monitor User Group Migration</td>
<td>140</td>
</tr>
<tr>
<td>Example: Migrating Users</td>
<td>140</td>
</tr>
<tr>
<td>Address Objects</td>
<td>142</td>
</tr>
<tr>
<td>Address Book Migration</td>
<td>142</td>
</tr>
<tr>
<td>Example: Migrating Address Book Objects</td>
<td>143</td>
</tr>
<tr>
<td>Schedule Objects</td>
<td>144</td>
</tr>
<tr>
<td>Schedule Object Migration</td>
<td>144</td>
</tr>
<tr>
<td>Example: Migrating Schedule Objects</td>
<td>144</td>
</tr>
<tr>
<td>Service Objects</td>
<td>145</td>
</tr>
<tr>
<td>Service Object Migration</td>
<td>145</td>
</tr>
</tbody>
</table>
### Table of Contents

- Example: Migrating Service Objects ................................................ 145
- Shared and Protected Resources .................................................... 146
  - Shared Resource Object Migration .............................................. 146
    - Example: Migrating Shared Resources ..................................... 146
- Global Objects .................................................................................. 148
  - Global Object Migration ............................................................... 148
    - Example: Migrating Global Objects ........................................... 148
- Authentication Servers ................................................................. 149
  - Authentication Server Object Migration .................................... 149
    - Example: Migrating Authentication Server Objects ................... 149
- Group Expressions .......................................................................... 151
  - Group Expression Migration ....................................................... 151
    - Example: Migrating Group Expression Objects ......................... 151
- Shared Configs ................................................................................ 152
  - Shared Config Object Migration .................................................. 152
    - Example: Migrating Shared Config Objects ............................... 153
- Zone Profile ..................................................................................... 154
  - Zone Profile Object Migration ...................................................... 154
    - Example: Migrating Zone Profile Objects .................................. 154
- Policies ............................................................................................ 155
  - Policy Migration ............................................................................ 155
    - Example: Migrating Policies NetScreen-Global PRO .................. 155
- VPNs .................................................................................................. 156
  - VPN Migration ............................................................................... 156
- P1 and P2 Proposals .......................................................................... 157
  - P1 and P2 Proposal Object Migration .......................................... 157
    - Example: Migrating P1 & P2 Proposal Objects ......................... 157
- IP Pools ............................................................................................ 158
  - IP Pool Migration ........................................................................... 158
    - Example: Migrating IP Pool Objects ......................................... 158
- Remote Settings ............................................................................... 159
  - Remote Setting Object Migration ................................................. 159
    - Example: Migrating Remote Settings Objects ............................ 159
- Events .............................................................................................. 160
- Certificates ....................................................................................... 161
- Data Collector Properties ............................................................... 162
- Master Controller Properties .......................................................... 163
- Historical Reports ............................................................................ 164
- Features No Longer Supported ....................................................... 165

#### Appendix C  Migration Details - FP1 to FP2

- Policy Migration .............................................................................. 168
  - Example: Migrating Policies Feature Pack 1 ............................... 168
About This Guide

This NetScreen-Security Manager 2004 FP3 Migration Guide describes how to install and setup an initial working NetScreen-Security Manager system using either new or existing hardware. It also describes how you can migrate data from your existing Juniper Networks management system into NetScreen-Security Manager.

This Migration Guide is intended primarily for IT administrators and primary application administrators who are responsible for installing NetScreen-Security Manager, and migrating data from either Juniper Networks NetScreen-Global PRO Express™ or Juniper Networks NetScreen-Global PRO™ into NetScreen-Security Manager.

NOTE: If you have not previously used a version of NetScreen-Global PRO or NetScreen-Global PRO Express, and are installing Juniper Networks management software for the first time, refer to the Juniper Networks NetScreen-Security Manager 2004 FP3 Installer’s Guide for more specific information on new installations of Juniper Networks NetScreen-Security Manager.
Audience

This guide is intended primarily for IT administrators who are responsible for installing NetScreen-Security Manager for the first.
Conventions

The sample screens used throughout this guide are representations of the screens you will see when you install and configure the SDX software. The actual screens may differ.

For convenience and clarity, the installation and configuration examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

The following tables define notice icons used in this guide and text conventions used throughout the book.

Table 1: Notice icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Info]</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![Caution]</td>
<td>Caution</td>
<td>Indicates that you may risk losing data or damaging your hardware.</td>
</tr>
<tr>
<td>![Warning]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury.</td>
</tr>
</tbody>
</table>

Table 2: Text conventions (except for command syntax)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold typeface</strong></td>
<td>Represents commands and keywords in text.</td>
<td>■ Command example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Issue the <strong>clock source</strong> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Keyword example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specify the keyword <em>exp-msg</em>.</td>
</tr>
<tr>
<td><strong>Bold sans serif typeface</strong></td>
<td>Represents text that the user must type.</td>
<td><strong>user input</strong></td>
</tr>
<tr>
<td>Key name in angle brackets</td>
<td>Indicates the name of a key on the keyboard.</td>
<td>Press <code>&lt;Enter&gt;</code>.</td>
</tr>
<tr>
<td>Key names linked with a plus sign (+) in angle brackets</td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Press <code>&lt;Ctrl+B&gt;</code>.</td>
</tr>
<tr>
<td><strong>Plain sans serif typeface</strong></td>
<td>Represents information as displayed on your terminal’s screen.</td>
<td><code>host1#show ip ospf 2</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Routing Process OSPF 2 with Router ID 5.5.0.250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Router is an Area Border Router (ABR)</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>■ Emphasize words.</td>
<td>■ There are two levels of access, user and privileged.</td>
</tr>
<tr>
<td></td>
<td>■ Identify variables.</td>
<td>■ clusterId, ipAddress.</td>
</tr>
</tbody>
</table>

Table 3: Syntax conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in plain text</td>
<td>Represent keywords.</td>
<td>terminal length</td>
</tr>
</tbody>
</table>
Table 3: Syntax conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in italics</td>
<td>Represent variables</td>
<td>mask, accessListName</td>
</tr>
<tr>
<td>Words separated by the</td>
<td>symbol</td>
<td>Represent a choice to select one keyboard or variable to the left or right of this symbol. (The keyboard or variable may be either optional or required.)</td>
</tr>
<tr>
<td>Words enclosed in [ brackets ]</td>
<td>Represent optional keywords or variables.</td>
<td>[ internal</td>
</tr>
<tr>
<td>Words enclosed in [ brackets ]*</td>
<td>Represent optional keywords or variables that can be entered more than once.</td>
<td>[ level1</td>
</tr>
<tr>
<td>Words enclosed in { braces }</td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

User Interface Conventions

The sample screens used throughout this guide are representations of the screens you will see when you administer the Netscreen-Security Manager 2004 FP3.

Throughout this book, a chevron ( > ) is used to indicate navigation through the UI by clicking menu options and links. For example, the path to the local user configuration is presented as **Object Manager > User Objects > Local User Objects**, as shown below.
1. In the main navigation tree, select Object Manager. The Object Manager tree expands to reveal a subset of objects.

2. In the Object Manager navigation tree, select User Objects. The main display area displays all defined user objects.

3. In the User Objects navigation tree, select Local User Objects. The main display area displays all defined local user objects.
Illustration Conventions

The following graphics make up the basic set of images used in illustrations throughout this book.

Figure 2: Illustration Conventions

Local Area Network (LAN) with a Single Subnet. (example: 10.1.1.0/24)

Security Zone

Internet

Security Zone Interfaces

White = Protected Zone Interface (example: Trust Zone)

Black = Outside Zone Interface (example: Untrust Zone)

Tunnel Interface

VPN Tunnel

Documentation

This section describes documentation for NetScreen-Security Manager.

NetScreen-Security Manager 2004 FP3 Migration Guide Overview

This guide details the steps to:

- Install NetScreen-Security Manager using new or existing hardware
- Migrate data previously configured in Global PRO or Express (i.e., using scripts and other manual migration steps)
- Map data and features in Global PRO/Express to NetScreen-Security Manager

This guide is intended for existing administrators of NetScreen-Global PRO or NetScreen-Global PRO Express who are installing NetScreen-Security Manager 2004 FP3 for the first time.
Related NetScreen-Security Manager Documentation

The NetScreen-Security Manager 2004 FP3 documentation set includes the following guides:

NetScreen-Security Manager 2004 FP3 Getting Started Guide—This guide details the steps to install the NetScreen-Security Manager management system on a single server. It also includes information on how to install and run the NetScreen-Security Manager user interface. This guide is intended for IT administrators responsible for the installation and initial setup of NetScreen-Security Manager.

NetScreen-Security Manager 2004 FP3 Rapid Deployment Getting Started Guide—This guide details the steps to install and implement Rapid Deployment (RD) configlets. It is intended for on-site administrators responsible for the installation and initial setup of devices to be managed by NetScreen-Security Manager in rapid deployment scenarios.

NetScreen-Security Manager 2004 FP3 Installer’s Guide—This guide details the steps to install the NetScreen-Security Manager management system on a single server or on separate servers. It also includes information on how to install and run the NetScreen-Security Manager user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NetScreen-Security Manager 2004 FP3.

NetScreen-Security Manager 2004 FP3 Administrator’s Guide—This guide describes how to use and configure key management features in the NetScreen-Security Manager. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NetScreen-Security Manager 2004 FP3 Online Help, which provides step-by-step instructions for performing management tasks in the NetScreen-Security Manager UI.

This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.

NetScreen-Security Manager 2004 FP3 Online Help—The online help provides task-oriented procedures describing how to perform basic tasks in the NetScreen-Security Manager user interface. It also includes a brief overview of the NetScreen-Security Manager system and a description of the GUI elements.

The online help is best used in conjunction with the NetScreen-Security Manager 2004 FP3 Administrator’s Guide, which provides conceptual information, suggested workflows, and examples for management tasks where applicable.

The online help is intended for network and security administrators who are using the UI to configure and manage devices.

NetScreen-Security Manager 2004 FP3 Release Notes—The release notes provide latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the Release Notes differs from the information found in the documentation set, follow the Release Notes.
Release notes are included on the corresponding software CD and are available on the Web.

The documentation is also available on the Web. You can order a set of printed documents from your Juniper Networks sales representative.

**Web Access**

To view the documentation on the Web, go to:

http://www.juniper.net/techpubs/

**Comments About the Documentation**

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Please e-mail your comments to:

- techpubs-comments@juniper.net

Along with your comments, be sure to indicate:

- Document name
- Document part number
- Page number
- Software release version
Contacting Customer Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (within the United States) or 408-745-9500 (from outside the United States).
Chapter 1
Introduction

In This Chapter:

- Migration and Installation Process
- Installation Package
- Minimum System Requirements
- Configuration Options
- Next Steps

Juniper Networks NetScreen-Security Manager is software that enables you to integrate control and management of your network security environment including firewalls and VPNs. You can install NetScreen-Security Manager using new hardware or over your existing hardware configuration. If you are currently using a previous version of Juniper Networks management software (NetScreen-Global PRO or NetScreen-Global PRO Express), you can also migrate your existing configuration data into NetScreen-Security Manager.

This chapter provides an overview of the NetScreen-Security Manager migration and installation process, minimum hardware and software requirements and other migration planning considerations.
Migration and Installation Process

There are two main software components that you need to install and run NetScreen-Security Manager, the NetScreen-Security Manager management system and the NetScreen-Security Manager User Interface (UI).

The overall process for installing NetScreen-Security Manager and migrating configuration data from your previous Juniper Networks management software is as follows:

- Management System Install Process on page 12
- Data Export Process (Optional) on page 13
- User Interface Install Process on page 14
- Data Import Process (Optional) on page 14
- Upgrade to NetScreen-Security Manager 2004 FP3 on page 15

Management System Install Process

The management system installer enables you to install all of the software required to run each component of the NetScreen-Security Manager management system.

The management system installer is a shell archive script that you can run on any dedicated Solaris 8 or 9, Red Hat Linux 8.0, 9.0, Red Hat Enterprise Linux ES 3.0, or Red Hat Enterprise Linux AS server that meets minimum system requirements. Refer to Minimum System Requirements on page 17 for more information on the minimum required hardware and software that you need to install the NetScreen-Security Manager management system.

There are separate installer scripts for Linux and Solaris installations. When you launch the management system installer, the script guides you through all the steps required to install and configure each management system component.

Migration Path

The migration of data from the following previous versions of Juniper Networks management software is supported up to NetScreen-Security Manager 2004 FP2:

- NetScreen-Global PRO Express
- NetScreen-Global PRO

NOTE: NetScreen-Security Manager does not support the migration of data from Juniper Networks NetScreen-IDP.

After you have migrated your data successfully to NetScreen-Security Manager 2004 FP2, you can then upgrade to NetScreen-Security Manager 2004 FP3.
**Data Export Process (Optional)**

If you wish to migrate data from your previous version of Juniper Networks management software, you must install and run the NetScreen-Global PRO data export utility over your existing hardware configuration.

**NetScreen-Global PRO Data Export Utility**

The NetScreen-Global PRO data export utility is a shell archive script (the file is called "nsm04fp2_gpexport_sol_sparc.sh" and is a part of the installation package for NetScreen-Security Manager 2004 FP2) that you can install and run on any Solaris system. If you run the NetScreen-Security Manager 2004 FP2 installer for Solaris on your existing NetScreen-Global PRO Express appliance or NetScreen-Global PRO arbitrator, the installer automatically detects if you are running NetScreen-Global PRO or NetScreen-Global PRO Express on the system. If NetScreen-Global PRO or NetScreen-Global PRO Express is detected, then the installer automatically installs and runs the utility.

The NetScreen-Global PRO data export utility performs all the functions necessary to export configuration data from your previous installation of NetScreen-Global PRO or NetScreen-Global PRO Express including device configuration data from the managed FW/VPN devices in your network. During the export process, you can specify whether you want to export data from all domains, a group of domains (you can do this by listing them separated by a comma), or a specific domain in Policy Manager.

The process by which the NetScreen-Global PRO data export utility extracts configuration data is as follows:

1. Initially, the NetScreen-Global PRO data export utility extracts configuration data from the local LDAP server on the NetScreen-Global PRO Express appliance or NetScreen-Global PRO arbitrator. For Report Manager, it extracts configuration data from the database on the Report Manager Master Controller.
2. It attempts to contact each individual managed device for the latest device configuration data. If the utility is successful in connecting to the device, then it retrieves the device configuration directly from the device.
3. If the utility is not successful in connecting to the device, then it extracts the device configuration from the latest configuration summary generated for the device in Policy Manager.

When it has completed this process, the NetScreen-Global PRO data export utility saves export data from Policy Manager and your device configurations in the following location:

```
/usr/netscreen/migration/var/data/pmexport.tar
```

The NetScreen-Global PRO data export utility saves the export data from Realtime Monitor or Report Manager in the following location:

```
/usr/netscreen/migration/var/data/RMexport.out
```
Using the NetScreen-Global PRO Data Export Utility

The following table outlines instructions for migrating from NetScreen-Global PRO Express and NetScreen-Global PRO.

<table>
<thead>
<tr>
<th>Migrating From...</th>
<th>Install and run the...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks NetScreen-Global PRO Express</td>
<td>NetScreen-Security Manager installer for Solaris on the NetScreen-Global PRO Express appliance. The installer automatically detects your previous installation of NetScreen-Global PRO Express and installs and runs the NetScreen-Global PRO data export utility.</td>
</tr>
<tr>
<td>Juniper Networks NetScreen-Global PRO</td>
<td>NetScreen-Global PRO data export utility on the servers where you are running your NetScreen-Global PRO arbitrator(s) for Policy Manager and device configuration data. NetScreen-Global PRO data export utility on the server where you are currently running your Report Manager Master Controller for Report Manager data.</td>
</tr>
</tbody>
</table>

Once you have completed exporting your data from your previous Juniper Networks management software, you can then import the data into NetScreen-Security Manager using the NetScreen-Security Manager User Interface.

Transferring Export Files

Once you have exported your data from NetScreen-Global PRO and NetScreen-Global PRO Express, you must transfer the files to the following directory location on the server where you have installed your GUI Server:

```
/usr/netscreen/GuiSvr/var/migration/
```

User Interface Install Process

The NetScreen-Security Manager User Interface installer launches an InstallAnywhere wizard that you can run on any Windows-based computer that meets minimum system requirements. Refer to Minimum System Requirements on page 17 for more information on the minimum required hardware and software that you need to install the NetScreen-Security Manager User Interface.

The InstallAnywhere wizard guides you through all the steps required to configure and install the User Interface. Once you install the User Interface, you can connect it to the management system.

Data Import Process (Optional)

Once you are connected to the NetScreen-Security Manager management system, you can import your exported data into NetScreen-Security Manager.
You can run the import process multiple times without corrupting the NetScreen-Security Manager database. The import of Policy Manager and Realtime Monitor/Report Manager data can be done at the same time or separately. If you are planning on importing data from both Policy Manager and Realtime Monitor/Report Manager, it is highly recommended that you perform the import of data from Policy Manager before or at the same time as you import your data from Realtime Monitor/Report Manager. This is because you want to establish your configuration data in NetScreen-Security Manager in the domains that applied in Policy Manager. This configuration data is inherent in Policy Manager. Data configured in Realtime Monitor/Report Manager is not domain-specific.

Refer to Chapter 2, Migrating From Global PRO Express for more information on migrating from NetScreen-Global PRO Express.

Refer to Chapter 3, Migrating From Global PRO for more information on migrating from NetScreen-Global PRO.

**Upgrade to NetScreen-Security Manager 2004 FP3**

After you have completed installing NetScreen-Security Manager 2004 FP2, and successfully migrated your previous management data to it, you can then proceed to upgrade to NetScreen-Security Manager 2004 FP3.
Installation Package

All of the software files required to install NetScreen-Security Manager 2004 FP2 and NetScreen-Security Manager 2004 FP3 are located on the NetScreen-Security Manager installation CD or on the Internet at the Juniper Networks corporate support web site. It is recommended that you download these files to the computers on which you plan to install NetScreen-Security Manager before beginning the installation process.

The following table describes the contents of the NetScreen-Security Manager 2004 FP3 installation CD.

Table 5: NetScreen-Security Manager 2004 FP3 Installation Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsm04fp3_ui_win_x86.exe</td>
<td>Installer for the NetScreen-Security Manager UI (for Windows-based computers).</td>
</tr>
<tr>
<td>nsm04fp3_ui_linux_x86.bin</td>
<td>Installer for the NetScreen-Security Manager UI (for Linux-based computers).</td>
</tr>
<tr>
<td>nsm04fp3_servers_linux_x86.sh</td>
<td>Installer for the NetScreen-Security Manager management system for Linux</td>
</tr>
<tr>
<td>nsm04fp3_servers_sol_sparc.sh</td>
<td>Installer for the NetScreen-Security Manager management system for Solaris</td>
</tr>
<tr>
<td>systemupdate-nsm-linux.tar</td>
<td>System update utility for Linux. You use this file to update files on your system required for the installer to run properly.</td>
</tr>
<tr>
<td>systemupdate-nsm-solaris.tar</td>
<td>System update utility for Solaris. You use this file to update files on your system required for the installer to run properly.</td>
</tr>
</tbody>
</table>

NOTE: The data export utility is a shell archive script called "nsm04fp2_gpexport_sol_sparc.sh". It is included with the installation package for NetScreen-Security Manager 2004 FP2.
Minimum System Requirements

The following minimum hardware and software requirements must be met to properly install and run NetScreen-Security Manager.

**System Requirements - Management System**

The following table describes the minimum requirements that must be met for the GUI Server and Device Server on the same server:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES 3.0, Red Hat Enterprise Linux AS</td>
</tr>
<tr>
<td>CPU</td>
<td>Sun Microsystems UltraSPARC IiI 500MHz (or higher), OR Linux 1GHz (x86) processor (or higher)</td>
</tr>
<tr>
<td>RAM</td>
<td>1GB (or higher); 2GB+ (depending on the number of managed devices and configuration size)</td>
</tr>
<tr>
<td>Swap Space</td>
<td>4 GB for both GUI Server and Device Server</td>
</tr>
<tr>
<td>Storage</td>
<td>IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)</td>
</tr>
<tr>
<td>Network Connection</td>
<td>100MBps NIC Ethernet adapter</td>
</tr>
<tr>
<td>Other</td>
<td>Server must be dedicated to running NetScreen-Security Manager</td>
</tr>
</tbody>
</table>

The following table describes the minimum requirements that must be met for the GUI Server and Device Server on separate servers:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES 3.0, Red Hat Enterprise Linux AS</td>
</tr>
<tr>
<td>CPU</td>
<td>Sun Microsystems UltraSPARC IiI 500MHz (or higher), OR Linux 1GHz (x86) processor (or higher)</td>
</tr>
<tr>
<td>RAM</td>
<td>512MB (or higher); 1GB (recommended)</td>
</tr>
<tr>
<td>Swap Space</td>
<td>2 GB for the GUI Server, 2 GB for the Device Server</td>
</tr>
<tr>
<td>Storage</td>
<td>IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)</td>
</tr>
<tr>
<td>Network Connection</td>
<td>100MBps NIC Ethernet adapter</td>
</tr>
</tbody>
</table>
System Requirements - User Interface

The following table describes the minimum system requirements that must be met for the User Interface:

Table 8: Minimum System Requirements - User Interface

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows XP, OR</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows NT® Workstation/Server 4.0, Service Pack 6a or higher, OR</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows 2000 Server, Advanced Server, or Professional editions OR</td>
</tr>
<tr>
<td></td>
<td>Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES 3.0, Red Hat Enterprise Linux AS</td>
</tr>
<tr>
<td></td>
<td>US English versions only</td>
</tr>
<tr>
<td>Hardware</td>
<td>IBM® compatible PC</td>
</tr>
<tr>
<td></td>
<td>400MHz Pentium® II or equivalent (minimum); 700 MHz Pentium II or equivalent (recommended)</td>
</tr>
<tr>
<td></td>
<td>RAM: 256 MB (minimum); 512 MB or above (recommended)</td>
</tr>
<tr>
<td></td>
<td>384kbps (DSL) or LAN connection - minimum bandwidth required to connect to the NetScreen-Security Manager management system</td>
</tr>
</tbody>
</table>

NOTE: You can extend system performance and data capacity by expanding the minimum requirements specified for each component.
Configuration Options

You can design and implement NetScreen-Security Manager to scale to small, medium, and large enterprises, as well as service provider deployments. There are two main options for configuring NetScreen-Security Manager:

- Typical Configuration on page 19
- Extended Configuration on page 20
- High Availability Configuration on page 21

NOTE: Juniper Networks NetScreen-Security Manager 2004 FP3 provides support for only one GUI Server and one Device Server. In future releases of NetScreen-Security Manager, you will be able to install and deploy multiple Device Servers in your network to provide greater scalability and performance.

Typical Configuration

The most straightforward implementation of the NetScreen-Security Manager management system is to install both components of the management system (GUI Server and Device Server) on the same server. This configuration is appropriate for most typical small to medium-sized enterprises.

Figure 3: Typical Management System Configuration
**Extended Configuration**

For larger enterprises, specifically where you expect to generate and store a large amount of traffic logs, it is recommended that you install the GUI Server and Device Server on separate servers.

