**Copyright