*Figure 4: Extended Management System Configuration*

**NetScreen-Statistical Report Server Interoperability**

If you are installing NetScreen-Statistical Report Server, you must configure it to work with NetScreen-Security Manager. During the installation or upgrade process, the installer script prompts you configure parameters enabling the management system to communicate with the Statistical Report Server database and web server. If you type "y", the installer script prompts you to configure the following additional parameters enabling the management system to work with the NetScreen-Statistical Report Server database:

- database type
- database server IP address
- database port
- database name
- database user name
- database password

Refer to the *NetScreen-Statistical Report Server Installer’s Guide* for more information.
Local/Remote Database Backup

You can also configure the management system to perform an automatic backup of the GUI Server database to the local server machine and if necessary, to a remote server machine. During the installation or upgrade process, the installer script prompts you to specify if this server machine requires local database backups. If you type “y”, the installer script prompts you to configure the following additional parameters enabling the management system to perform automatic daily backups of the database:

- Hour of Day to store the database backup
- Number of database backups to keep
- Directory where local database backups are stored
- Full path to the rsync command—the management system uses the rsync utility to perform the database backup

If you want to send copies of the database backup to a remote machine, the installer script prompts you to configure the following additional parameters:

- IP Address of the remote machine
- Full path to the ssh command—the management system uses the ssh utility to perform the database backup

**NOTE:** If you want the management system to perform remote database backups, you will need to setup a trust relationship between the management system server and the remote machine.

---

High Availability Configuration

You can also install and configure the management system to provide for high availability. This configuration option is recommended to minimize the impact of any unplanned server outages.

To implement the management system for high availability, you need to install two management systems: a primary server that runs on a server machine in active mode; and a secondary server that runs on a different server machine in standby mode. If for any reason, the primary server becomes unavailable, the secondary server takes over as the active management system.

During the installation or upgrade process, the installer script prompts you to specify whether or not you want the current server machine to participate in an HA cluster. If you type “y”, the installer script prompts you to configure additional parameters enabling the high availability features on the management system.
**HA Requirements**

Some system requirements that you need to keep in mind if you are planning on installing the management system for high availability:

- Both the primary and secondary management servers must share at least one network connection—there must be at least one network connection for data, and at least one network connection for heartbeat communication.

- The primary and secondary GUI Servers can be geographically separate.

The following illustration depicts the physical setup of the primary and secondary management systems:
**Data Replication**

The GUI Server uses the rsync utility to replicate configuration data to the standby GUI Server. The remote replication process occurs every 60 minutes by default. You can also configure the GUI Server to perform a local backup copy of the database automatically.

Note that device log data is not remotely replicated because of the large data size. If you want the standby Device Server to access log data also on the active Device Server, you must connect both servers to an external shared disk.

**Failover Process**

During normal operations, both the primary and secondary management systems monitor the health of the other using a series of heartbeat communications. Each server sends a heartbeat message to the other server every 15 seconds. If a series of consecutive heartbeat messages is not received by the primary server, the secondary server takes over for the primary server. So for example, if you are running the primary GUI Server and Device Server on Server 1 and the secondary GUI Server and Device Server on Server 2; and the primary GUI Server fails—both the primary GUI Server and primary Device Server on Server 1 are shutdown; and both the secondary GUI Server and Device Server on Server 2 start up.

In the event of a process failure on the primary server, the primary server proceeds as follows:

1. shuts down all local server processes
2. synchronizes all information to disk
3. un-mounts the shared partitions (if using a shared disk)
4. signals to the new server that it is done shutting down

The HA process in the old server then enters an ERROR mode, and stays in that mode until you manually restart the HA startup scripts. Refer to Controlling the Management System on page 104 for more information.
The new server, after receiving the signal or a signal-timeout, mounts the shared partitions and then cleans the file system (i.e., runs fsck on the shared partitions). Note that the mount and fsck actions are only taken if a shared disk is used.

**Restoring Connections**

In the event that the GUI Server fails over, the Device Server detects this status and automatically reconnects to the secondary GUI Server.

If you are attempting to connect to the GUI Server using the User Interface, you must enter the Secondary Server IP Address to reconnect to the new GUI Server IP Address.

**NOTE:** After failover, it will take some time for the standby management system to become fully active with the replicated database. For large networks, this can take up to 10 minutes.

In the event that the Device Server fails over, the managed FW/VPN devices in your network detect this, and automatically reconnect to the secondary Device Server.

**Capacity Planning For Additional Redundancy**

For additional redundancy, it is recommended that you install at least two additional heartbeat network connections. This installation protects against the heartbeat network connection from being the single point of failure for the entire system. For example, if a shared disk setup is used, in case one of the heartbeat network connections goes down, both servers would not consider the other server as dead, thus mounting the shared disk simultaneously, resulting in a corrupted file system.

If you choose to install two network cards, it is recommended that you use one dedicated interface for heartbeat communications, in addition to one for network communications.
Next Steps

This chapter has provided you with the following:

- an overview of the migration and installation process
- minimum system requirements to help you identify the appropriate hardware and software to install and run NetScreen-Security Manager
- options for implementing components of the NetScreen-Security Manager management system to provide for enhanced performance and scalability

You should use this information to plan how best to implement NetScreen-Security Manager and integrate it into your network. When you are ready to install NetScreen-Security Manager Feature Pack 2, there are several installation and migration scenarios that exist depending upon the type of Juniper Networks management software that you have previously used:

- See Chapter 2, Migrating From Global PRO Express for specific information on how to install and migrate to NetScreen-Security Manager if you are currently using NetScreen-Global PRO Express.

- See Chapter 3, Migrating From Global PRO for specific information on how to install and migrate to NetScreen-Security Manager if you are currently using NetScreen-Global PRO.

- See Chapter 4, Maintaining NetScreen-Security Manager for specific information describing how to maintain and uninstall the management system and UI.
Chapter 2

Migrating From Global PRO Express

In This Chapter:

- Migration and Installation Scenarios
- Pre-Migration Steps
- Defining System Parameters
- Prerequisite Steps
- Installing the Management System Software
- Exporting Data From NetScreen-Global PRO Express
- Installing the User Interface
- Importing Data Into NetScreen-Security Manager
- Post Migration Steps
- Upgrading to NetScreen-Security Manager 2004 FP3
- Next Steps

This chapter describes the NetScreen-Security Manager migration and installation process for those who have previously used Juniper Networks NetScreen-Global PRO Express. It describes scenarios and procedures for migrating your configuration data from NetScreen-Global PRO Express and installing NetScreen-Security Manager using new or existing hardware.
Migration and Installation Scenarios

If you are currently using NetScreen-Global PRO Express, migration and installation scenarios are as follows:

- Installing NetScreen-Security Manager Using Existing Hardware on page 28
- Installing NetScreen-Security Manager Using New Hardware on page 29
- Installing NetScreen-Security Manager Using Both Existing and New Hardware on page 29

Installing NetScreen-Security Manager Using Existing Hardware

The following table details the migration and installation process if you are using existing hardware. It also provides an estimate of the overall amount of time each step requires.

Table 9: Installation Process for Installing NSM Using Existing Hardware

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
</table>
| 1    | Copy the required software to install the NetScreen-Security Manager 2004 FP2 management system (for Solaris) on your existing NetScreen-Global PRO Express appliance.  
      Copy the required software for the NetScreen-Security Manager user interface to the computer where you plan to install the UI. (10 minutes) |
| 2    | Run the NetScreen-Security Manager 2004 FP2 management system installer on your existing NetScreen-Global PRO Express appliance to install the management system.  
      The installer automatically detects if you have NetScreen-Global PRO Express installed on the appliance. It then installs and runs the NetScreen-Global PRO data export utility automatically. The NetScreen-Global PRO data export utility exports your data from NetScreen-Global PRO Express and the managed FW/VPN devices in your network, and then saves the exported data in two files:  
      - pmexport.tar for your Policy Manager and device configuration data  
      - rmexport.out for your Realtime Monitor data  
      (2-8 hours) |
| 3    | Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server. (10 minutes) |
| 4    | Install the NetScreen-Security Manager 2004 FP2 User Interface. (5 minutes) |
| 5    | Launch the UI, and connect it to the management system. (5 minutes) |
| 6    | Import your configuration data into NetScreen-Security Manager. Validate the migration. (Optional) (2-4 hours (avg) - based on size of Express database) |
| 7    | Perform any necessary post-migration steps. Remove your previous Juniper Networks management software version. (Optional) (30 minutes) |
| 8    | Run the NetScreen-Security Manager 2004 FP3 management system installer and upgrade the system to NetScreen-Security Manager 2004 FP3. (10 minutes) |
| 9    | Run the NetScreen-Security Manager 2004 FP3 UI installer and upgrade the UI to NetScreen-Security Manager 2004 FP3. (5 minutes) |
Installing NetScreen-Security Manager Using New Hardware

It is possible to extend system performance by installing NetScreen-Security Manager onto new hardware that exceeds the prescribed minimum system requirements. The following table details the migration and installation process if you plan to install the NetScreen-Security Manager management system using new hardware. It also provides an estimate of the overall amount of time each step requires.

Installation Process for Installing NSM Using New Hardware (10 minutes)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Copy the required software to install the NetScreen-Security Manager 2004 FP2 management system on the server(s) where you plan to install the NetScreen-Security Manager GUI Server and Device Server. (5 minutes) Copy the NetScreen-Global PRO data export utility installer to your existing NetScreen-Global PRO Express appliance. (5 minutes) Copy the NetScreen-Security Manager 2004 FP2 User Interface installer to the computer where you plan to install the UI. (5 minutes)</td>
</tr>
<tr>
<td>2</td>
<td>Install the NetScreen-Security Manager management system. (10 minutes)</td>
</tr>
<tr>
<td>3</td>
<td>Install the NetScreen-Global PRO data export utility installer on your existing NetScreen-Global PRO Express appliance. Run the NetScreen-Global PRO data export utility to export your data from NetScreen-Global PRO Express and the managed FW/VPN devices in your network. The NetScreen-Global PRO data export utility saves the exported data in two files:</td>
</tr>
<tr>
<td></td>
<td>■ pmexport.tar for your Policy Manager and device configuration data</td>
</tr>
<tr>
<td></td>
<td>■ rmexport.out for your Realtime Monitor data</td>
</tr>
<tr>
<td>4</td>
<td>Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server. (10 minutes)</td>
</tr>
<tr>
<td>5</td>
<td>Install the NetScreen-Security Manager 2004 FP2 User Interface. (5 minutes)</td>
</tr>
<tr>
<td>6</td>
<td>Launch the UI, and connect it to the management system. (5 minutes)</td>
</tr>
<tr>
<td>7</td>
<td>Import your configuration data into NetScreen-Security Manager. Validate the migration. (Optional) (2-4 hours (avg) - based on size of Express database)</td>
</tr>
<tr>
<td>8</td>
<td>Perform any necessary post-migration steps. Remove your previous Juniper Networks management software version. (Optional) (30 minutes)</td>
</tr>
<tr>
<td>9</td>
<td>Run the NetScreen-Security Manager 2004 FP3 management system installer and upgrade the system to NetScreen-Security Manager 2004 FP3. (10 minutes)</td>
</tr>
<tr>
<td>10</td>
<td>Run the NetScreen-Security Manager 2004 FP3 UI installer and upgrade the UI to NetScreen-Security Manager 2004 FP3. (5 minutes)</td>
</tr>
</tbody>
</table>

Installing NetScreen-Security Manager Using Both Existing and New Hardware

If you are installing the GUI Server and Device Server on separate servers, and you wish to use both your existing hardware and new hardware, install the GUI Server on your existing NetScreen-Global PRO Express appliance and the Device Server on new hardware.
The following table details the migration and installation process if you plan to install the GUI Server on your existing NetScreen-Global PRO Express appliance and the Device Server using new hardware. It also provides an estimate of the overall amount of time each step requires.

**Table 10: Installation Process for Installing NSM Using Existing and New Hardware**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Copy the required software to install the NetScreen-Security Manager 2004 FP2 management system (for Solaris) on your existing NetScreen-Global PRO Express appliance. Copy the required software for the user interface to the Windows-based PC where you plan to install the UI. (10 minutes)</td>
</tr>
</tbody>
</table>
| 2    | Run the management system installer (for Solaris) on your existing NetScreen-Global PRO Express appliance to install the GUI Server. The installer automatically detects if you have NetScreen-Global PRO Express installed on the appliance. It then installs and runs the NetScreen-Global PRO data export utility automatically. The NetScreen-Global PRO data export utility exports your data from NetScreen-Global PRO Express and the managed FW/VPN devices in your network, and then saves the exported data in two files:  
  pmexport.tar for your Policy Manager and device configuration data  
  rmexport.out for your Realtime Monitor data  
  (2-8 hours) |
| 3    | Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server. (10 minutes) |
| 4    | Run the management system installer (for Linux or Solaris) on a new server to install the Device Server. (10 minutes) |
| 5    | Install the NetScreen-Security Manager 2004 FP2 User Interface. (10 minutes) |
| 6    | Start the UI and connect it to the management system. (10 minutes) |
| 7    | Import your configuration data into NetScreen-Security Manager. Validate the migration. (Optional) (2-4 hours (avg) - based on size of Express database) |
| 8    | Perform any necessary post-migration steps. Remove your previous Juniper Networks management software version. (Optional) (30 minutes) |
| 9    | Run the NetScreen-Security Manager 2004 FP3 management system installer and upgrade the system to NetScreen-Security Manager 2004 FP3. (10 minutes) |
| 10   | Run the NetScreen-Security Manager 2004 FP3 UI installer and upgrade the UI to NetScreen-Security Manager 2004 FP3. (5 minutes) |

**Migration Scenarios Not Supported**

NetScreen-Security Manager does not support the installation and migration over existing Juniper Networks NetScreen-IDP devices.

**Migration Path**

To migrate data from your previous version of NetScreen-Global PRO Express, you must be running at least version 4.1.3. Customers running a previous version of NetScreen-Global PRO Express must upgrade to version 4.1.3 before migrating to NetScreen-Security Manager.
**Supported Devices**

The NetScreen-Global PRO data export utility does not support the migration of devices running a version of ScreenOS not supported by NetScreen-Security Manager. If you have devices in NetScreen-Global PRO Express that are not supported by NetScreen-Security Manager, you need to delete these devices from NetScreen-Global PRO Express before beginning the export process. Refer to *Appendix A, Technical Overview* for a description of all the FW/VPN devices and versions of ScreenOS supported by NetScreen-Security Manager.

If the NetScreen-Global PRO data export utility detects a FW/VPN device configured in NetScreen-Global PRO Express, that is running a non-supported version of ScreenOS (ScreenOS 3.0.3), it reports the error and continues to export the next FW/VPN device.
Pre-Migration Steps

Before you begin the process of installing NetScreen-Security Manager, you need to perform several manual steps to ensure that your data in NetScreen-Global PRO Express is current.

To ensure that your devices are properly migrated, it is recommended that you:

- Perform an **AutoDetect** operation for all managed devices to verify they are all connected and online. This also verifies the Serial number and ScreenOS version information on the device.

- Perform a **Delta Configuration Summary** for all managed devices to verify that there are no discrepancies between the configuration information in Express and on the device.

- Verify that all virtual systems are connected during the export process.

- Verify all information for all "modeled" devices. These are devices that you may have configured in NetScreen-Global PRO Express, but are not currently managing. During the migration, configuration information for your "modeled" devices is derived from a Configuration Summary. Because this information is not validated, you may consider deleting these devices from NetScreen-Global PRO Express before you begin the migration process.

- Verify that there are no instances of cyclic containment in user, address and service objects in Policy Manager. Cyclic containment exists when objects are configured as members of themselves. For example, if you have three service objects, one named Service A, another named Service B, and another named Service C. If you have a scenario where Service A contains Service B, and Service B contains C, and C contains A, the migration fails.
Defining System Parameters

During the installation process, you are required to configure common system parameters such as the location of the directories where you want to store data for the GUI Server and Device Server. It is recommended that you define these system parameters before performing the management system installation. There are four main types of configuration parameters that you may need to define depending on your specific deployment of the management system:

- Typical Configuration Parameters on page 33
- Extended Configuration Parameters on page 34
- HA Configuration Parameters on page 35
- Shared Disk Parameters on page 35

**Typical Configuration Parameters**

The following table describes the system parameters that you need to identify to install the Device Server and GUI Server on the same server machine:

**Table 11: Typical HA Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>Directory location on the Device Server where device data is stored. Because the data on the Device Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process. By default, the Device Server stores data in: /var/netscreen/DevSvr/</td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location on the GUI Server where user data is stored. Because the data on the GUI Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/</td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
</tr>
<tr>
<td>Initial “super” user password</td>
<td>This is the password required to authenticate the initial user in the system. By default, the initial super user account receives all administrative privileges in the system.</td>
</tr>
</tbody>
</table>
Defining System Parameters

Extended Configuration Parameters

The following table describes additional system parameters that you need to identify to install HA with the Device Server and GUI Server on separate server machines:

Table 12: Extended HA Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server ID</td>
<td>Unique ID assigned when you add the Device Server.</td>
<td></td>
</tr>
<tr>
<td>Password for GUI Server Connection</td>
<td>Password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local database backup directory</td>
<td>Directory location where local database backup data is stored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server stores local database backup data at:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/netscreen/dbbackup/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default path is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/usr/bin/rsync</td>
<td></td>
</tr>
<tr>
<td>Path to the ssh utility executable</td>
<td>Path to the ssh utility executable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default path is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/usr/bin/ssh</td>
<td></td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the installer sets this to the IP address of the secondary HA Server.</td>
<td></td>
</tr>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>Time of day that you want the GUI Server to backup the database. Type a 2 digit number representing the time of day in a 24 hour day (00-23). For example, if you want the backup to begin at 4:00 A.M., type 04; if at 4:00 P.M., type 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI Server completes the daily backup process within the hour specified every day. By default, the GUI Server performs the daily backup within an hour after 2am.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>Total number of database backup files that the GUI Server stores. When the GUI Server reaches the maximum number of backup files you configure, it overwrites the oldest file. By default, the GUI Server stores seven backup files.</td>
<td></td>
</tr>
</tbody>
</table>
HA Configuration Parameters

The following table describes the system parameters that you need to identify to install HA with the Device Server and GUI Server on the same server machine:

**Table 13: Typical HA Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary HA Server IP address</td>
<td>IP address of the primary server participating in the HA cluster.</td>
</tr>
<tr>
<td>Secondary HA Server IP address</td>
<td>IP address of the secondary server participating in the HA cluster.</td>
</tr>
<tr>
<td>HA replications</td>
<td>Time interval with which you want the GUI Server to replicate the database. By default, the GUI Server replicates the database every 60 minutes.</td>
</tr>
<tr>
<td>Heartbeat links between primary and secondary machine</td>
<td>Number of heartbeat communication paths between the primary and secondary machine. By default, there is 1 communication link between the primary and secondary machine. This in addition to the data network link already existing in the primary/secondary HA Server IP Address.</td>
</tr>
<tr>
<td>Shared password for heartbeat authentication.</td>
<td>This is the password that is required to authenticate heartbeat messages between the primary and secondary HA servers.</td>
</tr>
<tr>
<td>IP Address for Primary machine’s heartbeat link</td>
<td>IP address used for heartbeat communications on the primary server machine.</td>
</tr>
<tr>
<td>Port used for heartbeat communication</td>
<td>The port number used for heartbeat communications. The default port is 7802.</td>
</tr>
<tr>
<td>Heartbeat messages time interval</td>
<td>Time interval (in seconds) between heartbeat messages. The default is 15 seconds.</td>
</tr>
<tr>
<td>Missing heartbeats before switchover occurs</td>
<td>Number of missing heartbeat messages before automatic switchover to the secondary machine occurs. The default is 4 messages.</td>
</tr>
<tr>
<td>IP Address outside the HA cluster</td>
<td>Network IP Address used to monitor this server’s network connection.</td>
</tr>
<tr>
<td>HA directory</td>
<td>Directory location where high availability data is stored. Note that the same directory location is used if you configure this machine to perform local database backups. By default, the HA Server stores data at: /var/netscreen/dbbackup/</td>
</tr>
</tbody>
</table>

Shared Disk Parameters

If you are using a shared disk partition, the installer prompts you to configure additional information. The following table identifies the additional system parameters that you need to identify to install HA with access to a shared disk:
### Table 14: Shared Disk Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to mount the shared disk partition</td>
<td>The command to mount the shared data partition. The default command is: /bin/mount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to unmount the shared disk partition</td>
<td>The command to unmount the shared data partition. Before configuring this command, you must first verify that you have defined your mounts properly. The default command is: /bin/umount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to check the integrity of the shared data partition</td>
<td>The command to check the integrity on the shared data partition. The default command is: /sbin/fsck</td>
<td></td>
</tr>
<tr>
<td>Directory path for the shared disk</td>
<td>Directory path of the shared disk mount point.</td>
<td></td>
</tr>
</tbody>
</table>
**Prerequisite Steps**

Before you install the management system, you need to perform the following prerequisite steps:

1. Ensure that the computer you install the management system on is connected to a serial console or monitor and keyboard.

2. Login to the computer as root.

   If you are already logged in as a user other than root, then type the following command to become root:

   `su -`

   At the password prompt, type the root password for the computer.

**NOTE:** The NetScreen-Security Manager management system runs as the root user. If you want to run the management system in a more secure mode, then refer to Changing Permissions To a Normal User on page 109.

3. Partition drives for sufficient disk space to accommodate your planned data requirements.

4. Run the system update utility for your appropriate platform to verify that you have all the prerequisite utilities and packages to run the installer properly. Refer to Running the System Update Utility on page 38 for more information on running the system update utility.

5. If you are installing the management system on Solaris 9, and are planning to perform local database backups, then you must update the Sun Solaris ssh daemon. Refer to Patching the Sun Solaris SSH Daemon on page 39 for more information.

6. If you are planning to send copies of your database backups to a remote machine, then you must establish a trust relationship between the management system server and the remote machine. Refer to Establishing a Trust Relationship on page 40 for more information.

**Other Recommended Actions**

It is highly recommended that you disable X server on all the server machines that you plan to install NetScreen-Security Manager. Disabling X server frees up additional server resources for enhanced system performance.

To disable X server on Linux:

1. Navigate to the `/etc` subdirectory.

2. Open the `inittab` file in any text editor.

3. Comment out the line that refers to `/etc/X11/prefdm`.

4. Run `init q`
5. Log out of the graphical console and make sure X does not re-appear.

To disable X server on Solaris, run the following commands:

/etc/rc2.d/S99dtlogin stop
mv /etc/rc2.d/S99dtlogin /etc/rc2.d/orig.S99dtlogin

**Running the System Update Utility**

Use the system update utility to upgrade your system with the latest patches and packages required to run the NetScreen-Security Manager management system installer properly.

To run the system update utility:

1. Save the system update utility appropriate for your platform (for example, systemupdate-nsm-linux for Linux, systemupdate-nsm-solaris for Solaris) that is provided on the NetScreen-Security Manager Installation CD or from the directory where it is saved, to a suitable directory on the server.

2. Unzip the appropriate system update utility file to decompress the utility. For example, you would run the following command on Linux:

   `gzip -d systemupdate-nsm-linux.tar.gz`

3. Untar the appropriate system update utility file to run the utility. For example, you would run the following command on Linux:

   `tar xfv systemupdate-nsm-linux.tar`

   A subdirectory called `/systemupdate-nsm-<platform>` is created and all of the files required to update your system packages and utilities are extracted into that directory.

4. Navigate to the `/systemupdate-nsm-<platform>` subdirectory.

5. Run the update shell archive script. For example, you can execute the shell archive script by running the following command:

   `./update.sh`

---

**NOTE:** It is recommended that you save the utility in the `/usr` subdirectory.
The script proceeds to check your system for required updates. It next prompts you to type <Enter> to continue or Ctrl-C to stop.

6. Press <Enter> to continue. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 20 minutes. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 10 minutes depending upon the number of packages that need to be installed.

**Patching the Sun Solaris SSH Daemon**

If you are running NetScreen-Security Manager 2004 FP2 on a Solaris 9 system, and you want to perform a database backup, replicate the database remotely, or enable high availability functionality, you must patch the Sun Solaris SSH daemon on both servers. This is because of a known issue in the Sun Solaris SSH daemon that may result in a failure to replicate.

To patch the Sun Solaris SSH daemon on Solaris 9:

1. Login to the server machine that you are running NetScreen-Security Manager as root. You must also be in single user mode.

2. Use a web browser to download the Sun Solaris patch 113273-07 from the following URL:

```<http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=113273&rev=01>`
3. Extract the packages. For example, run the following commands:

   ```
   unzip /tmp/113273-07.zip
   ```

4. Install the packages. Make sure that you are in the directory where you downloaded the packages. The following example installs the patch to a standalone system:

   ```
   patchadd /tmp/113273-07
   ```

   Checking installed patches...
   Verifying sufficient filesystem capacity (dry run method)...
   Installing patch packages...

   Patch number 113273-07 has been successfully installed.
   See /var/sadm/patch/113273-07/log for details

   Patch packages installed:
   SUNWsshdu

5. Verify that the patch has been installed. For example, run the following command:

   ```
   showrev -p | grep 113273-07
   ```

   Patch: 113273-07 Obsoletes: Requires: Incompatibles: Packages: SUNWsshdu

6. Restart the server machine.

**Establishing a Trust Relationship**

If you are planning to send copies of your database backups to a remote machine, then you must establish a trust relationship between the management system server and the remote machine.

To establish a trust relationship between 2 machines:

1. Run the following commands on the management system server:

   ```
   cd /root
   ssh-keygen -t rsa
   chmod 0700 .ssh
   ```

2. You then need to secure copy .ssh/id_rsa.pub to the remote machine’s .ssh/authorized_keys. For example, you would run the following command:

   ```
   scp .ssh/id_rsa.pub root@<IP addr rem machine>: /root/.ssh/authorized_keys2
   ```

   You should test connectivity via ssh from the management system server to the remote machine and vice versa. For example, to test ssh connectivity, type the following command:

   ```
   ssh root@<IP ADDRESS of remote machine>
   ```

   Validate that you do not receive a prompt to enter a password to access the remote machine.
Installing the Management System Software

In most typical cases, you install both the GUI Server and Device Server on the same server. The management system installer is designed to guide you through all of the steps to configure the required system parameters, and then run it to completion.

To install the management system on the same system:

1. Load the NetScreen-Security Manager 2004 FP2 management system installer software onto the server that you have decided to use as the NetScreen-Security Manager management system. You can run the installer directly from the NetScreen-Security Manager installation CD, copy the installer to a directory on the server, or download the installer from the Juniper Networks Customer Services Online web site.

2. Navigate to the directory where you saved the management system installer file. It is recommended that you save the management system installer in the /tmp subdirectory.

3. Run the management system installer.

   On Linux, run the following command:

   ```sh
   sh nsm04fp2_servers_linux_x86.sh
   ```

   On Solaris, run the following command:

   ```sh
   sh nsm04fp2_servers_sol_sparc.sh
   ```

   The installation begins automatically by performing a series of pre-installation checks. The installer ensures that:

   - You are installing the correct software for your operating system.
   - All of the needed software binaries are present.
   - You have correctly logged in as root.
   - The system has sufficient disk space and RAM.

   The installer then stops any running servers.

   **NOTE:** The management system installer indicates the results of its specific tasks and checks:

   - "Done" indicates that the installer successfully performed a task.
   - "ok" indicates that the installer performed a check and verified that the condition was satisfied.
   - "FAILED" indicates that the installer performed a task or check, but it was unsuccessful.
The installer then prompts you to specify the components of the NetScreen-Security Manager management system that you want to install.

4. Type 3, then press <Enter> to specify that you want to install the Device Server and GUI Server.

The following graphic depicts the installer running on Linux. The installer running on Solaris displays similar prompts and messages.

![Installer Graphic]

The script then prompts if this machine will participate in an HA cluster.

5. Type n, and then press <Enter> if you do not want the machine to participate in an HA cluster. If you are planning on configuring the management system with HA enabled, refer to the NetScreen-Security Manager 2004 FP3 Installer’s Guide for more information.

The script then prompts you to specify a location to store the management system data files.

6. Set the directory location for storing the management system data files:

   a. Type the directory location for storing the Device Server data files or press Enter to accept the default location /var/netscreen/DevSvr.

   **NOTE:** If you specify a new directory location, then the installer creates it. The installer does not however, allow you to specify an existing directory location. This feature safeguards against over-writing any existing data. If you try to specify an existing directory, the installer indicates that an existing directory already exists, and then prompts you to try again.

   The script then prompts you to specify a location for storing the GUI Server data files.
b. Type the directory location for storing the GUI Server data files or press <Enter> to accept the default location /var/netscreen/GuiSvr.

The script next prompts you to specify the management IP address for the server.

7. Type the management IP address for the server. This address should be the same IP address as the server that you are installing on. The installer sets the IP address and port number on the GUI Server enabling the Device Server to connect. The Device Server attempts to connect to the GUI Server using port 7800 by default.

The script then prompts you to type a password for the “super” user account. The initial administrator or “super” user account is the account that you use when you first login to NetScreen-Security Manager using the NetScreen-Security Manager User Interface (UI). This account is used to authenticate communication between the management system and the NetScreen-Security Manager UI. It possesses all administrative privileges by default.

8. Type any text string longer than 8 characters for the password. Type the password again for verification.

NOTE: Make a note of the password that you have set for the super user account. You need this when you first login to the UI.

The script then prompts you if you want to use a Statistical Report Server with the GUI Server.
9. Type \texttt{n} and then press <Enter>, if you are \textbf{not} planning on installing NetScreen-Statistical Report Server with NetScreen-Security Manager. Type \texttt{y} and then press <Enter> if you are installing NetScreen-Statistical Report Server with NetScreen-Security Manager. If you typed \texttt{y}, the script then prompts you to configure parameters required for the management system to work with the Statistical Report Server (i.e., database type, database server IP address, database port, database name, database user name, database password). Refer to the \textit{NetScreen-Statistical Report Server Installer's Guide} for more information about these parameters.

The script next prompts if you want this machine to perform a backup of the database locally.

10. Type \texttt{y} and then press <Enter> if you want the management system to perform a local backup of the database on a daily basis. If you specify that you want the management system to perform automatic backups, the script prompts you to configure options for the backup operation:

   a. Type a \textbf{two-digit number} (00-23) specifying the hour of day that you want the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, type 12; for midnight, type 00. Press <Enter> to accept the default setting of 02 (2:00 A.M.).

   b. Type \texttt{n}, and then press <Enter> so daily backups are not sent to a remote machine. If you select \texttt{y}, and then press <Enter>, then the script prompts you to enter an IP address for the remote backup machine.

   c. Type a number (up to seven) specifying how many database backup files the management system stores. After the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press <Enter> to accept the default setting of seven backup files. By default, the management system stores backup files in: 

   \texttt{/var/netscreen/dbbackup}

   d. Type the full path to the ssh utility executable.
Type n, and then press <Enter>, if you do not want the management system to backup the database locally.

The script then prompts you to start servers after installation is complete.

Type y, and then press <Enter>, if you want to start the GUI and Device Servers after the installation has finished. Type n, and then press <Enter>, if you do not want to start the servers.

The script then prompts you to verify your installation configuration settings.
12. Verify your settings, and if they are correct, type y, and then press <Enter> to proceed. If you type n, and press <Enter>, then the installer returns you to the original selection prompt.

The installer performs the following actions:

- Extracts the software payloads
- Performs any applicable migration tasks (disregard since this is a new installation)
- Installs the Device Server
- Installs the GUI Server
- Installs the HA Server
Performing post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server.

Several messages display to confirm the installation progress.
The installer runs for several minutes, and then returns you to the command prompt.

**Viewing the Management System Installation Log**

The installer generates a log file with the output of the installation commands for troubleshooting purposes. The naming convention used for the installation log file is:

```
netmgtInstallLog.<current date><current time>
```

For example, if you ran the installer on December 1, 2004 at 6:00 P.M., the installation log file would be named:

```
netmgtInstallLog.20041201180000
```

--- SETTING START SCRIPTS ---

Enabling Device Server start script.........................ok
Enabling GUI Server start script...........................ok
Enabling HA Server start script...........................ok

DESTROYING POST-INSTALLATION TASKS

Running mmtCertGeneration.................................ok
Removing staging directory...............................ok
Starting GUI Server........................................ok
Starting Device Server......................................ok
Starting HA Server..........................................ok

**NOTES:**

- Installation log is stored in /usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20040812165849
- This is the GUI Server fingerprint:
  You will need this for verification purposes when logging into the GUI Server. Please make a note of it.

---

**NOTE:** After the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.

**Starting Server Processes Manually**

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory (/usr/netscreen/HaSvr/bin).
2. Run the following command:
Installing the Management System Software

```sh
./haSvr.sh start
```

**Validating Management System Status**

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes.

To validate the management system is started and running properly, it is recommended that you view the status of all the running server processes (the HA server, Device Server and GUI Server) to confirm that all services are up and running.

Refer to Controlling the Management System on page 104 for more information on manual commands that you can send to the HA Server, Device Server and GUI Server.

**NOTE:** If you start the HA Server process, then it automatically starts the GUI Server and Device Server processes.
Exporting Data From NetScreen-Global PRO Express

If you are installing the management system over existing hardware (for example, if you are installing the management system using your existing NetScreen-Global PRO Express appliance), the management system installer detects if you are running NetScreen-Global PRO Express, and installs and runs the NetScreen-Global PRO data export utility automatically.

If you are installing the management system using new hardware, you must install and run the NetScreen-Global PRO data export utility \( \text{nsm04fp2_gpexport_sol_sparc.sh} \) separately on the NetScreen-Global PRO Express appliance.

For more information on the data export process, refer to Chapter 1, Introduction.

Transferring the Export Data Files

Once you have completed the export process, you must transfer these data files to the following subdirectory on the server on which you are installing the NetScreen-Security Manager GUI Server:

\[ \text{/usr/netscreen/GuiSvr/var/migration/} \]

You need to give the user "nsm" permission to the file. You can do so by running the following command:

\[ \text{chmod -R 777 /usr/netscreen/GuiSvr/var/migration/} \]

You can then install the User Interface and import the data into NetScreen-Security Manager.
Installing the User Interface

The NetScreen-Security Manager 2004 FP2 User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based computer that meets minimum system requirements. Refer to Chapter 1, Introduction for more information on the minimum system requirements for the UI.

The InstallAnywhere wizard guides you through all the steps required to configure and install the NetScreen-Security Manager UI. Once you install the UI, you can connect it to the management system.

NOTE: It is recommended that you quit all running applications before installing the UI.

To install the NetScreen-Security Manager 2004 FP2 UI:

1. Login as an Administrator user on the computer where you are installing the UI.

   NOTE: For instructions on adding users to the Administrator group, please refer to your operating system manual.

2. Download the UI installer from the NetScreen-Security Manager installation CD or the Juniper Networks corporate web site to the computer where you are installing the UI.

3. Run the UI installer.

   If you are installing the UI on a Windows-based PC, you can double-click on the installer executable.

   If you are installing the UI on a Linux-based computer, you can launch it from a command line. From the command line, you can launch the UI installer using the following command:

   `sh nsm04fp2_ui_linux_x86.bin`

   Initially, the following messages appear in the Linux terminal.

   An Introduction screen for the InstallAnywhere wizard appears.
Follow the wizard through all the steps required to configure and install the UI. Click **Next** to continue the installation. The License Agreement screen appears.

4. Review the License Agreement carefully. If you choose to accept the terms of the License Agreement, click the button next to the appropriate statement. Click **Next** to continue.

**NOTE:** If you choose to not accept the terms of the License Agreement, you will not be able to proceed with the installation.

If you accepted the License Agreement, the Choose Install Folder screen appears.
5. To accept the default install folder, click **Next**.

**NOTE:** If you are installing on a Windows-based computer, the installer saves the UI software files in `C:\Program Files\NetScreen-Security Manager` by default. If you are installing on a Linux-based computer, the installer saves the UI software files in `/root/NetScreen-Security Manager` by default.

To specify a new or different folder location, click **Choose...**. If you decide to accept the default install folder, then click **Restore Default Folder**.

On Windows-based computers, the Choose Shortcut Folder screen appears.

6. Select where you would like to create the NetScreen-Security Manager product icons. Or, if you are installing on a Linux-based computer, then select where you would like to create links to the NetScreen-Security Manager UI program. Click **Next** to continue. The Pre-Installation Summary screen appears.

On Linux-based computers, the Choose Link Folder screen appears.

7. Verify that the information is correct. To make a change to any of the previous configuration options, click **Previous**. When you are satisfied that the information is correct for this installation, click **Install**. The installer proceeds to install the software files for the UI.

8. If you do not have a default web browser configured, the Select Browser screen appears. Use the **Choose** button to navigate to the subdirectory where your web browser software files are located. Click **Next** to continue.
When the installation is complete, a screen indicating “Install Complete” appears.

**NOTE:** If you do not select a default web browser, the UI will not be able to launch the NetScreen-Security Manager online help. If you still wish to use the online help, you can configure your web browser using the Preferences menu from the UI.

9. Click **Done** to exit the installation program.

**Viewing the User Interface Installation Log**

The installer generates a log file with information describing the context of the installation process. For troubleshooting purposes, you may need to access it. The installation log is saved by default in the following directory locations:

For Windows-based computers:

C:\Documents and Settings\<user name>\.nsm\

For Linux-based computers:

/root/.nsm/

**NOTE:** The .nsm subdirectory is a hidden subdirectory on Linux systems.

The Installation log file is named:

_out.<date/time stamp>.dat

**Running the User Interface**

Once you have completed installing the UI, you can launch the application and verify that you can connect to the management system.

The first time you open the UI, you need to specify the host name (or IP address) of the management system that you want to connect to, a user name, and password. The default user name for new installations is “super”; the default password is the password you specified when configuring the management system. Passwords and user names are case-sensitive.

To log in to the UI for the first time:

1. Run the NetScreen-Security Manager UI.

   If you are running the UI on a Windows-based PC, you can double-click on the NetScreen-Security Manager icon.
Installing the User Interface

If you are running the UI on a Linux-based computer, you can either launch it by double-clicking on the NetScreen-Security Manager application icon (specify that you want to run the program) or you can launch it from a command line. From the command line, navigate to the subdirectory where you have installed the UI software files, and then run the UI application shell archive script. The Login window appears.

2. Verify that the user name in the **Login** field provided is the initial admin user called “super”. If not, type “super” in the Login field.

3. Type the password that you specified when you installed the management system in the **Password** field provided.

4. Type the IP address you assigned to the GUI Server in the **Server** field provided. If you have enabled DNS-lookup, you can type the host name instead of the IP address.

5. Click **OK**.

The UI appears indicating that the installation was successful.

**Validating the Installation**

Once you have installed the management system and UI, it is recommended that you validate basic information configured on the Device Server. You can use the Server Manager to view and edit your configuration on the management system.

To validate your configuration on the Device Server:

1. From the NetScreen-Security Manager UI, double-click the **Server Manager** module. The Server Manager module expands, and the Servers and Server Monitor appears.

2. Select the **Servers** node. The Servers view displays Device Server and GUI Server information.

3. Select the Device Server and click **Edit** or right-click the Device Server and select **Edit** to view all information available on the Device Server.
4. Use the **General** tab to verify the following information:

   - **Device Server Manager Port** - the default port is 7800.
   - **Device Server ID** - the ID number identifies the Device Server; you cannot change the Device Server ID.
   - **Mapped IP Address** - the IP address that is manually defined in the UI.

```
NOTE: You can configure the Device Server to use a Mapped IP (MIP) address. A MIP maps the destination IP address in an IP packet header to another static IP address, enabling the FW/VPN device to receive incoming traffic at one IP address, and automatically forward that traffic to the mapped IP address. MIPs enable inbound traffic to reach private addresses in a zone that contains NAT mode interfaces.
```

   - **Mapped Port** - the port number of the device.

5. Click OK when you are done.

**Running the UI in Demo Mode**

Before you begin using NetScreen-Security Manager to configure and manage your network, it is recommended that you first run the UI in Demo mode. Demo mode is an option in the UI enabling you to run the UI disconnected from the management system.

To run the UI in Demo mode:

1. Run the NetScreen-Security Manager UI. The Login window appears.

2. Type any user name in the **Login** field provided.

3. Type any password in the **Password** field provided.

4. Select *DEMO MODE* from the **Server** field pull-down menu.

5. Click OK. The Log Viewer main window appears.
Importing Data Into NetScreen-Security Manager

Once you have completed installing the User Interface, you can launch the UI and import configuration data previously exported from NetScreen-Global PRO Express into NetScreen-Security Manager.

Import Process

You can run the import process multiple times without corrupting the NetScreen-Security Manager database. The import of Policy Manager and Realtime Monitor data can be done at the same time or separately.

If you are planning on importing data from both Policy Manager and Realtime Monitor, it is highly recommended that you perform the import of data from Policy Manager before or at the same time as you import your data from Realtime Monitor. This is because you want to establish your configuration data in NetScreen-Security Manager in the domains that applied in Policy Manager. This configuration data is inherent in Policy Manager. Data configured in Realtime Monitor is not domain-specific.

If you are importing domains individually into NetScreen-Security Manager, it is also highly recommended that you backup your previous installation of NetScreen-Security Manager before running the import. This is to ensure that you can reverse the migration process in the event of an error.

Resolving Domain Name Conflicts

The import identifies all name conflicts before performing the import operation allowing you to determine how to resolve them. Once you have done this, the rest of the migration process can be executed automatically.

During the import, if a domain name already exists in NetScreen-Security Manager (from a previous domain import), the import utility does not merge the two domains with the same name. The import utility prompts the user to resolve the name conflict. You can resolve the domain name conflict by choosing one of the following options:

- Rename the Policy Manager domain
- Rename the existing domain in the NetScreen-Security Manager database
- Overwrite the existing domain with the Policy Manager domain
- Do not import the Policy Manager domain

The import resolves conflicts by not importing the new domain by default. Note that the import utility does not try to merge two domains with the same name.

Because there is no concept of domains in Realtime Monitor, users and user groups are imported to the global domain only. Access privileges associated with your Realtime Monitor users and user groups are not imported. After the migration is completed, you have to create new admin roles for these users and user groups.
**Importing Migration Data**

Before importing data from NetScreen-Global PRO Express, you must ensure that no other Admins are logged into the system. Any changes made to NetScreen-Security Manager system during the migration process will result in database corruption.

To import data from NetScreen-Global PRO Express:

1. From the **Tools** menu, select **Import Global PRO**. A window appears prompting you to specify the type of data (Policy Manager, Realtime Monitor data) that you wish to import and the directory locations where you saved the import files.

2. Click in the appropriate checkbox to select the type of data that you wish to import. Click **Next** to continue. The import process begins automatically.

3. Occasionally, name conflicts occur when an import object has the same name as an existing object. If the import tool experiences a name conflict, a window appears prompting you to resolve the name conflict.

   Click in the radio button provided to specify how you want to resolve any name conflicts. Click **Next** to continue. The Admin Role Options window appears next.

4. During the import of administrators from Policy Manager, the administrative permissions for administrators do not map entirely into NetScreen-Security Manager. You need to select whether to give your administrators more access rights or less access rights in NetScreen-Security Manager.

   **NOTE:** If you choose "less access rights", the administrators that you migrate from NetScreen-Global PRO may not have sufficient permissions to perform all the tasks in NetScreen-Security Manager that they were previously allowed to perform.

5. Click **Next** to continue. A window appears indicating the status of the import process.
If the UI performs the import process successfully, no errors are indicated.

**NOTE:** If you receive a warning message indicating that the IP Address of your current server is invalid for Global-Pro primary server (i.e., “Currently, only Device Server IP is allowed. server_1 will be used instead. 10.5.94.3 is invalid for Global-Pro primary server. Currently, only Device Server IP is allowed. server_1 will be used instead.”), you can safely disregard it. This message serves as a reminder that Global-Pro is no longer in service, and that the NetScreen-Security Manager Device Server is replacing Global-Pro as the management system. This warning message appears if you have not previously deleted your Global-Pro settings.

If the UI encounters error(s) during the import process, it indicates the error count in the Error and Fatal Error fields provided. Click **Cancel** and the UI rolls back all changes and restores the NetScreen-Security Manager database to its pre-migration state.

6. Click **Finish** to exit the import dialog.

**Rolling Back a Failed Migration**

If you are migrating additional domain information after initially performing an import, and you encounter an error, you need to restore the previous NetScreen-Security Manager database from backup.

**Validating a Successful Migration**

To validate that the migration process completed successfully, you need to perform a delta configuration summary on all devices in the network, and verify that there are no deltas.
Post Migration Steps

Once you are satisfied that all your data has successfully migrated from NetScreen-Global PRO Express into NetScreen-Security Manager, it is recommended that you perform the following manual post-migration steps:

Manually Configuring Protected Resources

If you wish to configure the server/client parameter in the NetScreen-Security Manager Protected Resource as uni-directional, you need to manually reconfigure this after the migration.

Manually Configuring Authentication Servers

If you do not want an authentication server to be used for a specific purpose in NetScreen-Security Manager, you need to manually disable these purposes (FWauth, Xauth, L2TP, or Policy Manager Auth) after the migration.

Manually Configuring VPNs

If you implemented Hub and Spoke VPNs in Policy Manager, it was possible to control the granularity of your VPN tunnels by defining each tunnel endpoint as a main or branch. In NetScreen-Security Manager, VPN tunnel endpoints are device-specific. Because of this, “branch” VPN tunnels in NetScreen-Security Manager may have greater access to other branch VPN endpoints than they did in Policy Manager. If this occurs, you need to manually configure a firewall policy to deny this traffic.

Transferring Certificate Files

If you plan to continue managing FW/VPN devices running ScreenOS 4.0.X using NACN, you must transfer and load the private key and certificate file packed in PKCS12 into your security database.

To transfer certificate files:

1. On the server where you have installed the Device Server, navigate to the /usr/Netscreen/DevSvr/utils subdirectory.

2. Run the nacnLoadPKCS12 utility. The script prompts you to type the full path location to the PKCS12 file.

3. Type the path to the PKCS12 file. The script next prompts you to type the PKCS12 password.

4. Type the password. The script next prompts you whether or not you want to set the migration flag on the file.

5. Type y to set the migration flag, and then press Enter to continue. The script runs to completion.
Upgrading to NetScreen-Security Manager 2004 FP3

After you have completed installing NetScreen-Security Manager 2004 FP2, and successfully migrated your previous management data to it, you can then proceed to upgrade to NetScreen-Security Manager 2004 FP3.

Next Steps

Congratulations! You have just completed migration and installation of the NetScreen-Security Manager management system and User Interface. You can now begin to manage your network using NetScreen-Security Manager. Refer to the NetScreen-Security Manager 2004 FP3 Administrator’s Guide or Online Help for information describing how to plan and implement NetScreen-Security Manager for your network.
Chapter 3

Migrating From Global PRO

In This Chapter:

- Migration and Installation Scenarios
- Pre-Migration Steps
- Defining System Parameters
- Prerequisite Steps
- Installing the Management System Software
- Exporting Data From NetScreen-Global PRO
- Importing Data Into NetScreen-Security Manager
- Post Migration Processes
- Upgrading to NetScreen-Security Manager 2004 FP3
- Next Steps

This chapter describes the NetScreen-Security Manager migration and installation process for those who have previously used Juniper Networks NetScreen-Global PRO. It describes scenarios and procedures for migrating your configuration data from NetScreen-Global PRO and installing NetScreen-Security Manager using new or existing hardware. It also describes how features in NetScreen-Global PRO map to NetScreen-Security Manager, and other considerations to ensure that you have installed NetScreen-Security Manager and migrated data from NetScreen-Global PRO successfully.
Migration and Installation Scenarios

There are multiple options for installing NetScreen-Security Manager if you are currently using NetScreen-Global PRO:

- Installing Management System Using New Hardware on page 64
- Installing Management System Using Existing Hardware on page 65
- Considerations If You Are Running Multiple Arbitrators on page 66
- Considerations If You Are Running Multiple Data Collectors on page 68
- Maintaining Historical Reporting Functionality on page 68

Installing Management System Using New Hardware

It is possible to extend system performance by installing NetScreen-Security Manager onto new hardware that exceeds the prescribed minimum system requirements.

The following table details the migration and installation process if you are using new hardware. It also provides an estimate of the overall amount of time each step requires.

Table 15: Installation Process for Installing NSM Using New Hardware

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
</table>
| 1    | Copy the NetScreen-Security Manager 2004 FP2 management system installer to the server(s) where you plan to install the NetScreen-Security Manager GUI Server and Device Server. (5 minutes)  
  | Copy the NetScreen-Security Manager 2004 FP2 User Interface installer to the computer where you plan to install the UI. (5 minutes)  
  | Copy the NetScreen-Global PRO data export utility installer onto your existing Policy Manager arbitrator and onto the server where you are currently running your Report Manager Master Controller. (5 minutes) |
| 2    | Install the NetScreen-Security Manager management system. (10 minutes) |
| 3    | Run the NetScreen-Global PRO data export utility installer (nsm04fp2_gexport Sol_sparc.sh) on your existing Policy Manager arbitrator. Run the NetScreen-Global PRO data export utility to export your configuration data.  
  | Run the NetScreen-Global PRO data export utility installer on your existing Report Manager Master Controller. Run the NetScreen-Global PRO data export utility to export your configuration data. (2-8 hours)  
  | The NetScreen-Global PRO data export utility exports your data from NetScreen-Global PRO and the managed FW/VPN devices in your network, and then saves the exported data in two files:  
  | pmexport.tar for your Policy Manager and device configuration data  
  | rmexport.out for your Realtime Monitor data |
| 4    | Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server. (10 minutes) |
| 5    | Install the NetScreen-Security Manager 2004 FP2 User Interface. (5 minutes) |
| 6    | Start the UI and connect it to the management system. (5 minutes) |
Installing Management System Using Existing Hardware

If you wish to use your existing hardware, you can install the NetScreen-Security Manager management system over your existing NetScreen-Global PRO hardware infrastructure. It is recommended that you:

1. Install the NetScreen-Security Manager management system over your existing Policy Manager arbitrator.

2. Install the NetScreen-Security Manager User Interface over your existing Global PRO admin console.

If you plan to install the NetScreen-Security Manager management system on separate servers:

1. Install the NetScreen-Security Manager GUI Server over your existing NetScreen-Global PRO arbitrator.

2. Install the NetScreen-Security Manager Device Server over any one of your other existing NetScreen-Global PRO servers (master controller, data collector).

3. Install the NetScreen-Security Manager User Interface over your existing NetScreen-Global PRO admin console.

The following table details the migration and installation process if you are using existing hardware. It also provides an estimate of the overall amount of time each step requires.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Import your configuration data into NetScreen-Security Manager. Validate the migration. (Optional) (2-4 hours based on the size of your database)</td>
</tr>
<tr>
<td>8</td>
<td>Perform any necessary post-migration steps. Remove your previous Juniper Networks management software version. (Optional) (30 minutes)</td>
</tr>
<tr>
<td>9</td>
<td>Run the NetScreen-Security Manager 2004 FP3 management system installer and upgrade the system to NetScreen-Security Manager 2004 FP3. (10 minutes)</td>
</tr>
<tr>
<td>10</td>
<td>Run the NetScreen-Security Manager 2004 FP3 UI installer and upgrade the UI to NetScreen-Security Manager 2004 FP3. (5 minutes)</td>
</tr>
</tbody>
</table>
Table 16: Installation Process for Installing NSM Using New Hardware

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
</table>
| 1    | Copy the NetScreen-Security Manager 2004 FP2 management system installer (for Solaris) and the NetScreen-Global PRO data export utility installer to your existing NetScreen-Global PRO arbitrator. (10 minutes)  
Copy the Global PRO data export utility installer (nsm04fp2_gpexport_sol_sparc.sh) also to the server where you are currently running your Report Manager Master Controller. (10 minutes)  
Copy the required software for the user interface to the computer where you are currently running the NetScreen-Global PRO admin console. (10 minutes) |
| 2    | Run the NetScreen-Security Manager 2004 FP2 management system installer on your existing NetScreen-Global PRO arbitrator to install the management system.  
After performing the server install, the installer automatically detects if you are running NetScreen-Global PRO on the arbitrator. If so, it then installs and runs the NetScreen-Global PRO data export utility automatically. The NetScreen-Global PRO data export utility installer exports data configured in Policy Manager and saves your exported data in a file called pmexport.tar. (2-8 hours)  
* If you are installing the GUI Server and Device Server on separate servers, run the management system installer to install the GUI Server only. You also need to run the management system installer on another server of your choice to install the Device Server. |
| 3    | Install the NetScreen-Global PRO data export utility on the server where you are currently running your Report Manager Master Controller. Run the NetScreen-Global PRO data export utility. The NetScreen-Global PRO data export utility exports data configured in Report Manager and saves your exported data in a file called rmexport.out. (2-8 hours) |
| 4    | Transfer both data files to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server. (10 minutes) |
| 5    | Install the NetScreen-Security Manager 2004 FP2 User Interface. (5 minutes) |
| 6    | Start the UI and connect it to the management system. (5 minutes) |
| 7    | Import your configuration data into NetScreen-Security Manager. Validate the migration. (Optional) (2-4 hours (avg) - based on size of database) |
| 8    | Perform any necessary post-migration steps. Remove your previous Juniper Networks management software version. (Optional) (30 minutes) |
| 9    | Run the NetScreen-Security Manager 2004 FP3 management system installer and upgrade the system to NetScreen-Security Manager 2004 FP3. (10 minutes) |
| 10   | Run the NetScreen-Security Manager 2004 FP3 UI installer and upgrade the UI to NetScreen-Security Manager 2004 FP3. (5 minutes) |

Considerations If You Are Running Multiple Arbitrators

If you are running multiple arbitrators in NetScreen-Global PRO, you can use any one of the servers that they are running on to install the NetScreen-Security Manager GUI Server.

If you wish to migrate configuration data from Policy Manager, you need to install and run the NetScreen-Global PRO data export utility on one arbitrator, move the export data file to the GUI Server migration directory, and then run the import for that specific data file. You need to follow this process for each arbitrator individually.
The following table details the migration and installation process if you are using existing hardware with multiple arbitrators. It also provides an estimate of the overall amount of time each step requires.

**Table 17: Installation Process for Installing NSM Using New Hardware**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
</table>
| 1    | Copy the NetScreen-Security Manager 2004 FP2 management system installer (for Solaris) and the NetScreen-Global PRO data export utility installer to one of your existing NetScreen-Global PRO arbitrators. (10 minutes)  
Copy the NetScreen-Global PRO data export utility installer also to the other servers running your arbitrators, and to the server where you are currently running your Report Manager Master Controller. (10 minutes)  
Copy the required software for the NetScreen-Security Manager 2004 FP2 User Interface to the computer where you are currently running the NetScreen-Global PRO admin console. (10 minutes) |
| 2    | Run the NetScreen-Security Manager 2004 FP2 management system installer on your existing NetScreen-Global PRO arbitrator to install the management system.  
After performing the NetScreen-Security Manager server install, the installer automatically detects if you are running NetScreen-Global PRO on the arbitrator. If so, it then installs and runs the NetScreen-Global PRO data export utility automatically. The NetScreen-Global PRO data export utility installer exports data configured in Policy Manager and saves your exported data in a file called pmexport.tar. (2-8 hours)  
* If you are installing the GUI Server and Device Server on separate servers, run the management system installer to install the GUI Server only. You also need to run the management system installer on another server of your choice to install the Device Server. |
| 3    | Install the NetScreen-Global PRO data export utility on the server where you are currently running your Report Manager Master Controller. Run the NetScreen-Global PRO data export utility. The NetScreen-Global PRO data export utility exports data configured in Report Manager and saves your exported data in a file called rmexport.out. (2-8 hours) |
| 4    | Transfer the rmexport.out file to the /usr/netscreen/GuiSvr/var/migration subdirectory on the server where you have installed the GUI Server. (10 minutes) |
| 5    | Install the NetScreen-Security Manager 2004 FP2 User Interface. (5 minutes) |
| 6    | Start the UI and connect it to the management system. (5 minutes) |
| 7    | Import the configuration data for Policy Manager into NetScreen-Security Manager. (Optional) (2-4 hours (avg) - based on size of database) |
| 8    | Install the Global PRO data export utility on another server where you are currently running an arbitrator. Run the Global PRO data export utility. The Global PRO data export utility exports data configured in Policy Manager for this arbitrator and saves your exported data in a file called pmexport.tar. (4-8 hours (avg) - based on size of database)  
Transfer the pmexport.tar file to the migration directory in the GUI Server data directory. From the UI, run the import process again for Policy Manager using the data from this arbitrator.  
Repeat this process for all your arbitrators. |
| 9    | Import the configuration data for Report Manager into NetScreen-Security Manager. (Optional) (2-4 hours (avg) - based on size of database) |
| 10   | Perform any necessary post-migration steps. Remove your previous Juniper Networks management software version. (Optional) (30 minutes) |
Considerations If You Are Running Multiple Data Collectors

If you have deployed multiple data collectors in Global PRO, then you can use any of the servers that they are running on to install the NetScreen-Security Manager Device Server.

Maintaining Historical Reporting Functionality

NetScreen-Security Manager does not provide historical reporting functionality. If you have previously used historical reports in Report Manager, you can continue to use it with NetScreen-Security Manager.

To continue using historical reports with NetScreen-Security Manager, you need to continue to maintain the historical reports server, database, and Report Manager Admin Console previously implemented for Report Manager.

The recommended installation process is as follows:

1. Install the GUI Server over your existing Global PRO arbitrator.
2. Install the Device Server over any one of your existing data collectors.

You can continue to use the HRS server and database for your historical report data. You will also continue to use the NetScreen-Global PRO Report Manager Admin console to add new devices and admins to the database. You can use any web browser to access historical reports. Refer to the Juniper Networks NetScreen-Global PRO Report Manager 4.0 documentation set for more information on using historical reporting.

Migration Scenarios Not Supported

NetScreen-Security Manager does not support the installation and migration over existing IDP devices nor over existing PRO deployments where devices exist behind a port NAT.

Migration Path

To migrate data from your previous version of NetScreen-Global PRO, you must be running at least version 4.1.3. Customers running a previous version of NetScreen-Global PRO must upgrade to version 4.1.3, before migrating to NetScreen-Security Manager.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/Estimated Time to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Run the NetScreen-Security Manager 2004 FP3 management system installer and upgrade the system to NetScreen-Security Manager 2004 FP3. (10 minutes)</td>
</tr>
<tr>
<td>12</td>
<td>Run the NetScreen-Security Manager 2004 FP3 UI installer and upgrade the UI to NetScreen-Security Manager 2004 FP3. (5 minutes)</td>
</tr>
</tbody>
</table>
**Supported Devices**

The NetScreen-Global PRO data export utility does not support the migration of devices running a version of ScreenOS not supported by NetScreen-Security Manager. If you have devices in NetScreen-Global PRO that are not supported by NetScreen-Security Manager, you need to delete these devices from NetScreen-Global PRO before beginning the export process. Refer to Appendix A, Technical Overview for a description of all the FW/VPN devices and versions of ScreenOS supported by NetScreen-Security Manager.

If the NetScreen-Global PRO data export utility detects a FW/VPN device configured in NetScreen-Global PRO, that is running a non-supported version of ScreenOS (ScreenOS 3.0.3), it reports the error and continues to export the next FW/VPN device.
Pre-Migration Steps

Before you begin the process of installing NetScreen-Security Manager, you need to perform several manual steps to ensure that your data in NetScreen-Global PRO Express is current.

To ensure that your devices are properly migrated, it is recommended that you:

- Perform an **AutoDetect** operation for all managed devices to verify they are all connected and online. This also verifies the Serial number and ScreenOS version information on the device.

- Perform a **Delta Configuration Summary** for all managed devices to verify that there are no discrepancies between the configuration information in Express and on the device.

- Verify that all virtual systems are connected during the export process.

- Verify all information for all "modeled" devices. These are devices that you may have configured in NetScreen-Global PRO Express, but are not currently managing. During the migration, configuration information for your "modeled" devices is derived from a Configuration Summary. Because this information is not validated, you may consider deleting these devices from NetScreen-Global PRO Express before you begin the migration process.

- Verify that there are no instances of cyclic containmentship in user, address and service objects in Policy Manager. Cyclic containmentship exists when objects are configured as members of themselves. For example, if you have three service objects, one named Service A, another named Service B, and another named Service C. If you have a scenario where Service A contains Service B, and Service B contains C, and C contains A, then the migration fails.
Defining System Parameters

During the installation process, you are required to configure common system parameters such as the location of the directories where you want to store data for the GUI Server and Device Server. It is recommended that you define these system parameters before performing the management system installation. There are four main types of configuration parameters that you may need to define depending on your specific deployment of the management system:

- Typical Configuration Parameters on page 71
- Extended Configuration Parameters on page 72
- HA Configuration Parameters on page 73
- Shared Disk Parameters on page 73

Typical Configuration Parameters

The following table describes the system parameters that you need to identify to install the Device Server and GUI Server on the same server machine:

**Table 18: Typical Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>Directory location on the Device Server where device data is stored. Because the data on the Device Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process. By default, the Device Server stores data in: /var/netscreen/DevSvr/</td>
<td></td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location on the GUI Server where user data is stored. Because the data on the GUI Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, then specify the new location during the install process. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/</td>
<td></td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
<td></td>
</tr>
<tr>
<td>Initial “super” user password</td>
<td>This is the password required to authenticate the initial user in the system. By default, the initial super user account receives all administrative privileges in the system.</td>
<td></td>
</tr>
</tbody>
</table>
Extended Configuration Parameters

The following table describes additional system parameters that you need to identify to install HA with the Device Server and GUI Server on separate server machines:

Table 19: Extended HA Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local database backup directory</td>
<td>Directory location where local database backup data is stored. By default, the GUI Server stores local database backup data at: /var/netscreen/dbbackup/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable. The default path is: /usr/bin/rsync</td>
<td></td>
</tr>
<tr>
<td>Path to the ssh utility executable</td>
<td>Path to the ssh utility executable. The default path is: /usr/bin/ssh</td>
<td></td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent. By default, the installer sets this to the IP address of the secondary HA Server.</td>
<td></td>
</tr>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>Time of day that you want the GUI Server to backup the database. Type a 2 digit number representing the time of day in a 24 hour day (00-23). For example, if you want the backup to begin at 4:00 A.M., type 04; if at 4:00 P.M., type 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI Server completes the daily backup process within the hour specified every day. By default, the GUI Server performs the daily backup within an hour after 2am.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>Total number of database backup files that the GUI Server stores. When the GUI Server reaches the maximum number of backup files you configure, it overwrites the oldest file. By default, the GUI Server stores seven backup files.</td>
<td></td>
</tr>
</tbody>
</table>
HA Configuration Parameters

The following table describes the system parameters that you need to identify to install HA with the Device Server and GUI Server on the same server machine:

Table 20: Typical HA Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary HA Server IP address</td>
<td>IP address of the primary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>Secondary HA Server IP address</td>
<td>IP address of the secondary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>HA replications</td>
<td>Time interval with which you want the GUI Server to replicate the database.</td>
<td>By default, the GUI Server replicates the database every 60 minutes.</td>
</tr>
<tr>
<td>Heartbeat links between primary and secondary machine</td>
<td>Number of heartbeat communication paths between the primary and secondary machine.</td>
<td>By default, there is 1 communication link between the primary and secondary machine. This in addition to the data network link already existing in the primary/secondary HA Server IP Address.</td>
</tr>
<tr>
<td>Shared password for heartbeat authentication.</td>
<td>This is the password that is required to authenticate heartbeat messages between the primary and secondary HA servers.</td>
<td></td>
</tr>
<tr>
<td>IP Address for Primary machine’s heartbeat link</td>
<td>IP address used for heartbeat communications on the primary server machine.</td>
<td></td>
</tr>
<tr>
<td>Port used for heartbeat communication</td>
<td>The port number used for heartbeat communications. The default port is 7802.</td>
<td></td>
</tr>
<tr>
<td>Heartbeat messages time interval</td>
<td>Time interval (in seconds) between heartbeat messages. The default is 15 seconds</td>
<td></td>
</tr>
<tr>
<td>Missing heartbeats before switchover occurs</td>
<td>Number of missing heartbeat messages before automatic switchover to the secondary machine occurs. The default is 4 messages.</td>
<td></td>
</tr>
<tr>
<td>IP Address outside the HA cluster</td>
<td>Network IP Address used to monitor this server’s network connection.</td>
<td></td>
</tr>
<tr>
<td>HA directory</td>
<td>Directory location where high availability data is stored. Note that the same directory location is used if you configure this machine to perform local database backups. By default, the HA Server stores data at: /var/netscreen/dbbackup/</td>
<td></td>
</tr>
</tbody>
</table>

Shared Disk Parameters

If you are using a shared disk partition, the installer prompts you to configure additional information. The following table identifies the additional system parameters that you need to identify to install HA with access to a shared disk:
### Table 21: Shared Disk Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to mount the shared disk partition</td>
<td>The command to mount the shared data partition.</td>
<td>The default command is: &lt;br&gt; <code>/bin/mount /var/netscreen/DevSvr</code></td>
</tr>
<tr>
<td>Command to unmount the shared disk partition</td>
<td>The command to unmount the shared data partition.</td>
<td>Before configuring this command, you must first verify that you have defined your mounts properly. &lt;br&gt; The default command is: &lt;br&gt; <code>/bin/umount /var/netscreen/DevSvr</code></td>
</tr>
<tr>
<td>Command to check the integrity of the shared data partition</td>
<td>The command to check the integrity on the shared data partition.</td>
<td>The default command is: &lt;br&gt; <code>/sbin/fsck</code></td>
</tr>
<tr>
<td>Directory path for the shared disk</td>
<td>Directory path of the shared disk mount point.</td>
<td></td>
</tr>
</tbody>
</table>
**Prerequisite Steps**

Before you install the management system, you need to perform the following prerequisite steps:

1. Ensure that the computer you install the management system on is connected to a serial console or monitor and keyboard.

2. Login to the computer as root.

   If you are already logged in as a user other than root, then type the following command to become root:

   ```
   su -
   ```

   At the password prompt, type the root password for the computer.

3. Partition drives for sufficient disk space to accommodate your planned data requirements.

4. Run the system update utility for your appropriate platform to verify that you have all the prerequisite utilities and packages to run the installer properly. Refer to Running the System Update Utility on page 76 for more information on running the system update utility.

5. If you are installing the management system on Solaris 9, and are planning to perform local database backups, then you must update the Sun Solaris ssh daemon. Refer to Patching the Sun Solaris SSH Daemon on page 77 for more information.

**NOTE:** The NetScreen-Security Manager management system runs as the root user. If you want to run the management system in a more secure mode, then refer to “Changing Permissions To a Normal User” on page 149.

---

3. Partition drives for sufficient disk space to accommodate your planned data requirements.

4. Run the system update utility for your appropriate platform to verify that you have all the prerequisite utilities and packages to run the installer properly. Refer to Running the System Update Utility on page 76 for more information on running the system update utility.

5. If you are installing the management system on Solaris 9, and are planning to perform local database backups, then you must update the Sun Solaris ssh daemon. Refer to Patching the Sun Solaris SSH Daemon on page 77 for more information.

---

**Other Recommended Actions**

It is highly recommended that you disable X server on all the server machines that you plan to install NetScreen-Security Manager. Disabling X server frees up additional server resources for enhanced system performance.

To disable X server on Linux:

1. Navigate to the `/etc` subdirectory.

2. Open the `initab` file in any text editor.

3. Comment out the line that refers to `/etc/dX11/prefdm`.

4. Run `init q`

5. Log out of the graphical console and make sure X does not re-appear.

To disable X server on Solaris, run the following commands:

---

Prerequisite Steps  ■  75
Running the System Update Utility

Use the system update utility to upgrade your system with the latest patches and packages required to run the NetScreen-Security Manager management system installer properly.

To run the system update utility:

1. Save the system update utility appropriate for your platform (for example, `systemupdate-nsm-linux` for Linux, `systemupdate-nsm-solaris` for Solaris) that is provided on the NetScreen-Security Manager Installation CD or from the directory where it is saved, to a suitable directory on the server.

2. Unzip the appropriate system update utility file to decompress the utility. For example, you would run the following command on Linux:

   ```bash
   gzip -d systemupdate-nsm-linux.tar.gz
   ```

3. Untar the appropriate system update utility file to run the utility. For example, you would run the following command on Linux:

   ```bash
   tar xfv systemupdate-nsm-linux.tar
   ```

   A subdirectory called `/systemupdate-nsm-<platform>` is created and all of the files required to update your system packages and utilities are extracted into that directory.

4. Navigate to the `/systemupdate-nsm-<platform>` subdirectory.

5. Run the update shell archive script. For example, you can execute the shell archive script by running the following command:

   ```bash
   ./update.sh
   ```
The script proceeds to check your system for required updates. It next prompts you to type <Enter> to continue or Ctrl-C to stop.

6. Press <Enter> to continue. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 20 minutes. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 10 minutes depending upon the number of packages that need to be installed.

**Patching the Sun Solaris SSH Daemon**

If you are running NetScreen-Security Manager 2004 FP2 on a Solaris 9 system, and you want to perform a database backup, replicate the database remotely, or enable high availability functionality, you must patch the Sun Solaris SSH daemon on both servers. This is because of a known issue in the Sun Solaris SSH daemon that may result in a failure to replicate.

To patch the Sun Solaris SSH daemon on Solaris 9:

1. Login to the server machine that you are running NetScreen-Security Manager as root. You must also be in single user mode.

2. Use a web browser to download the Sun Solaris patch 113273-07 from the following URL:

   `<http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=113273&rev=01>`
3. Extract the packages. For example, run the following commands:

   `unzip /tmp/113273-07.zip`

4. Install the packages. Make sure that you are in the directory where you downloaded the packages. The following example installs the patch to a standalone system:

   `patchadd /tmp/113273-07`

   Checking installed patches...
   Verifying sufficient filesystem capacity (dry run method)...
   Installing patch packages...
   Patch number 113273-07 has been successfully installed.
   See /var/sadm/patch/113273-07/log for details
   Patch packages installed:
      SUNWsshdu

5. Verify that the patch has been installed. For example, run the following command:

   `showrev -p | grep 113273-07`

   Patch: 113273-07 Obsoletes: Requires: Incompatibles: Packages: SUNWsshdu

6. Restart the server machine.
Installing the Management System Software

In most typical cases, you install both the GUI Server and Device Server on the same server. The management system installer is designed to guide you through all of the steps to configure the required system parameters, and then run it to completion.

To install the management system on the same system:

1. Load the NetScreen-Security Manager 2004 FP2 management system installer software onto the server that you have decided to use as the NetScreen-Security Manager management system. You can run the installer directly from the NetScreen-Security Manager installation CD, copy the installer to a directory on the server, or download the installer from the Juniper Networks Customer Services Online web site.

2. Navigate to the directory where you saved the management system installer file. It is recommended that you save the management system installer in the /tmp subdirectory.

3. Run the management system installer.

   On Linux, run the following command:

   ```
   sh nsm04fp2_servers_linux_x86.sh
   ```

   On Solaris, run the following command:

   ```
   sh nsm04fp2_servers_sol_sparc.sh
   ```

   The installation begins automatically by performing a series of pre-installation checks. The installer ensures that:

   - You are installing the correct software for your operating system.
   - All of the needed software binaries are present.
   - You have correctly logged in as root.
   - The system has sufficient disk space and RAM.

   The installer then stops any running servers.

---

**NOTE:** The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the installer successfully performed a task.
- “ok” indicates that the installer performed a check and verified that the condition was satisfied.
- “FAILED” indicates that the installer performed a task or check, but it was unsuccessful.
The installer then prompts you to specify the components of the NetScreen-Security Manager management system that you want to install.

4. Type 3, then press <Enter> to specify that you want to install the Device Server and GUI Server.

The following graphic depicts the installer running on Linux. The installer running on Solaris displays similar prompts and messages.

The script then prompts if this machine will participate in an HA cluster.

5. Type n, and then press <Enter> if you do not want the machine to participate in an HA cluster. If you are planning on configuring the management system with HA enabled, refer to the NetScreen-Security Manager 2004 FP3 Installer’s Guide for more information.

The script then prompts you to specify a location to store the management system data files.

6. Set the directory location for storing the management system data files:
   a. Type the directory location for storing the Device Server data files or press <Enter> to accept the default location /var/netscreen/DevSvr.

   **NOTE:** If you specify a new directory location, then the installer creates it. The installer does not however, allow you to specify an existing directory location. This feature safeguards against over-writing any existing data. If you try to specify an existing directory, the installer indicates that an existing directory already exists, and then prompts you to try again.

The script then prompts you to specify a location for storing the GUI Server data files.
b. Type the directory location for storing the GUI Server data files or press
<Enter> to accept the default location /var/netscreen/GuiSvr.

The script next prompts you to specify the management IP address for the
server.

7. Type the management IP address for the server. This address should be the
same IP address as the server that you are installing on. The installer sets the IP
address and port number on the GUI Server enabling the Device Server to
connect. The Device Server attempts to connect to the GUI Server using port
7800 by default.

The script then prompts you to type a password for the “super” user account.
The initial administrator or “super” user account is the account that you use
when you first login to NetScreen-Security Manager using the
NetScreen-Security Manager User Interface (UI). This account is used to
authenticate communication between the management system and the
NetScreen-Security Manager UI. It possesses all administrative privileges by
default.

8. Type any text string longer than 8 characters for the password. Type the
password again for verification.

NOTE: Make a note of the password that you have set for the super user account.
You need this when you first login to the UI.

The script then prompts you if you want to use a Statistical Report Server with
the GUI Server.

9. Type n and then press <Enter>, if you are not planning on installing
NetScreen-Statistical Report Server with NetScreen-Security Manager. Type y
and then press <Enter> if you are installing NetScreen-Statistical Report
Server with NetScreen-Security Manager. If you typed y, the script then
prompts you to configure parameters required for the management system to
work with the Statistical Report Server (i.e., database type, database server IP
address, database port, database name, database user name, database
password). Refer to the NetScreen-Statistical Report Server Installer’s Guide for
more information about these parameters.
The script next prompts if you want this machine to perform a backup of the database locally.

10. Type \textbf{y} and then press \texttt{<Enter>} if you want the management system to perform a local backup of the database on a daily basis. If you specify that you want the management system to perform automatic backups, the script prompts you to configure options for the backup operation:

   a. Type a \textbf{two-digit number} (00-23) specifying the hour of the day that you want the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, type 12; for midnight, type 00. Press \texttt{<Enter>} to accept the default setting of 02 (2:00 A.M.).

   b. Type \textbf{n}, and then press \texttt{<Enter>} so daily backups are not sent to a remote machine. If you select \textbf{y}, and then press \texttt{<Enter>}, then the script prompts you to enter an IP address for the remote backup machine.

   c. Type a number (up to seven) specifying how many database backup files the management system stores. After the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press \texttt{<Enter>} to accept the default setting of seven backup files. By default, the management system stores backup files in: /var/netscreen/dbbackup

   d. Type the full path to the ssh utility executable.

   Type \textbf{n}, and then press \texttt{<Enter>}, if you do not want the management system to backup the database locally.

The script then prompts you to start servers after installation is complete.
11. Type `y`, and then press `<Enter>`, if you want to start the GUI and Device Servers after the installation has finished. Type `n`, and then press `<Enter>`, if you do not want to start the servers.

The script then prompts you to verify your installation configuration settings.

12. Verify your settings, and if they are correct, type `y`, and then press `<Enter>` to proceed. If you type `n`, and press `<Enter>`, then the installer returns you to the original selection prompt.

The installer performs the following actions:

- Extracts the software payloads
- Performs any applicable migration tasks (disregard since this is a new installation)
- Installs the Device Server
- Installs the GUI Server
- Installs the HA Server
Performing post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server. Several messages display to confirm the installation progress.
The installer runs for several minutes, and then returns you to the command prompt.

**Viewing the Management System Installation Log**

The installer generates a log file with the output of the installation commands for troubleshooting purposes. The naming convention used for the installation log file is:

`netmgmtInstallLog.<current date><current time>`

For example if you ran the installer on December 1, 2004 at 6:00 P.M., the installation log file would be named:

`netmgmtInstallLog.20041201180000`

---

**NOTE:** After the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.

**Starting Server Processes Manually**

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory `/usr/netscreen/HaSvr/bin`. 

   ```bash
   root@docent-attack:~# cd /usr/netscreen/HaSvr/bin
   ```

   You will need this for verification purposes when logging into the GUI Server. Please make a note of it.
2. Run the following command:

```bash
./haSvr.sh start
```

**NOTE:** If you start the HA Server process, then it automatically starts the GUI Server and Device Server processes.

---

**Validating Management System Status**

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes.

To validate the management system is started and running properly, it is recommended that you view the status of all the running server processes (the HA server, Device Server and GUI Server) to confirm that all services are up and running.

If you are experiencing problems with the HA Server, run the following command for more detailed information:

```bash
/usr/netscreen/HaSvr/utils/haStatus
```

The haStatus utility provides additional information describing the state and status of the local/peer servers.

Refer to Controlling the Management System on page 104 for more information on manual commands that you can send to the HA Server, Device Server and GUI Server.
Exporting Data From NetScreen-Global PRO

If you are installing the management system over existing hardware (for example, if you are installing the management system using your existing NetScreen-Global PRO arbitrator), the management system installer detects if you are running NetScreen-Global PRO, and installs and runs the NetScreen-Global PRO data export utility automatically.

If you are installing the management system using new hardware, you must install and run the NetScreen-Global PRO data export utility \( (nsm04fp2_gpelexport_sol_sparc.sh) \) separately on the NetScreen-Global PRO arbitrator and Report Manager Master Controller.

Policy Manager Export Data

Recall that for Policy Manager, you run the NetScreen-Global PRO data export utility on your existing Policy Manager arbitrator. The utility proceeds as follows:

- extracts configuration data from the local LDAP server
- attempts to contact each individual managed device for the latest device configuration data. If utility is successful in connecting to the device, it downloads the device configuration directly from the device. If the utility is not successful in connecting to the device, it extracts the device configuration from the latest configuration summary generated for the device in Policy Manager.

When it has completed this process, the NetScreen-Global PRO data export utility saves the export data in the following location:

\[
/usr/netscreen/var/migration/pmexport.tar
\]

Report Manager Export Data

Recall that for Report Manager, you run the NetScreen-Global PRO data export utility on your existing Report Manager master controller. The utility extracts configuration data from the Report Manager database and saves it in the following location:

\[
/usr/netscreen/var/migration/RMexport.out
\]

Transferring the Export Data Files

Once you have completed the export process, you must transfer these data files to the following subdirectory on the server on which you are installing the NetScreen-Security Manager GUI Server:

\[
/usr/netscreen/GuiSvr/var/migration/
\]

You need to give the user "nsm" permission to the file (the GUI Server runs as this user). You can do so by running the following command:

\[\texttt{chmod \textasciitilde777 /usr/netscreen/GuiSvr/var/migration/}\]

You can then install the User Interface and import the data into NetScreen-Security Manager.
Installing the User Interface

The NetScreen-Security Manager 2004 FP2 User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based computer that meets minimum system requirements. Refer to Chapter 1, Introduction for more information on the minimum system requirements for the UI.

The InstallAnywhere wizard guides you through all the steps required to configure and install the NetScreen-Security Manager UI. Once you install the UI, you can connect it to the management system.

NOTE: It is recommended that you quit all running applications before installing the UI.

To install the NetScreen-Security Manager UI:

1. Login as an Administrator user on the computer where you are installing the UI.

NOTE: For instructions on adding users to the Administrator group, please refer to your operating system manual.

2. Download the UI installer from the NetScreen-Security Manager installation CD or the Juniper Networks corporate web site to the computer where you are installing the UI.

3. Run the UI installer.

   If you are installing the UI on a Windows-based PC, you can double-click on the installer executable.

   If you are installing the UI on a Linux-based computer, you can launch it from a command line. From the command line, you can launch the UI installer using the following command:

   `sh nsm04fp2_ui_linux_x86.bin`

   An Introduction screen for the InstallAnywhere wizard appears.
Follow the wizard through all the steps required to configure and install the UI. Click **Next** to continue the installation. The License Agreement screen appears.

4. Review the License Agreement carefully. If you choose to accept the terms of the License Agreement, click the button next to the appropriate statement. Click **Next** to continue.

**NOTE:** If you choose to not accept the terms of the License Agreement, you will not be able to proceed with the installation.

If you accepted the License Agreement, the Choose Install Folder screen appears.
5. To accept the default install folder, click **Next**.

**NOTE:** If you are installing on a Windows-based computer, the installer saves the UI software files in `C:\Program Files\NetScreen-Security Manager` by default. If you are installing on a Linux-based computer, the installer saves the UI software files in `/root/NetScreen-Security Manager` by default.

To specify a new or different folder location, click **Choose**.... If you decide to accept the default install folder, then click **Restore Default Folder**.

On Windows-based computers, the Choose Shortcut Folder screen appears.

![Choose Shortcut Folder](image)

On Linux-based computers, the Choose Link Folder screen appears.

6. Select where you would like to create the NetScreen-Security Manager product icons. Or, if you are installing on a Linux-based computer, then select where you would like to create links to the NetScreen-Security Manager UI program. Click **Next** to continue. The Pre-Installation Summary screen appears.

7. Verify that the information is correct. To make a change to any of the previous configuration options, click **Previous**. When you are satisfied that the information is correct for this installation, click **Install**. The installer proceeds to install the software files for the UI.

8. If you do not have a default web browser configured, the Select Browser screen appears. Use the **Choose** button to navigate to the subdirectory where your web browser software files are located. Click **Next** to continue.
When the installation is complete, a screen indicating “Install Complete” appears.

**NOTE:** If you do not select a default web browser, the UI will not be able to launch the NetScreen-Security Manager online help. If you still wish to use the online help, you can configure your web browser using the Preferences menu from the UI.

9. Click **Done** to exit the installation program.

**Viewing the Management System Installation Log**

The installer generates a log file with information describing the context of the installation process. For troubleshooting purposes, you may need to access it. The installation log is saved by default in the following directory locations:

For Windows-based computers:

C:\Documents and Settings\<user name>\.nsm\n
For Linux-based computers:

/root/.nsm/

**NOTE:** The .nsm subdirectory is a hidden subdirectory on Linux systems.

The Installation log file is named:

_out.<date/time stamp>.dat

**Running the User Interface**

Once you have completed installing the UI, you can launch the application and verify that you can connect to the management system.

The first time you open the UI, you need to specify the host name (or IP address) of the management system that you want to connect to, a user name, and password. The default user name for new installations is “super”; the default password is the password you specified when configuring the management system. Passwords and user names are case-sensitive.

To log in to the UI for the first time:

1. Run the NetScreen-Security Manager UI.

   If you are running the UI on a Windows-based PC, you can double-click on the NetScreen-Security Manager icon.
If you are running the UI on a Linux-based computer, you can either launch it by double-clicking on the NetScreen-Security Manager application icon (specify that you want to run the program) or you can launch it from a command line. From the command line, navigate to the subdirectory where you have installed the UI software files, and then run the UI application shell archive script. The Login window will appear.

2. Verify that the user name in the **Login** field provided is the initial admin user called “super”. If not, type “super” in the Login field.

3. Type the password that you specified when you installed the management system in the **Password** field provided.

4. Type the IP address you assigned to the GUI Server in the **Server** field provided. If you have enabled DNS-lookup, you can type the host name instead of the IP address.

5. Click **OK**.

The UI appears indicating that the installation was successful.

### Validating the Installation

Once you have installed the management system and UI, it is recommended that you validate basic information configured on the Device Server. You can use the Server Manager to view and edit your configuration on the management system.

To validate your configuration on the Device Server:

1. From the NetScreen-Security Manager UI, double-click the **Server Manager** module. The Server Manager module expands, and the Servers and Server Monitor appears.

2. Select the **Servers** node. The Servers view displays Device Server and GUI Server information.

3. Select the Device Server and click the **Edit** icon or right-click the Device Server and select **Edit** to view all information available on the Device Server.
4. Use the **General** tab to verify the following information:

- **Device Server Manager Port** - the default port is 7800.
- **Device Server ID** - the ID number identifies the Device Server; you cannot change the Device Server ID.
- **Mapped IP Address** - the IP address that is manually defined in the UI.

**NOTE:** You can configure the Device Server to use a Mapped IP (MIP) address. A MIP maps the destination IP address in an IP packet header to another static IP address, enabling the FW/VPN device to receive incoming traffic at one IP address, and automatically forward that traffic to the mapped IP address. MIPs enable inbound traffic to reach private addresses in a zone that contains NAT mode interfaces.

- **Mapped Port** - the port number of the device.

5. Click **OK** when you are done.

**Running the UI in Demo Mode**

Before you begin using NetScreen-Security Manager to configure and manage your network, it is recommended that you first run the UI in Demo mode. Demo mode is an option in the UI enabling you to run the UI disconnected from the management system.

To run the UI in Demo mode:

1. Run the NetScreen-Security Manager UI. The Login window appears.
2. Type any user name in the **Login** field provided.
3. Type any password in the **Password** field provided.

4. Select *DEMO MODE* from the **Server** field pull-down menu.

5. Click **OK**.

6. The Log Viewer main window appears.
Importing Data Into NetScreen-Security Manager

Once you have completed installing the NetScreen-Security Manager User Interface, you can use launch the UI and import configuration data previously exported from NetScreen-Global PRO into NetScreen-Security Manager.

Import Process

Note that you can run the import process multiple times without corrupting the NetScreen-Security Manager database. The import of Policy Manager and Report Manager data can be done at the same time or separately. It is highly recommended that you perform the import of Policy Manager data before or at the same time as the import of Report Manager data. This is because you want to establish your configuration data in NetScreen-Security Manager in the domains that applied in Policy Manager. This configuration data is inherent in Policy Manager. Data configured in Report Manager is not domain-specific.

If you are importing domains individually into NetScreen-Security Manager, it is also highly recommended that you backup your previous installation of NetScreen-Security Manager before running the import. This is to ensure that you can reverse the migration process in the event of an error.

Resolving Domain Name Conflicts

The import identifies all name conflicts before performing the import operation allowing you to determine how to resolve them. Once you have done this, the rest of the migration process can be executed automatically.

During the import, if a domain name already exists in NetScreen-Security Manager (from a previous domain import), the import utility does not try to merge the two domains with the same name. The import utility prompts the user to resolve the name conflict. You can resolve the domain name conflict by choosing one of the following options:

- Rename the Policy Manager domain
- Rename the existing domain in the NetScreen-Security Manager database
- Overwrite the existing domain with the Policy Manager domain
- Do not import the Policy Manager domain

The import resolves conflicts by not importing the new domain by default. Note that the import utility does not try to merge two domains with the same name.

Because there is no concept of domains in Report Manager, users and user groups are imported to the global domain only. Access privileges associated with your Report Manager users and user groups are not imported. After the migration is completed, you have to create new admin roles for these users and user groups.

Import Migration Data

Before importing data from NetScreen-Global PRO, you must ensure that no other Admins are logged into the system. Any changes made to NetScreen-Security Manager system during the migration process will result in database corruption.
To import data from NetScreen-Global PRO:

1. From the **Tools** menu, select **Import Global PRO**. A window appears prompting you to specify the type of data (Policy Manager, Realtime Monitor data) that you wish to import.

2. Click in the appropriate checkbox to select the type of data that you wish to import.

---

**NOTE:** It is recommended that you import your data from Policy Manager first before importing any other data type.

---

Click **Next** to continue. The import process begins automatically.

3. Occasionally, name conflicts occur when an import object has the same name as an existing object. If the import tool experiences a name conflict, a window appears prompting you to resolve the name conflict.

   Click in the radio button provided to specify how you want to resolve any name conflicts. Click **Next** to continue. The Admin Role Options window appears next.

4. During the import of administrators from Policy Manager, the administrative permissions for administrators do not map entirely into NetScreen-Security Manager. You need to select whether to give your administrators more access rights or less access rights in NetScreen-Security Manager.

---

**NOTE:** If you choose "less access rights", the administrators that you migrate from NetScreen-Global PRO may not have sufficient permissions to perform all the tasks in NetScreen-Security Manager that they were previously allowed to perform.

---

5. Click **Next** to continue. A window appears indicating the status of the import process.

   If the UI performs the import process successfully, no errors are indicated.

---

**NOTE:** If you receive a warning message indicating that the IP Address of your current server is invalid for Global-Pro primary server (i.e., “Currently, only Device Server IP is allowed. server_1 will be used instead. 10.5.94.3 is invalid for Global-Pro primary server. Currently, only Device Server IP is allowed. server_1 will be used instead.”), you can safely disregard it. This message serves as a reminder that Global-PRO is no longer in service, and that the NetScreen-Security Manager Device Server is replacing Global-PRO as the management system. This warning message appears if you have not previously deleted your Global-PRO settings.

---

If the UI encounters error(s) during the import process, then it indicates the error count in the Error and Fatal Error fields provided. Click **Cancel** and the UI rolls back all changes and restores the NetScreen-Security Manager database to its pre-migration state.
6. Click **Finish** to exit the import dialog.

**Rolling Back a Failed Migration**

If you are migrating additional domain information after initially performing an import, and you encounter an error, you need to restore the previous NetScreen-Security Manager database from backup.

**Validating a Successful Migration**

To validate that the migration process completed successfully, you need to perform a delta configuration summary on all devices in the network, and verify that there are no deltas.
Post Migration Processes

Once you are satisfied that all your data has successfully migrated from NetScreen-Global PRO into NetScreen-Security Manager, it is recommended that you perform the following manual post-migration steps:

Historical Reporting

If you plan to continue to use Historical Reports with NetScreen-Security Manager, it is very important that you restart the GUI Server after performing the NetScreen-Global PRO import. The restart enables the forwarding of device statistics to the HRS database.

Manually Configuring Protected Resources

If you wish to configure the server/client parameter in the NetScreen-Security Manager Protected Resource as uni-directional, you need to manually reconfigure this after the migration.

Manually Configuring Authentication Servers

If you do not want an authentication server to be used for a specific purpose in NetScreen-Security Manager, you need to manually disable these purposes (FWauth, Xauth, L2TP, Policy Manager Auth) after the migration.

Manually Configuring VPNs

If you implemented Hub and Spoke VPNs in Policy Manager, it was possible to control the granularity of your VPN tunnels by defining each tunnel endpoint as a main or branch. In NetScreen-Security Manager, VPN tunnel endpoints are device-specific. Because of this, “branch” VPN tunnels in NetScreen-Security Manager may have greater access to other branch VPN endpoints than they did in Policy Manager. If this occurs, you need to manually configure a firewall policy to deny this traffic.

Transferring Certificate Files

If you plan to continue managing FW/VPN devices running ScreenOS 4.0.X using NACN, you must transfer and load the private key and certificate file used in your previous Juniper Networks management deployment. During the migration process, these files are stored in a file called PKCS12 in your security database. To transfer and load these files for use in NetScreen-Security Manager, you must manually run the nacnLoadPKCS12 utility.

To transfer your previous private key and certificate files:

1. Login to the computer where you are running the Device Server.
2. Navigate to the /usr/Netscreen/DevSvr/utils subdirectory.
3. Run the nacnLoadPKCS12 utility. The script prompts you to type the full path location to the PKCS12 file.
4. Type the path to the PKCS12 file. The script next prompts you to type a password allowing you to access the PKCS12 file.

**NOTE:** The default password for the PKCS12 file is “production”.

5. Type the password. The script next prompts you whether or not you want to set the migration flag on the file. When set to “y”, the migration flag enables FW/VPN devices using NACN to properly load your old private key and certificate file.

6. Type y to set the migration flag, and press Enter to continue. The script runs to completion.

**NOTE:** If you do not set the migration flag to “y”, FW/VPN devices using NACN will use the newly created private key and certificate file generated during the NetScreen-Security Manager installation.

---

**Disabling the Realtime Monitor Console**

If you are planning on using historical reports, you will need to maintain the Realtime Admin Console to add new devices and users. You do not however, need to continue to use the Monitor Console. It is recommended that you disable the Monitor Console.

To disable the Realtime Monitor Console:

1. Open the pro.admin.init file in any text editor. The pro.admin.init file is located in the Report Manager console installation directory (e.g., C:\Program Files\NetScreen\Report Manager\Console\).

2. Edit the value that appears for the "pro.admin.monitoring.enable" parameter to “false”.

3. Save the file.

---

**Disabling Historical Reporting**

If you do not plan to use historical reporting with NetScreen-Security Manager, it is recommended that you disable forwarding of information from the Master Controller to the Report Manager database.

To disable MC forwarding:

1. Open the Report Manager export data file in any text editor - before performing the import.

2. Delete the line containing the "db_ip_address" parameter.

3. Save the file.
**Upgrading to NetScreen-Security Manager 2004 FP3**

After you have completed installing NetScreen-Security Manager 2004 FP2, and successfully migrated your previous management data to it, you can then proceed to upgrade to NetScreen-Security Manager 2004 FP3.

Congratulations! You have just completed migration and installation of the NetScreen-Security Manager management system and User Interface. You can now begin to manage your network using NetScreen-Security Manager. Refer to the NetScreen-Security Manager 2004 FP3 Administrator’s Guide or Online Help for information describing how to plan and implement NetScreen-Security Manager for your network.
In This Chapter:

- Controlling the Management System
- Archiving and Restoring Logs and Configuration Data
- Configuring High Availability
- Relocating the Database
- Installing a tftp Server
- Downgrading from Feature Pack 3 to Feature Pack 2
- Removing the Management System
- Uninstalling the User Interface

This chapter describes basic procedures used to administer NetScreen-Security Manager. This includes instructions describing how to manually send commands to the management system such as start and stop, configure the GUI Server, Device Server and HA Server manually, configure the local database backup option, install a tftp server (required if you are managing FW/VPN devices running ScreenOS 4.0.x), and uninstall the management system and User Interface.
Controlling the Management System

On occasion, it may become necessary to start or stop the management system processes manually. You can control the management system by navigating to the appropriate “bin” subdirectory for the Device Server, GUI Server, or HA Server, and then issuing a manual command.

Viewing Management System Commands

To view the manual commands that you can send to the GUI Server:

1. Navigate to the GUI Server bin subdirectory. For example, you would run the following command:

   `cd /usr/netscreen/GuiSvr/bin`

2. Run the following command:

   `./guiSvr.sh`

To view the manual commands that you can send to the Device Server:

1. Navigate to the Device Server bin subdirectory. For example, you would run the following command:

   `cd /usr/netscreen/DevSvr/bin`

2. Run the following command:

   `./devSvr.sh`

To view the manual commands that you can send to the HA Server:

1. Navigate to the HA Server bin subdirectory. For example, you would run the following command:

   `cd /usr/netscreen/HaSvr/bin`

2. Run the following command:

   `./haSvr.sh`

Common Management System Commands

The management system supports the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>Sends a hangup signal to the management system process, and then instructs the process to reload its configuration and start again.</td>
</tr>
<tr>
<td>restart</td>
<td>Stops the management system process for two seconds, and then restarts the process.</td>
</tr>
</tbody>
</table>
Starting All Server Processes Using the HA Server

If you have installed the HA Server process, it is highly recommended that you start all the management server processes by simply starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory. For example, you would run the following command:
   
   `cd /usr/netscreen/HaSvr/bin`

2. Run the following command:
   
   `./haSvr.sh start`

NOTE: The HA Server process automatically starts the GUI Server and Device Server processes.

Starting GUI Server and Device Server Processes Manually

If you have not installed the HA Server process, you can manually start the GUI Server and Device Server processes.

To start the GUI Server manually:

1. Navigate to the GUI Server bin subdirectory. For example, you would run the following command:
   
   `cd /usr/netscreen/GuiSvr/bin`

2. Run the following command:
   
   `./guiSvr.sh start`

NOTE: Always start the GUI Server before starting the Device Server. When started, the Device Server attempts to connect to the GUI Server. If the GUI Server is inactive and not running, then the Device Server fails to connect to it.

To start the Device Server manually:

1. Navigate to the Device Server bin subdirectory. For example, you would run the following command:
cd /usr/netscreen/DevSvr/bin

2. Run the following command:

./devSvr.sh start

Stopping Server Processes

You can manually stop each server process as follows.

To stop the GUI Server manually:

1. Navigate to the GUI Server bin subdirectory. For example, you would run the following command:

   cd /usr/netscreen/GuiSvr/bin

2. Run the following command:

   ./guiSvr.sh stop

To stop the Device Server manually:

1. Navigate to the Device Server bin subdirectory. For example, you would run the following command:

   cd /usr/netscreen/DevSvr/bin

2. Run the following command:

   ./devSvr.sh stop

To stop the HA Server process manually:

1. Navigate to the HA Server bin subdirectory. For example, you would run the following command:

   cd /usr/netscreen/HaSvr/bin

2. Run the following command:

   ./haSvr.sh stop
Maintaining the Management System

The following procedures are provided for your reference:

- Changing the Management System IP Address on page 107
- Changing the Device Server IP Address on page 107
- Changing the GUI Server IP Address on page 108
- Changing Permissions To a Normal User on page 109

**Changing the Management System IP Address**

If you have installed the NetScreen-Security Manager management system on a single server (in the basic configuration), and you move it later to a different server, then you need to re-configure the management IP address and port enabling your managed FW/VPN devices to connect to it at its new location.

To change the management system IP address:

1. Update the Device Server IP on each FW/VPN device or set the secondary management server IP to the new IP address.
2. Login to the server that is running the Device Server as root.
3. Navigate to `usr/netscreen/DevSvr/var`
4. Open the Device Server configuration file (`devSvr.cfg`) in any text editor.
5. Edit the values for the `guiSvr.addr` and `guiSvr.port` variables using the new IP address and port number.
7. Navigate to `usr/netscreen/GuiSvr/var`
8. Open the `server_table.nml` file in any text editor.
9. Edit the values for the IP Address in both GUI and Device Server sections.
10. Save the `server_table.nml` file.
11. Restart the GUI Server, and then restart the Device Server.

**Changing the Device Server IP Address**

If you have installed the NetScreen-Security Manager management system on separate servers (in the extended configuration), and you later move the Device Server to a different server, you need to re-configure the management IP address and port enabling your managed FW/VPN devices to connect to it at its new location.

To change the Device Server IP address:
1. Update the Device Server IP on each FW/VPN device or set the secondary management server IP to the new IP address.

2. Login to the server that is running the GUI Server as root.

3. Navigate to /usr/netscreen/GuiSvr/var

4. Open the server_table.nml file in any text editor.

5. Edit the values for the IP Address in the Device Server section only.


7. Restart the GUI Server.

**Configuring the Device Server Manually**

You can also manually configure parameters on the Device Server that control connection timing with the managed FW/VPN devices in your network.

1. Login to the server that is running the Device Server as root.

2. Navigate to /usr/netscreen/DevSvr/var

3. Open the Device Server configuration file (called devSvr.cfg) in any text editor.

4. Edit the time value (in thousandths of a second) for the devSvrDirectiveHandler.fastCli.timeout parameter to change the way the Device Server controls connection timing with managed FW/VPN devices running ScreenOS 4.x.

5. Save the file.

6. Restart the Device Server.

**Changing the GUI Server IP Address**

If you have installed the NetScreen-Security Manager management system on separate servers (in the extended configuration), and you later move the GUI Server to a different server, then you need to re-configure the management IP address and port enabling the Device Server to connect to it at its new location.

To change the GUI Server IP address:

1. Login to the server that is running the Device Server as root.

2. Navigate to /usr/netscreen/DevSvr/var

3. Open the Device Server configuration file (devSvr.cfg) in any text editor.
4. Edit the values for the guiSvr.addr and guiSvr.port variables using the new IP address and port number. Save the Device Server configuration file.

5. Login to the server that is running the GUI Server as root.

6. Navigate to /usr/netscreen/GuiSvr/var

7. Open the server_table.nml file in any text editor.

8. Edit the values for the IP Address in the GUI Server section only.

9. Save the server_table.nml file.

10. Restart the GUI Server, then restart the Device Server.

**Changing Permissions To a Normal User**

The NetScreen-Security Manager management system runs by default as the root user. If you want to change this default behavior to a more secure setup, you can create a normal user (i.e., called “nsm”), and change permissions to that user. For your convenience, a shell archive script called “setperms.sh” is included for both the Device Server and GUI Server that automatically changes the setuid.user value in case you want to switch to the more secure setup.

To create a normal user and change permissions:

1. Stop the HA Server, the Device Server, then the GUI Server.

2. On each of the management system server machines, create a normal user called “nsm” and a group called “nsm”, with the user nsm as the only member.

   You can do so by running the following commands:

   ```
   groupadd nsm
   useradd -g nsm nsm
   ```

3. Run the change permissions script on the Device Server.

   ```
   /usr/netscreen/DevSvr/utils/setperms.sh DevSvr
   ```

4. Run the change permission script on the GUI Server.

   ```
   /usr/netscreen/GuiSvr/utils/setperms.sh GuiSvr
   ```

5. Start the HA Server, GUI Server, and then the Device Server.

6. Verify that the permissions you set are working correctly. One way to check is to verify that the NetScreen-Security Manager servers can write to disk. You can do this by adding a new device and seeing if it appears in the device table file.

**NOTE:** You cannot change permissions and run the HA Server as any user other than root. You must run the HA Server as root.
Archiving and Restoring Logs and Configuration Data

You can archive and retrieve configuration and log data in NetScreen-Security Manager using standard Unix commands. All your configuration information, including device configuration data, administrators, policies, audit logs, and job information is stored on the GUI Server. Logs reside on the Device Server.

Before you begin archiving, it is important that you first stop the processes running on both servers. After you have stopped both servers, you will then need to identify the actual location of the GUI Server and Device Server data directories. These are the directories that you need to back up. You can do this by running an "ls -al" command on the following directory locations:

- /usr/netscreen/GuiSvr/var (or the path that you configured when you initially installed the GUI Server)
- /usr/netscreen/DevSvr/var (or the path that you configured when you initially installed the Device Server)

To archive log and configuration data:

1. Stop the HA Server; stop the Device Server; and then stop the GUI Server.

2. Use the "ls -al" command to discover the actual paths of the GUI Server and Device Server data directories.

   ls -al /usr/netscreen/GuiSvr/var

   lrwxrwxrwx 1 root root 21 Feb 25 16:04 /usr/netscreen/GuiSvr/var -> /var/netscreen/GuiSvr

   The output above indicates that the actual location of the GUI Server data is in: /var/netscreen/GuiSvr

   Verify where your data is stored and which directories should be backed up on your own system. Follow the same procedure to determine the location of your data on the Device Server.

3. Run the appropriate backup command on your Solaris or Linux platform to backup the GUI Server data. For example, you can do so by running the following command:

   tar -cvf /netscreen_backup/db-data.tar /var/netscreen/GuiSvr
   gzip db-data.tar

4. Run the appropriate backup command on your Solaris or Linux platform to backup the Device Server data. It is recommended that you use either Secure Copy or FTP to backup the Device Server data.

   For example, you can use scp by running the following command:

   scp -r <local directory> usr@host:<remote-directory>

   NOTE: Using tar may not be appropriate for log data in the Device Server which may be very large.
For example, you can use ftp by running the following command:

```
ftp <host name>
bi
hash
lcd <local directory>
prompt
mput
```

5. It is recommended that you relocate backup copies of both the GUI Server configuration data and Device Server log data to an external location or disk.

6. Start the HA Server, GUI Server, and then the Device Server.

**Restoring Logs and Configuration Data**

To restore log and configuration data:

1. Stop the HA Server, Device Server, and then the GUI Server.

2. Use the mv command to move data from the "var" directories to a safe location.

3. Untar or place your backups into both of the locations described above.

4. Start the HA server, the GUI Server, and then finally, the Device Server.

**NOTE:** These instructions apply only to systems where the "var" links point to a true location outside the prescribed locations (/usr/netscreen/GuiSvr or /usr/netscreen/DevSvr). It is not recommend that you have these links point to locations that are inside /usr/netscreen/GuiSvr or /usr/netscreen/DevSvr. This will complicate any upgrade of NetScreen-Security Manager and will require special precautions during backup and restore.
Configuring High Availability

You can manually configure the high availability options on the management system by editing the High Availability configuration file (called haSvr.cfg).

**Enabling and Disabling High Availability Processes**

To enable high availability:

1. Stop the running server process(es).

1. Navigate to the High Availability configuration directory. For example, you would run the following command:

   ```
   cd /usr/netscreen/HaSvr/var/haSvr.cfg
   ```

2. Open the High Availability configuration file (haSvr.cfg) in any text editor.

3. Configure the following parameters:

   ```
   highAvail.isHaEnabled=y
   highAvail.isWatchdogEnabled=n
   ```

4. Save the file.

5. Restart the running server process. You can do so by running the following command:

   ```
   /usr/netscreen/HaSvr/bin/haSvr.sh restart
   ```

To disable high availability, follow the above procedures to High Availability configuration file, configure the following parameter, and save the file:

```
highAvail.isHaEnabled=n
```

**Configuring High Availability Options**

Other parameters in the High Availability configuration file enable you to change how high availability works in your network.

To configure other high availability options:

1. Stop the running server process(es).

2. Navigate to the local database backup configuration directory (var/netscreen/HaSvr by default).

3. Open the local database backup option configuration file (haSvr.cfg) in any text editor.

4. Configure the file as needed:

   - To change the local database backup directory, edit the value for the highAvail.pathDbBackup variable.
To change the time of day that the local database backup begins, edit the value for the `highAvail.backupTimeHour` variable.

To change the number of backup files that the tool saves, edit the value for the `highAvail.numofBackup` variable.

To change the path to the rsync package, edit the value for the `highAvail.rsyncLocation` variable.

For example, if you wanted to change the time of day that the local database backup begins to 4:00 A.M., and you wanted to reduce the number of backup files to 3, the configuration file would appear as follows:

5. Save the file.
6. Restart the running server process.

**Running the Remote Replication Utility as a Non-Root User**

If you are prohibited from establishing a trust-relationship between root users on different machines, you can run the remote replication utility as a non-root user. For your convenience, a script called `setRsyncUser` is provided in the utils directory of the HaSvr under `/usr/netscreen` (i.e., `/usr/netscreen/HaSvr/utils/setRsyncUser`), enabling you to run the remote replication utility as non-root user. A README called `README.remote.replication.as.nonroot` file is also provided (in the same directory) with instructions on running the script.

**Backing Up the Database Locally**

A shell archive script is provided for your convenience to manually backup the database locally.

To replicate the database locally:

1. Stop the running server process(es).
2. Navigate to the HA Server utilities subdirectory `/usr/netscreen/HaSvr/utils` by default.
3. Run the replicate database shell archive script. You can do so by running the following command:

   `./replicateDb backup`

The local backup is created under the directory specified by the `highAvail.pathDbBackup` parameter in the High Availability configuration file. By default, it is created in `/var/netscreen/dbbackup`.

**Restoring the Database**

If for any reason you are required to restore the database, then you can invoke a shell archive script.

To restore the database:
1. Install NetScreen-Security Manager 2004 FP2 on a new server machine. The new server machine is required to use:
   - the same IP Address as the previous server that you ran the GUI Server
   - the same operating system that you ran on the previous server

   During the installation, you must also install and configure the local database backup option on both the GUI Server and Device Server.

2. Save your remote copy of the database backup file(s) for the appropriate day of the week to the local database backup data directory on your new management system server.

3. Navigate to the HA Server utilities subdirectory (/usr/netscreen/HaSvr/utils by default).

4. Run the database restore shell archive script and specify the number day of the week for the backup file that you want to restore from (N = backup day of the week). You can do so by running the following command:

   `restoreDbFromBackup.sh N`

   For example, to restore the backup file from Friday:

   `sh restoreDbFromBackup.sh 5`

   The restore script first prompts you to confirm stopping the running server process(es). It proceeds to verify that you have properly logged in as the root user. It then verifies that the backup file specified exists. If so, then the script proceeds to stop all running server processes. It then uses rsync to copy the backup file to the appropriate server directories. After it has completed restoring the files, it restarts all server processes.

**Validating the Database Recovery Process**

If you are using the local database backup option on a network where the GUI Server and Device Server are installed on separate systems, then it is possible that you may experience issues with devices reconnecting to the management system after you have restored the database. This is likely to occur if you did not install the local database backup option properly on the GUI and Device Servers. In this event, contact technical support for assistance.
Relocating the Database

The following process is recommended in the event that you want to move the database from one system to another:

- Archive the database on the GUI Server
- Archive the log database on the Device Server
- Install NetScreen-Security Manager on a new system.
- Copy over the GUI Server database on the new system
- Copy over the Device Server log database on the new system.

Archiving the GUI Server Database and Device Server Log Database

To archive the GUI Server database and the Device Server log database:

1. Verify that the system is working properly.

2. Stop the GUI Server and any High Availability processes (for example, iHaSvr, if you are running NetScreen-Security Manager 2004 FP1 or haSvr, if you are running NetScreen-Security Manager 2004 FP3). You can do so by running the following commands:

   ```
   /etc/init.d/haSvr stop
   /etc/init.d/guiSvr stop
   ```

3. Tar and compress the current GUI Server database. You can do so by running the following commands:

   ```
   tar -cvf guidb.tar /var/netscreen/GuiSvr
   gzip guidb.tar
   ```

4. Stop the Device Server and any High Availability processes (for example, iHaSvr, if you are running NetScreen-Security Manager 2004 FP1 or haSvr, if you are running NetScreen-Security Manager 2004 FP2). You can do so by running the following commands:

   ```
   /etc/init.d/haSvr stop
   /etc/init.d/devSvr stop
   ```

5. Verify that you have sufficient disk space available on the Device Server to backup your current logs.

6. Tar and compress the current Device Server logs. You can do so by running the following commands:

   ```
   tar -cvf devsvrdb.tar /var/netscreen/DevSvr/logs
   gzip devsvrdb.tar
   ```
Installing NetScreen-Security Manager On a New System

Refer to the NetScreen-Security Manager 2004 FP3 Installer’s Guide for more information on installing the management system on the same server machine.

Refer to NetScreen-Security Manager 2004 FP3 Installer’s Guide for more information on installing the management system on separate server machines.

Moving the Databases to the New System

To move the GUI Server database on the new system:

1. On the new GUI Server, make a backup directory for your configurations. You can do so by running the following commands.

   ```bash
   mkdir /backup
   cp /var/netscreen/GuiSvr/server_table.nml /backup
   cp /var/netscreen/GuiSvr/shadow_server_table.nml /backup
   cp /var/netscreen/GuiSvr/global/admin_table.nml /backup
   ```

2. Unzip and untar the database. You can either recursive copy the files or replace the new database with the old one.

3. Replace the configuration files from backup. You can do so by running the following commands:

   ```bash
   # cp /backup/server_table.nml /var/netscreen/GuiSvr
   # cp /backup/shadow_server_table.nml /var/netscreen/GuiSvr
   # cp /backup/admin_table.nml /var/netscreen/GuiSvr/global
   ```

   **NOTE:** This is only required if the passwords/admins are different.

4. Start the GUI Server and verify that all processes are running properly. You can do so by running the following commands:

   ```bash
   /etc/init.d/guiSvr start
   /etc/init.d/haSvr start
   /etc/init.d/guiSvr status
   /etc/init.d/haSvr status
   ```

To copy the Device Server log database on the new system:

1. On the Device Server, unzip and untar the old Device Server logs database. You can either recursive copy the files or replace the new database with the old one.

2. Navigate to the `/var/netscreen/DevSvr/logs` directory and delete all the "*.mark" files. You can do so by running the following commands:

   ```bash
   rm -rf *.mark
   ```

3. Start the Device Server and verify that all the server processes are running.

   ```bash
   /etc/init.d/devSvr start
   /etc/init.d/devSvr status
   ```
/etc/init.d/haSvr start
/etc/init.d/haSvr status
Installing a tftp Server

If you are using NetScreen-Security Manager to manage FW/VPN devices running ScreenOS 4.0.x, then you need to install and run a tftp server on the system that you are running the GUI Server. The tftp server is required to enable firmware updates for FW/VPN devices running ScreenOS versions 4.0.x.

It is not recommended that you use a tftp server to download software for your ScreenOS 4.0.x device because communications are not secured. If your devices are running ScreenOS 4.0.x, and you want to use a tftp server to download software to your devices, then it is highly recommended that you use the ScreenOS WebUI to download software via https.

Installing a tftp Server on Linux

Before installing the tftp server on your Red Hat Linux server, check for previous installations.

To verify if the tftp server is already installed on your Linux server, run the following command:

```
 rpm -q tftp-server
```

If the tftp server is installed, the output indicates the following:

```
tftp-server-<version>-<revision>
```

For example, the output for an unpatched Red Hat 9.0 server is as follows:

```
tftp-server-0.32-4
```

If the tftp server is not installed, then download and install the package from the Red Hat Linux installation CD or from the Internet at the Red Hat or Red Hat mirror site. After the package is installed, you must enable and configure the tftp server.

To configure and enable the tftp server on Linux:

1. Open the `/etc/xinetd.d/tftp` file in any text editor.
2. Edit the parameter “server_args =” so that the value is “-s /usr/netscreen/DevSvr/var/cache
3. Edit the parameter “disable” so that the value is “no”. The file should now appear as follows:

```
 service tftp
 {
   socket_type = dgram
   protocol = udp
   wait = yes
   user = root
   server = /usr/sbin/in.tftpd
   server_args = -s /usr/netscreen/DevSvr/var/cache
   disable = no
   per_source = 11
   cps = 100 2
 }
```

118  ■  Installing a tftp Server
4. Restart the `xinetd` service. You can do so by running the following command:

    service xinetd restart

---

**Installing a tftp Server on Solaris**

By default, Solaris installs the tftp service on your machine but leaves it disabled.

To configure and enable the tftp service on Solaris:

1. Open the `/etc/inetd.conf` file in any text editor.
2. Uncomment the line that begins with the word “tftp” or “#tftp”.
3. Edit the same line by replacing the words “in.tftpd -s /tftpboot” at the end of the line with “in.tftpd -s /usr/netscreen/DevSvr/var/cache”. The line should now appear as follows:

    tftp dgram udp wait root /usr/sbin/in.tftpd
    in.tftpd -s /usr/netscreen/DevSvr/var/cache

4. Restart the `inetd` service. You can do so by running the following commands:

    /etc/init.d/inetsvc stop
    /etc/init.d/inetsvc start
Downgrading from Feature Pack 3 to Feature Pack 2

If you upgrade to FP3, and then decide to downgrade back to FP2, then you need to reinstall FP2 and restore your old data. Before you upgrade NetScreen-Security Manager to FP3, verify that you have made a backup copy of all of your existing data from FP2.

NOTE: Before downgrading, check the audit log for any changes that you might have made, that you may need to restore once the downgrade is complete.

To downgrade from FP3 to FP2:

1. Make a backup copy of all your existing data.
2. Remove the management system. Refer to Removing the Management System on page 121 for more information.
3. Install FP2.
4. Restore your backup database. Refer to Restoring the Database on page 113 for more information.
Removing the Management System

To remove previous management system installations:

1. Stop the HA Server by running the following commands:

   cd /usr/netscreen/HaSvr/bin
   ./HaSvr.sh stop

2. Stop the Device Server by running the following commands:

   cd /usr/netscreen/DevSvr/bin
   ./devSvr.sh stop

3. Stop the GUI Server by running the following commands:

   cd /usr/netscreen/GuiSvr/bin
   ./guiSvr.sh stop

4. Navigate to the /usr subdirectory, and remove all the files in the netscreen subdirectory.

   rpm -e netscreen-DevSvr
   rpm -e netscreen-GuiSvr
   rpm -e netscreen-HaSvr
   rm -rf netscreen

5. Navigate to the /var subdirectory, and remove all the files in the netscreen subdirectory.

   rm -rf netscreen
Uninstalling the User Interface

If you need to uninstall the NetScreen-Security Manager UI, run the NetScreen-Security Manager uninstall program.

NOTE: If you are uninstalling the UI on a Windows-based computer, it is not recommended that you use the Add/Remove Programs utility to remove the NetScreen-Security Manager UI.

To uninstall the NetScreen-Security Manager UI:

1. On a Windows-based computer, use the Start menu, and then select NetScreen-Security Manager > Uninstall NetScreen-Security Manager.

   On a Linux-based computer, you can either double-click on the Uninstall_NetScreen_Security Manager icon, or you can launch the UI uninstaller from a command line.

   sh Uninstall_Netscreen-Security_Manager

   The uninstaller launches.

2. Click the Uninstall button to uninstall the UI. The uninstaller proceeds to uninstall all the UI software files, shortcuts, folders, and registry entries.

   When the uninstaller has finished, a window appears indicating that all files were successfully uninstalled.

3. Click Done to exit the uninstaller.
Appendix A

Technical Overview

This appendix describes the NetScreen-Security Manager three-tiered architecture. This includes a description of the management system, User Interface (UI), and the FW/VPN devices managed in your network.
Technical Overview

The NetScreen-Security Manager management architecture is designed to provide optimum security, scalability, and flexibility for integrating with your specific network security environment. It includes the following key components:

- Management System
- User Interface (UI)
- Managed FW/VPN devices

About the Management System

The management system used in NetScreen-Security Manager provides all of the functionality required to integrate management of all the components in your network security environment. It enables you to centrally gather, store, configure, manage, monitor, and generate reports on the FW/VPN devices you have deployed in your network.

The management system itself is composed of two distinct components:

- GUI Server
- Device Server

Both the GUI Server and Device Server working together are collectively referred to as the NetScreen-Security Manager management system.
You can install both components of the management system on the same physical server or on separate servers. By separating the two server components, you can improve system performance.

**GUI Server**

The GUI Server receives and responds to requests and commands from the NetScreen-Security Manager UI. It manages all the system resources and configuration data required to manage your network. It also contains a local data store where information about your managed FW/VPN devices, administrators, and configurations are centralized.

**NOTE:** The GUI Server can accommodate no more than 20 User Interfaces connected to it at any time. This is the maximum number of UI clients supported in this release of NetScreen-Security Manager.

**Device Server**

The Device Server acts as a collection point for all data generated by each FW/VPN device in your network. The Device Server stores this data, primarily traffic logs generated by the device, in a local data store.

**NOTE:** The Device Server can accommodate no more than 1000 FW/VPN devices connected to it at any time. This is the maximum number of FW/VPN devices supported in this release of NetScreen-Security Manager.

**HA Server**

There is an additional server process called the HA Server that continuously monitors the GUI Server and Device Server processes. If the HA Server process detects that either the GUI Server or Device Server is down, then it automatically restarts the process.
About the NetScreen-Security Manager User Interface (UI)

The NetScreen-Security Manager User Interface (UI) is a java-based software application that you use to access and configure data about your network on the management system. After you have installed the UI, you can launch it and connect it to the management system. From the UI, you can view, configure, and manage your network from a single, central administrative location. Refer to the NetScreen-Security Manager 2004 FP3 Administrator’s Guide or the Online Help included in the UI for more information about the NetScreen-Security Manager UI.

About Managed FW/VPN Devices

The managed FW/VPN devices that you have implemented in your network are the lowest tier of the NetScreen-Security Manager management architecture. The following table details the FW/VPN devices and versions of ScreenOS supported by NetScreen-Security Manager.

Table 23: FW/VPN Devices and ScreenOS Versions Supported in FP3

<table>
<thead>
<tr>
<th>FW/VPN Device</th>
<th>ScreenOS Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS5XP</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5X5T</td>
<td>4.0.0, 4.0.0-DIAL2, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS25</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS50</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS100</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.1</td>
</tr>
<tr>
<td>NS204</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS208</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS500</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS500 GPRS</td>
<td>5.0.0 only</td>
</tr>
<tr>
<td>NS5200/8</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5200/8 GPRS</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS5200/24</td>
<td>4.0.1-SBR, 4.0.1-SIBR, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5200/24 GPRS</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS5400</td>
<td>4.0.1-SBR, 4.0.1-SIBR, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5400 GPRS</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS5GT</td>
<td>4.0.0-DIAL2, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5GT ADSL</td>
<td>5.0.0r6 only</td>
</tr>
<tr>
<td>NS-HSC</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS-2SG-2000</td>
<td>5.0 only</td>
</tr>
</tbody>
</table>

You need to enable each FW/VPN device to communicate and work with NetScreen-Security Manager. Refer to the ScreenOS 5.1 Concepts and Examples Guide for more information describing how to enable management on your FW/VPN devices.
Once enabled, each FW/VPN device communicates and sends information to the NetScreen-Security Manager management system. From NetScreen-Security Manager, you can centralize all configuration data and manage the network from a single, central, administrative location. You can then implement your security policies by “pushing” or sending configuration updates back to your devices.

Based on the device configuration and security policies you define in NetScreen-Security Manager, the managed FW/VPN devices provide the firewall and VPN services required to secure your network environment.

**Communications**

As you plan your installation, it helps to understand how NetScreen-Security Manager establishes communication between the UI, Management System, and FW/VPN devices.

**Communication Ports and Protocols**

For optimum security, the number of total ports on the GUI Server and Device Server is kept to a minimum:

- There is only one open port on the GUI Server — an inbound TCP port that listens for incoming connection requests from the UI(s) and Device Server.

- There are six ports on the Device Server — four inbound TCP ports supporting connection requests from existing FW/VPN devices and two outbound TCP ports used to establish communication with FW/VPN devices running ScreenOS 4.0.X.

The following table summarizes the port that is open on the GUI Server.

**Table 24: GUI Server Communication Ports and Protocols**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7801</td>
<td>TCP</td>
<td>INBOUND</td>
<td>Listens for incoming connection requests from the NetScreen-Security Manager UI(s) and Device Server. Used to establish communication session with Device Server and/or NetScreen-Security Manager UI(s). This communication session uses an encrypted form of TCP called Secure Server Protocol (SSP). It is also a duplexed connection enabling the UI and GUI Server to communicate back and forth to each other after the connection is established.</td>
</tr>
</tbody>
</table>

The following table summarizes the ports that are open on the Device Server.
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7800</td>
<td>TCP</td>
<td>INBOUND</td>
<td>Listens for incoming connection requests from FW/VPN device(s) running ScreenOS 5+. Used to establish encrypted communication sessions with the GUI Server and FW/VPN devices (running ScreenOS 5+).</td>
</tr>
<tr>
<td>15400</td>
<td>TCP</td>
<td>INBOUND</td>
<td>Listens for incoming Report Manager NetScreen protocol (NSP) connection requests from FW/VPN device(s) using ScreenOS 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS 4.0.x. <strong>These sessions are not encrypted.</strong> To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>11122</td>
<td>TCP</td>
<td>INBOUND</td>
<td>Listens for incoming NACN connection requests from FW/VPN device(s) using ScreenOS 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS 4.0.x. <strong>These sessions are not encrypted.</strong> To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>69</td>
<td>UDP</td>
<td>INBOUND</td>
<td>Listens for incoming tftp connection requests from FW/VPN device(s) using ScreenOS 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS 4.0.x. <strong>These sessions are not encrypted.</strong> To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>22/23</td>
<td>TCP</td>
<td>OUTBOUND</td>
<td>Sends outbound Telnet/SSH connection requests to FW/VPN device(s) using ScreenOS 4.0.x. Used to establish communication sessions with FW/VPN devices running ScreenOS 4.0.x. While SSH sessions are encrypted, <strong>Telnet sessions are not encrypted.</strong> To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections. It is not recommended that you use a Telnet session to communicate between devices because it is insecure. If your devices are running with ScreenOS 4.0.x, then use a SSH connection.</td>
</tr>
</tbody>
</table>
Using the Secure Server Protocol (SSP)

NetScreen-Security Manager uses the Secure Server Protocol (SSP) to provide secure communication between each management system component (i.e., GUI Server, Device Server, and UI), as well as between the Device Server and the FW/VPN devices managed in your network. SSP offers strong encryption and authentication mechanisms, so management traffic is protected and kept confidential. SSP utilizes RSA public key cryptography, AES symmetric encryption, and HMAC-SHA-1 hashing.

Communications With Devices Running ScreenOS 5.0+

If you are deploying NetScreen-Security Manager in a network with FW/VPN devices running ScreenOS 5.0 and higher, note that SSP uses two TCP ports for communication:

- TCP port 7800 for the Device Server
- TCP port 7801 for the GUI Server
You must therefore, allow TCP port 7800 on firewalls deployed between the NetScreen-Security Manager management system and the FW/VPN devices managed in your network. You must also configure firewalls between the GUI Server and UI clients to permit TCP port 7801.

The following table lists and describes the ports used specifically in communications between NetScreen-Security Manager and ScreenOS 5.0 devices.

**Table 26: Communications between NSM and Devices Running ScreenOS 5.0**

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 7800</td>
<td>Accepts incoming ScreenOS 5.0 device connections.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 7801</td>
<td>On a separated install, used to communicate with GUI server.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to import initial configs of devices running ScreenOS 5.0.</td>
</tr>
<tr>
<td>GUI Server</td>
<td>Inbound TCP: 7801</td>
<td>Accepts communication from the Device Server and UI.</td>
</tr>
</tbody>
</table>

**NOTE:** The Device Server can use port 22 (SSH) to do a first connect to devices running ScreenOS 5.0, enabling you to set the NSM agent. The NSM agent enables the device to communicate back to the Device Server using SSP port 7800. FW/VPN devices running ScreenOS 5.0 also support SSH v2.

**Communicating With Devices Running Screen 4.x and Earlier**

FW/VPN devices running ScreenOS 4.x and earlier use the same communication protocols for communicating with NetScreen-Security Manager that were supported with Juniper Networks NetScreen-Global PRO:

- Device configuration is performed via telnet or SSH1.
- Logging information is sent over the Juniper Networks Server Protocol (TCP port 15400).
- tftp (UDP port 69) is used for sending firmware updates.
- NetScreen Address Change Notification (NACN), supported in ScreenOS 4.x devices, uses TCP port 11122.

Since some of these protocols (TCP port 15400, Telnet port 23, and tftp) are not encrypted or authenticated, an IPSEC tunnel between the management server and the FW/VPN devices running 4.x and earlier is strongly recommended.

The following table lists and describes the ports used specifically in communications between NetScreen-Security Manager and ScreenOS 4.x and earlier devices.

**Table 27: between NSM and Devices Running ScreenOS 5.0**
Table 28: Communications between NSM and Devices Running ScreenOS 5.0

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to manage FW/VPN devices running ScreenOS 4.0.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 15400</td>
<td>Management for FW/VPN devices running ScreenOS 4.0.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound UDP: 69</td>
<td>tftp server for updating FW/VPN devices running ScreenOS 4.0.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 11122</td>
<td>Accepts incoming NACN requests for FW/VPN devices running ScreenOS 4.0.x.</td>
</tr>
</tbody>
</table>

Creating a Separate Management Network

It is recommended that you isolate the NetScreen-Security Manager management system from the rest of your network traffic. You should send management traffic on a separate management network, and you should deploy a firewall to enforce access policies on the management network.

If you are deploying NetScreen-Security Manager in a network with FW/VPN devices running ScreenOS 5.0 and ScreenOS 4.0.x, then you must configure the firewall protecting the management network to allow:

- TCP ports 7800 and 11122 to the Device Server.
- TCP port 15400 and UDP port 69 to the Device Server over VPN tunnels.
- TCP port 22 outbound from the Device Server.

You do not need to allow traffic to or from the GUI Server if you deploy your UI clients inside the management network. If you must deploy UI clients outside the management network, then you must allow TCP port 7801 access to the GUI Server in the firewall protecting the management network.

For management of ScreenOS 5.0 devices, it is recommended that you use SSP on the untrust interface, as this configuration reduces the possibility of losing access to the device due to an invalid configuration update.

For management of ScreenOS 4.x and earlier devices, it is recommended that you use SSH to the untrust interface. In addition, you should configure a VPN tunnel to send logs/events via TCP port 15400 and firmware updates via tftp.
Appendix B

Migration Details - Global PRO to NetScreen Security Manager

This Appendix provides details on how data is migrated from NetScreen-Global PRO Express and NetScreen-Global PRO into NetScreen-Security Manager 2004 Feature Pack 2.
Domains

The use of domains in Policy Manager enabled you to group and manage separate components of your network. NetScreen-Security Manager extends the domain functionality by enabling you to organize them hierarchically.

In NetScreen-Security Manager, a global domain maintains a parent-child relationship with all other sub-domains. In Policy Manager, there is no concept of domain hierarchy.

Domain Migration

For every domain configured in Policy Manager, a sub-domain is created in NetScreen-Security Manager. All sub-domains created in NetScreen-Security Manager have a child relationship to the global domain.

Sub-domain names are unique in NetScreen-Security Manager. If you attempt to import a domain whose name matches a domain name that already exists in NetScreen-Security Manager, then the import process identifies the conflict, and then prompts you to resolve the name conflict before proceeding with the import.

Configuration data in Policy Manager migrates to NetScreen-Security Manager as part of the same domain that the data resides in Policy Manager (though, these domains may be renamed in the event of name conflicts).

As there is no concept of domains in Report Manager/Realtime Monitor, configuration data in Report Manager/Realtime Monitor migrates to the global domain in NetScreen-Security Manager.

Configuration data in Policy Manager migrates to NetScreen-Security Manager on a per domain basis. During both the export and import processes, you can specify if you want to migrate individual domains or all domains at the same time. Refer to Chapter 1, Introduction for more information on exporting and importing domains.

Example

You configured two domains in Policy Manager - one called “sub0” and another called “sub1”. During the migration, both domains and all the configuration data in them are created in NetScreen-Security Manager. Both sub-domains have a child-relationship to the global domain.
Devices and Device Groups

NetScreen-Security Manager enables you to manage devices and device groups in a similar manner that you were accustomed to in NetScreen-Global PRO. However, during migration, you may notice subtle differences in the way that your device types are abstracted in NetScreen-Security Manager.

There are five main device types in NetScreen-Security Manager:

- FW/VPN Device
- VSYS device
- Extranet device
- Cluster
- Group

Policy Manager Device Migration

For every device configured in Policy Manager (except those mentioned below), a FW/VPN device object is created in NetScreen-Security Manager.

Exceptions:

- For every VSYS device configured in Policy Manager, a “VSYS device” is created in NetScreen-Security Manager.

NOTE: NetScreen-Security Manager does not support the migration of virtual systems that are offline at the time of export. Policy Manager does not store information on the virtual system if offline as required. If you intend to migrate a domain that has virtual systems, then you need to verify that the VSYS root device is online during the export.

- For every Extranet device type configured in Policy Manager, an Extranet device is created in NetScreen-Security Manager.

- For every "configuration-related" Shared Config object in Policy Manager, a template in the Device Manager is created in NetScreen-Security Manager.

- For every device where HA is enabled (where "Active/Passive", "Active/Active" is enabled in the HA screen), a cluster device is created in NetScreen-Security Manager. In addition, for every cluster member configured in the HA device, a cluster member device is created in NetScreen-Security Manager within the cluster device.

All data that is configured for each device in Policy Manager migrates to the configuration of the FW/VPN device object. You can configure the following data in Policy Manager:

- device name
- device type
- device ScreenOS version
- serial number
- admin name/password
- contact IP address (management IP Address)
- SCS use and information
- NACN information
- OSPF information

**Report Manager/Realtime Monitor Device Migration**

Devices configured in Report Manager/Realtime Monitor migrate to NetScreen-Security Manager as follows:

- For every device configured in Report Manager/Realtime Monitor where the serial number configured in Report Manager/Realtime Monitor matches the serial number of any FW/VPN device object already existing in NetScreen-Security Manager (imported from Policy Manager), the configuration data related to that device in Report Manager/Realtime Monitor is merged with the FW/VPN device object (not VSYS device) already created in that sub-domain. This merge means that any additional data in Report Manager/Realtime Monitor is added to the FW/VPN device configuration. Note that no data from the existing FW/VPN device object is overwritten by data from Report Manager/Realtime Monitor.

- For every device configured in Report Manager/Realtime Monitor where the serial number configured in Report Manager/Realtime Monitor does not match the serial number of any FW/VPN device object already existing in NetScreen-Security Manager, a new FW/VPN device object is created in NetScreen-Security Manager and placed in the global domain.

- For every device group in Policy Manager, a device group is created in NetScreen-Security Manager. In addition, all the devices that are members of that device group are listed as members of the device group in NetScreen-Security Manager.

Device groups in Report Manager/Realtime Monitor are not migrated.

**Example: Migrating Devices**

For example, you configured three devices in Policy Manager:

- NS-500 with HA enabled called “NS-500”
- VSYS device called “VS1”
- Extranet device called “Extranet Device 1”

During the migration, the same devices and all the configuration data in them are created in NetScreen-Security Manager. In addition, a cluster device is also created.
Figure 10: Devices in Global PRO and in NetScreen-Security Manager
Users and User Groups

In NetScreen-Global PRO, you could define and configure one type of user only. You could also assign users of NetScreen-Global PRO specific administrative privileges to access objects in the management system.

NetScreen-Security Manager enables you to specifically manage users of the management system and users in your network. There are two main types of users in NetScreen-Security Manager:

- **Admins.** Users of the NetScreen-Security Manager system with specific roles and privileges. Admins are allowed to log into a domain and perform specific activities such as configure and manage devices in the network.

- **Users.** User objects in NetScreen-Security Manager represent users of the devices you manage with NetScreen-Security Manager. User objects can be remote members of a VPN or those referenced in security policies.

During the migration, all users configured in Policy Manager migrate to NetScreen-Security Manager as local user objects. Those users associated with administrative roles in NetScreen-Global PRO also migrate to NetScreen-Security Manager as Admins.

Due to differences inherent in how NetScreen-Global PRO and NetScreen-Security Manager deal with administrative privileges, there is not an exact 1:1 mapping of privileges. Admins as they are configured in NetScreen-Global PRO may have more or less privileges in NetScreen-Security Manager. During the import process, the import utility prompts you to specify a general guideline to apply to all these cases.

You can group “Users” in NetScreen-Security Manager. You cannot however group “Admins” in this release of NetScreen-Security Manager.

Policy Manager User Migration

Users configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every user created in Policy Manager, a local user object is created in NetScreen-Security Manager.

- For every user configured in a firewall policy under the "restricted usage" screen using an external authentication server (Radius, LDAP, SecurID) in Policy Manager, an external user object is created in NetScreen-Security Manager.

**NOTE:** If the user is authenticated locally (using local DB), then a local user object is created in NetScreen-Security Manager only.

- For every user configured as part of a manual key VPN, a manual key user object is created in NetScreen-Security Manager.

- For every user configured with administrative roles in Policy Manager, an Admin user object is created in NetScreen-Security Manager.
If the Policy Manager user has privileges in a specific domain in Policy Manager, then they are created in NetScreen-Security Manager in that specific domain.

If the Policy Manager user has privileges in multiple domains in Policy Manager, then they are created in NetScreen-Security Manager in the global domain.

Since there is no concept of domains in Report Manager/Realtime Monitor, all users from Report Manager/Realtime Monitor are imported into the global domain.

All data configured in the user object in Policy Manager migrates to NetScreen-Security Manager.

**Report Manager/Realtime Monitor User Migration**

Users configured in Report Manager/Realtime Monitor migrate to NetScreen-Security Manager as follows:

- For every user configured in Report Manager/Realtime Monitor, an Admin user object is created and placed in the global domain in NetScreen-Security Manager. However, administrative privileges configured in Report Manager/Realtime Monitor are not migrated.

If the user name configured in Report Manager/Realtime Monitor matches the name of any Admin object already existing in NetScreen-Security Manager (already imported from Policy Manager), then the import utility prompts you to resolve the conflict. You can resolve the conflict by renaming the existing Admin object in the NetScreen-Security Manager database, overwriting the existing Admin object, or you can choose not to import the Report Manager/Realtime Monitor user.

**Policy Manager User Group Migration**

User groups configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every user group created in Policy Manager that includes users without administrative privileges, a local user group object is created in NetScreen-Security Manager.

- If a user is part of a user group in Policy Manager that has administrative privileges, a user has "inherited permissions", then an Admin user object is created for that user in NetScreen-Security Manager.

**NOTE:** Admin users created from Report Manager data have no administrative privileges associated with them. They are effectively useless until you assign them privileges in NetScreen-Security Manager.
If a user has administrative privileges in Policy Manager and is part of a local user group (no permissions), then the local user object associated with the user is created in the local user group.

**NOTE:** Importing Policy Manager domains separately can impact where your users are created in NetScreen-Security Manager. For example, if you have a user in Policy Manager with privileges in subdomain1 and subdomain2, and you import subdomain1 only, then the export process does not know that the user has privileges in subdomain2. During the migration, a user object is created only in subdomain1. This creation is different than if you imported both domains together. In this case, the same user object is created in the global domain (but with privileges to subdomain1 and subdomain2).

**Report Manager/Realtime Monitor User Group Migration**

If a user in Report Manager/Realtime Monitor is part of a user group, then that association is still maintained in NetScreen-Security Manager.

**NOTE:** Users and user groups could share the same name in Policy Manager. In NetScreen-Security Manager, they cannot share the same name. During the migration process, a text string (“i_”) is prepended to the user group name in the event that a user and user group share the same name. For example, if you have both a user and user group called “California”, then the user group is renamed “i_California”.

If you want to maintain the administrative privileges configured for your Admin users and Admin groups in Report Manager/Realtime Monitor, then you need to manually re-create the new admin roles in NetScreen-Security Manager.

**Example: Migrating Users**

You configured a user in Policy Manager named “Shingo Katayama” with administrative roles. During the migration, both a local user object with the same name and an Admin is created in NetScreen-Security Manager.
Figure 11: Users in Global PRO and in NetScreen-Security Manager
**Address Objects**

Both NetScreen-Security Manager and Policy Manager support the creation of security policies and VPNs by referencing shared objects. Objects such as addresses, services, or schedules represent elements of a network or network configuration that you can share across multiple devices.

In Policy Manager, you create and configure address objects in an Address Book. You could also define and associate multiple address members and network mask pairs in a single address book entry.

In a similar manner, NetScreen-Security Manager enables you to configure address objects in the Object Manager module under Address Objects.

In NetScreen-Security Manager, however, you cannot associate multiple addresses within a single address object as you could with address members or network mask pairs in Policy Manager. Each address entry is managed as a separate object entity in NetScreen-Security Manager. During the migration process, each address member and network mask pair in a Policy Manager address book entry is created as an individual address object in NetScreen-Security Manager. Because of this, you may notice after the migration that you now have more address objects in NetScreen-Security Manager than you previously configured in Policy Manager.

NetScreen-Security Manager also introduces the concept of address network objects and address groups.

**Address Book Migration**

Address objects configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every individual address entry configured in Policy Manager, an address object is created in NetScreen-Security Manager. This includes individual address entries configured as a network mask pair as well as those configured as an address member in every address object Policy Manager.

- Address entries with a less than 32 bit mask configured in Policy Manager are created as an address network object in NetScreen-Security Manager. Address entries with a 32 bit mask in Policy Manager are created as an address host object in NetScreen-Security Manager.

- For every address book entry configured in Policy Manager with multiple address entries, an address group is created in NetScreen-Security Manager. The address group is named with the same name as in Policy Manager. Host address entries in the group are however renamed with the IP Address appended to it ("_10.1.1.1"). Network address entries in the group are renamed with the IP Address/NetMask appended to it (10.1.1.0/16).

All data configured in the address object in Policy Manager migrates to NetScreen-Security Manager.
Example: Migrating Address Book Objects
You configured several address objects in Policy Manager. During migration, the same address objects and all the configuration data in them are created in NetScreen-Security Manager. The West Region Address Book with several address members associated with it becomes an address group in NetScreen-Security Manager. Note also that the Site A address object becomes an address network object in NetScreen-Security Manager.

Figure 12: Address Book Objects in Global PRO and in NetScreen-Security Manager
Schedule Objects

Like addresses in Policy Manager, you could also define and configure schedule objects in a Schedule Book. In a similar manner, NetScreen-Security Manager enables you to configure schedule objects in the Object Manager module under Schedule Objects.

Schedule Object Migration

For every individual schedule object configured in Policy Manager, a schedule object is created in NetScreen-Security Manager. Any text string configured as a description in Policy Manager migrates as a comment in NetScreen-Security Manager.

All data configured in the Schedule object in Policy Manager migrates to NetScreen-Security Manager.

Example: Migrating Schedule Objects

You configured two schedule objects in Policy Manager - one named “Operating Hours” and another named “After-Hours”. During migration, both schedule objects are created in NetScreen-Security Manager.

Figure 13: Schedule Objects in Global PRO and in NetScreen-Security Manager
Service Objects

In Policy Manager, you create and configure service objects in a Service Book. You could also define and associate multiple services in a single service book entry.

In a similar manner, NetScreen-Security Manager enables you to configure service objects in the Object Manager module under Service Objects. In NetScreen-Security Manager, however, you cannot associate multiple services within a single service object as you could with services in Policy Manager. Each service member is configured as a separate object entity in NetScreen-Security Manager. During the migration process, each service member in a Policy Manager service book is created as an individual service object in NetScreen-Security Manager. Because of this, you may notice after the migration that you now have more service objects in NetScreen-Security Manager than you previously configured in Policy Manager.

Service Object Migration

Service objects configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every individual service object configured in Policy Manager, a service object is created in NetScreen-Security Manager.

- For every service member configured as part of a service object in Policy Manager, a service object is created in NetScreen-Security Manager.

- For every service object configured with multiple user-defined services in Policy Manager, a service group object is created in NetScreen-Security Manager. The service group is named with the same name as in Policy Manager. The service entry in the group is however, renamed using the name of the service group and a text string appended to it (currently this is "_svc"). For example, if the service group is called "service" in Policy Manager, the service entry is renamed "service_svc" in NetScreen-Security Manager.

- For the "AOL" pre-defined service object in Policy Manager, a service group and a service object called "AOL" is created in NetScreen-Security Manager. The "AOL" service object is then added as a member of the group.

All data configured in the Service object in Policy Manager migrates to NetScreen-Security Manager.

Example: Migrating Service Objects

For example, if you configured a service object in Policy Manager named “Service Book 1”, with two service members (Gopher and FTP). During the migration, the individual service objects are created in NetScreen-Security Manager for Gopher and FTP, and has a service group called “Service Book 1” that includes Gopher and FTP.
Shared and Protected Resources

In Policy Manager, you create and configure shared resource objects in a Shared Resource Book. You could further define Protected Resources for use in creating a VPN for a specific FW/VPN device. In a similar manner, NetScreen-Security Manager enables you to configure shared resource objects in the Object Manager module under Protected Resources.

Because both shared and protected resources defined in Policy Manager as a shared object and those specifically protected by a specific device are migrated as shared resource objects in NetScreen-Security Manager, you may notice more shared resource objects in NetScreen-Security Manager than you had in NetScreen-Global PRO.

Shared Resource Object Migration

Shared Resource objects configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every Shared Resource object configured in Policy Manager, a Protected Resource object is created in NetScreen-Security Manager. This includes those “Protected Resources” defined for every device as well as those defined as a Shared resource (protected by multiple devices) in Policy Manager.

- All configuration data for the Shared Resource is collapsed into the Protected Resources object in NetScreen-Security Manager.

- Server/Client parameter in NetScreen-Security Manager is set to “Both” by default.

Example: Migrating Shared Resources

You defined a Protected Resource called “My Protected Resources” as part of a VPN for a FW/VPN device in Policy Manager. During the migration, the object is created as a Protected Resource object in the VPN Manager.
Figure 14: Protected Resources in Global PRO and in NetScreen-Security Manager
Global Objects

In Policy Manager, you create and configure global objects under Global Objects. You could further define device-specific Dynamic IPs, Mapped IPs, and Virtual IPs under the NAT settings associated with a FW/VPN device.

In a similar manner, NetScreen-Security Manager enables you to configure global objects in the Object Manager module under NAT Objects. Note that you may notice more NAT objects in NetScreen-Security Manager than those configured as global objects in Policy Manager because device-specific global objects in Policy Manager are migrated as NAT objects in NetScreen-Security Manager.

Global Object Migration

For every Global object configured in Policy Manager, a NAT object is created in NetScreen-Security Manager.

For device-specific objects in Policy Manager:

- For every device-specific MIP objects in Policy Manager, a NAT object is created in NetScreen-Security Manager. If there are multiple device-specific MIP objects in Policy Manager with the same MIP IP Address/Mask, they all merge into one NAT object in NetScreen-Security Manager. The name of the object in NetScreen-Security Manager is "MIP(IP Address/Mask)".

- For every device-specific DIP object in Policy Manager, a NAT object is created in NetScreen-Security Manager. If there are multiple device-specific DIP objects in Policy Manager with the same DIP IP range, they all merge into one NAT object in NetScreen-Security Manager. The name of the object in NetScreen-Security Manager is "DIP id (start_IP address-end_IP address)".

- For every device-specific DIP group object in Policy Manager, a NAT object is created in NetScreen-Security Manager. If there are multiple device-specific DIP group objects in Policy Manager with the same DIP group id, they all merge into one NAT object in NetScreen-Security Manager. The name of the group object in NetScreen-Security Manager is "DIP group id(group)" for example ("5(group)").

All data configured in the Global object in Policy Manager migrates to NetScreen-Security Manager.

Example: Migrating Global Objects

You configured a Global object in Policy Manager. During the migration, the object and all of its configuration data are created in NetScreen-Security Manager in the Object Manager module under NAT Objects.
Authentication Servers

NetScreen-Security Manager enables you to configure authentication server objects in the Object Manager module under Authentication Servers.

Authentication Server Object Migration

For every authentication server object configured in Policy Manager, an authentication server object is created in NetScreen-Security Manager. All data configured in the authentication server object in Policy Manager migrates to NetScreen-Security Manager. You could enable multiple purposes for authentication servers in Policy Manager. During the migration, all purposes are enabled in NetScreen-Security Manager.

NOTE: In Policy Manager, the default global authentication server object called "Local Database" does not migrate into NetScreen-Security Manager.

Example: Migrating Authentication Server Objects

You configured an authentication server object in Policy Manager named “Corporate Authentication Server”. During the migration, the object and all of its configuration data are created in NetScreen-Security Manager in the Object Manager module under Authentication Servers.
Figure 15: Authentication Servers in Global PRO and in NetScreen-Security Manager
**Group Expressions**

NetScreen-Security Manager enables you to configure group expression objects in the Object Manager module under Group Expressions.

**Group Expression Migration**

For every Group Expression configured in Policy Manager, a Group Expression object is created in NetScreen-Security Manager. All data configured in the group expression object in Policy Manager migrates to NetScreen-Security Manager.

**Example: Migrating Group Expression Objects**

You configured two group expression objects in Policy Manager named “exp1” and “exp2”. During the migration, both objects and all of their configuration data are created in NetScreen-Security Manager in the Object Manager module under Group Expressions.

**Figure 16: Group Expression Objects in Global PRO and in NetScreen-Security Manager**
**Shared Configs**

Shared Configs in Policy Manager enabled you to define and configure common settings that you could apply to multiple devices or other NetScreen-Global PRO components.

In NetScreen-Security Manager, the same functionality is achieved using templates. Templates in NetScreen-Security Manager enable you to configure a device or multiple devices with a set of pre-defined configuration settings.

**Shared Config Object Migration**

Shared config objects configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every "configuration-related" Shared Config object in Policy Manager (NetScreen-Global Pro Monitoring, Packet Flow, AuthServer, Banner, NTP/Clock, DNS, SNMP, E-mail Alerts, Syslog, URL Filter, WebTrends), a template in the Device Manager is created in NetScreen-Security Manager. All data configured in the shared config object in Policy Manager migrates to NetScreen-Security Manager.

- "Action-related" Shared Configs in Policy Manager including CA Certs and CRL By File are not migrated.

NetScreen-Security Manager does not permit device templates and device objects to share the same name. During the migration process, the following text strings are prepended to the device template name in the event of a device template and device name conflict.

**Table 29: Shared Config Template Name Conversion**

<table>
<thead>
<tr>
<th>Shared Configuration Type</th>
<th>Text String Prepended to Device Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Group</td>
<td>AdminGroup_</td>
</tr>
<tr>
<td>Auth Server</td>
<td>AuthServerTemplate_</td>
</tr>
<tr>
<td>Banner</td>
<td>BannerTemplate_</td>
</tr>
<tr>
<td>Email Alert</td>
<td>Email AlertTemplate_</td>
</tr>
<tr>
<td>Flow Shared</td>
<td>FlowTemplate_</td>
</tr>
<tr>
<td>GlobalPRO</td>
<td>GlobalPROTemplate_</td>
</tr>
<tr>
<td>NTP</td>
<td>NTPTemplate_</td>
</tr>
<tr>
<td>SNMP</td>
<td>SNMPTemplate_</td>
</tr>
<tr>
<td>Syslog</td>
<td>SyslogTemplate_</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>UrlFilteringTemplate_</td>
</tr>
<tr>
<td>WebTrend</td>
<td>WebTrendTemplate_</td>
</tr>
</tbody>
</table>

The export tool prints out a table at the end of the exporting process to list all the objects that are renamed due to name conflicts.
Example: Migrating Shared Config Objects

You configured a shared config object in Policy Manager called “No Dog Sites”. During the migration, the configuration data appears in NetScreen-Security Manager as a template in the Device Manager.

Figure 17: Shared Configs in Global PRO and in NetScreen-Security Manager
Zone Profile

Similar to Shared Configs, Zone Profiles enabled you to define common zone settings that you could apply to multiple devices. In NetScreen-Security Manager, the same functionality is achieved using templates.

Zone Profile Object Migration

For every Zone Profile configured in Policy Manager, a template in the Device Manager is created in NetScreen-Security Manager. Data configured for each zone profile in Policy Manager migrates to the configuration of the template (Network > Zone) in NetScreen-Security Manager. This includes the zone name, interfaces, traffic filtering settings, VR settings etc.

NOTE: Configuration data for Zone profiles is migrated into NetScreen-Security Manager as part of the device configuration import process.

Example: Migrating Zone Profile Objects

You configured a zone profile object in Policy Manager called “Zone1”. During the migration, the configuration data appears in NetScreen-Security Manager as a template in the Device Manager.

Figure 18: Zone Profiles in Global PRO and in NetScreen-Security Manager
Policies

Both NetScreen-Security Manager and Policy Manager support the definition and configuration of firewall policies enabling you to either deny or permit specific network traffic across your FW/VPN devices. In Policy Manager, you could apply multiple policies to a specific FW/VPN device in a priority list order.

NetScreen-Security Manager provides the same functionality, but without the concept of hierarchical policy lists. In NetScreen-Security Manager, the same functionality is achieved by installing one active policy with multiple rules on each FW/VPN device.

Policy Migration


Rule Groups allow you to:

- Map Policy Groups into Feature Pack 2.
- Group rules together and manage groups as discrete elements.
- Assign a name and comments, and the groups can be expanded and collapsed.
- Preform delete and move rule group operations.

Example: Migrating Policies NetScreen-Global PRO

You have three Policy Groups configured in Policy Manager, Policy A, Policy B, and Policy C, each policy has five rules. When migrated, the three individual policies are merged and stacked according to priority and built into a single shared policy with 15 rules. Each policy in NetScreen-Global PRO becomes a rule in the shared policy in NetScreen-Security Manager.
VPNs

Both NetScreen-Security Manager and Policy Manager support the creation and management of virtual private networks (VPNs). In Policy Manager, you created and configured all your VPNs using a VPN abstraction tool. Once you were done configuring your VPN, the tool would proceed to generate policies that enabled your VPN tunnels.

In NetScreen-Security Manager, you use a similar type of tool called the VPN Manager to create and configure your VPNs. Manual VPNs are however, not supported in the VPN Manager component in NetScreen-Security Manager. Manual VPNs are device-specific in NetScreen-Security Manager.

During the migration, policies for your manual VPNs are generated and added to the top of the active policy list. In addition, VPN pointers or links are created for all other VPN policies and merged with the active policy list. "5-tuple" firewall policies are also merged with their related VPN policies allowing you to specify traffic shaping, logging options. This is done via a Device Configuration Import operation performed during the import process.

VPN Migration

VPNs configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every IKE Autokey and Manual VPN configured in Policy Manager, an IPsec VPN is created in NetScreen-Security Manager. Policy-based members and route-based members that are configured in Policy Manager migrate to these VPNs as well. All relevant configuration data in Policy Manager migrates to the object in NetScreen-Security Manager.

- For every IKE Autokey VPN with users configured as policy-based members, an IPsec User VPN in NetScreen-Security Manager is created. All relevant configuration data in Policy Manager migrates to the object in NetScreen-Security Manager.

- For every L2TP VPN configured in Policy Manager, an L2TP VPN object is created in NetScreen-Security Manager. All relevant configuration data in Policy Manager migrates to the object in NetScreen-Security Manager.

- For every L2TP over IPsec VPN configured in Policy Manager, an L2TP over IPsec VPN object is created in NetScreen-Security Manager. All relevant configuration data in Policy Manager migrates to the object in NetScreen-Security Manager.
**P1 and P2 Proposals**

NetScreen-Security Manager enables you to manage P1 and P2 Proposals objects in the VPN Manager module.

**P1 and P2 Proposal Object Migration**

P1 and P2 Proposal objects configured in Policy Manager migrate to NetScreen-Security Manager as follows:

- For every P1 Proposal object configured in Policy Manager, a Custom IKE Phase1 Proposal object is created in NetScreen-Security Manager under the VPN Manager. These objects are renamed with the VPN name prepended to the name of the proposal (“VPN Name:P1 Proposal”).

- For every P2 Proposal object configured in Policy Manager, a Custom IKE Phase2 Proposal object is created in NetScreen-Security Manager under the VPN Manager. These objects are renamed with the VPN name prepended to the name of the proposal (“VPN Name:P2 Proposal”).

**Example: Migrating P1 & P2 Proposal Objects**

You configured a P1 Proposal object in Policy Manager named “P1”. During the migration, the object and all of its configuration data are created in NetScreen-Security Manager in the VPN Manager module under IKE Phase 1 Proposals.
**IP Pools**

NetScreen-Security Manager enables you to manage IP Pools in the VPN Manager module.

**IP Pool Migration**

For every IP Pool object configured in Policy Manager, an IP Pool object is created in NetScreen-Security Manager under the VPN Manager.

**Example: Migrating IP Pool Objects**

You configured an IP Pool in Policy Manager. During the migration, the object is created in NetScreen-Security Manager in the VPN Manager module under IP Pools with all of the configuration data related to the IP Range.
Remote Settings

NetScreen-Security Manager enables you to manage Remote Settings objects in the VPN Manager module.

Remote Setting Object Migration

For every IP Pool object configured in Policy Manager, an IP Pool object is created in NetScreen-Security Manager under the VPN Manager.

Example: Migrating Remote Settings Objects

You configured a remote setting in Policy Manager. During the migration, the object is created in NetScreen-Security Manager in the VPN Manager module with all of the relevant return values configured.
**Events**

Mapping tables configured in Realtime Monitor enabling events to appear in NetScreen-Security Manager as they did in Realtime Monitor - by group, type, and severity level, are migrated into NetScreen-Security Manager.
Certificates

Certificates used for communications with FW/VPN devices running ScreenOS 4.0.X using NACN are also migrated from Policy Manager into NetScreen-Security Manager. After the migration, you must copy the private certificate key using the NACN certificate transfer utility to the Device Server.
Data Collector Properties

The polling attributes and intervals used by each data collector to collect data from each device configured in Report Manager/Realtime Monitor are migrated in NetScreen-Security Manager. Assuming that the Device Server in NetScreen-Security Manager is installed on the same server as the Report Manager/Realtime Monitor data collector, the configuration parameters enable NetScreen-Security Manager to connect to FW/VPN devices running ScreenOS 4.0.x. If the Device Server is installed on a server with a new IP address, you can still connect to legacy devices by changing the NetScreen-Global PRO IP addresses in all devices.

**NOTE:** Server properties from your previous configuration in NetScreen-Global PRO override any existing data configured in NetScreen-Security Manager.
Master Controller Properties

Properties enabling the Master Controller to connect and forward data to the Report Manager database (database name, IP Address, protocol and port) are migrated in NetScreen-Security Manager. This is applicable only if you plan to continue using historical reports with NetScreen-Security Manager.

E-mail properties enabling NetScreen-Security Manager e-mail alerts to be sent to the NetScreen-Security Manager admin are also migrated.

**NOTE:** Server properties from your previous configuration in NetScreen-Global PRO override any existing data configured in NetScreen-Security Manager.
**Historical Reports**

If you wish to continue using historical reports with NetScreen-Security Manager, it is highly recommended that you install NetScreen-Statistical Report Server. Refer to the *NetScreen-Statistical Report Server* documentation set for more information.

You can also continue to use historical reports in Report Manager with NetScreen-Security Manager. By maintaining your HRS infrastructure, you can still receive resource statistics, traffic, and service level agreement data from managed FW/VPN devices using ScreenOS versions 4.0.X.

---

*NOTE:* You can use the NetScreen-Security Manager UI to view realtime alarm and log data from managed FW/VPN devices using ScreenOS versions 5.0.X.
Features No Longer Supported

NetScreen-Security Manager does not support the migration of logs from NetScreen-Global PRO.

NetScreen-Security Manager does not support the following features in Policy Manager:

- Policy Queries
- NSRP - previously depicted in the HA tab in Device Objects, now appears as a cluster object (containing devices).
- Admin Groups
- Authenticate ‘N Go (ANG) support for NetScreen-Remote clients.
- Hierarchical policy lists in PRO are manifested in a different manner in NetScreen-Security Manager. In NetScreen-Security Manager, you can only have 1 active policy per device.
- Manual VPNs - are abstracted in a different manner in NetScreen-Security Manager.
- VSYS - manifested differently in NetScreen-Security Manager
- Templates - manifested differently in NetScreen-Security Manager

NetScreen-Security Manager does not support the migration of the following data configured in Report Manager:

- Admin privileges
- Device Groups

NetScreen-Security Manager does not support the following features in Report Manager:

- Global properties configured in Report Manager that controlled how data was integrated with other third party management systems, archived and purged are not migrated.
- Oracle, MS-SQL, or PGSGL database support.
- Report Manager/Realtime Monitor monitor and display filters. You need to manually create new filters in the Log Viewer.
- Report Manager/Realtime Monitor histograms. You can no longer view a histogram of your events.
Appendix C

Migration Details - FP1 to FP2

This Appendix describes how data is migrated from NetScreen-Security Manager Feature Pack 1 to NetScreen-Security Manager Feature Pack 2.
Policy Migration

In NetScreen-Security Manager 2004 Feature Pack 3 there is only one type of policy— called a Security Policy. A Security Policy consists of one or all of the following rulebases:

- Firewall
- VPN
- Multicast

The firewall and multicast policies that you configured in FP1 are migrated to rulebases in FP2. Every new NetScreen-Security Manager FP2 Security Policy contains the firewall rulebase by default.

Example: Migrating Policies Feature Pack 1

You have two policies configured in FP1. One policy is a firewall policy and the other is a multicast policy. Each policy has five rules. Both policies are used by the same FW/VPN device. When migrated to FP2, each policy is migrated into a rulebase. A new FP2 policy is created to include both rulebases.
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>D</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>E</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>G</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>H</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>I</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
log file
management system install................................. 48, 85
UI installation.............................................. 54, 91
logging in to the UI ........................................ 54, 91
logs
restoring ......................................................... 111

management IP address
for GUI-server, described ................................... 33, 71
management system
changing default user .......................................... 109
commands ......................................................... 104
installing on same server .................................... 41–48, 79–86
restarting ......................................................... 104
status ................................................................. 105
stopping ............................................................. 105
uninstalling ...................................................... 121
manuals, SDX
comments on ..................................................... 8
memory requirements
for UI ............................................................... 18
management system on same server ................. 17
management system on separate servers .......... 17
migration and installation process ...................... 12–15
migration and installation scenarios
Global PRO ........................................................ 64–68
Global PRO Express ............................................ 28–30
migration path .................................................... 30
migration scenarios
not supported (Global PRO Express) .................. 30
not supported (Global PRO) ............................... 68
minimum system requirements
described ........................................................... 17–18
for UI ............................................................... 18
management system ........................................... 17–18

network connection
requirements for UI ............................................. 18
requirements on management system, same server 17
requirements on management system, separate servers 17

operating system
requirements for management system ................. 17
requirements for UI ............................................. 18

password
super user, configuring ......................................... 43, 81
Password for GUI Server connection
described .......................................................... 34, 72
pexport.tar
see Policy Manager data export file

Policy Manager
export data file .................................................. 87
post migration steps ........................................... 60
pre-migration steps
Global PRO Express ........................................... 32, 70
prerequisites before installing ............................ 37, 75

replicating
database .......................................................... 113
Report Manager
export data file .................................................. 87
restoring
management system manually ......................... 104
restoring management system ......................... 104
restoring
database .......................................................... 113
logs and configuration data ................................ 111
rmexport.out
see Report Manager data export file
root user
changing user that management system runs as ... 109
running
UI ............................................................... 54, 91
UI, in Demo Mode ........................................... 56, 95

SDX documentation set
comments on ..................................................... 8
starting
Device Server .................................................. 105
GUI Server ...................................................... 105
HA Server ....................................................... 105
management system manually ......................... 105
stopping
Device Server .................................................. 106
GUI Server ...................................................... 106
HA Server ....................................................... 106
management system manually ......................... 105
super user
password, configuring ......................................... 43, 81
password, described .......................................... 53, 71
swap space
requirements on management system, same server 17
requirements on management system, separate servers 17
system parameters ............................................. 33, 71

TFTP server
installing on Linux ............................................. 118
installing on Solaris .......................................... 119
transferring
export data files (for Global PRO Express) ........ 50
export data files (for Global PRO) ................. 87

UI

installing .................................................. 51–54, 88–91
running ............................................................... 54, 91
uninstalling .............................................................. 122
uninstalling UI .......................................................... 122

V
validating
  database recovery ........................................ 114
  management system installation .................. 55, 92
  management system status ......................... 49, 86
  viewing management system commands .......... 104

X
X Server
  disabling ......................................................... 37, 75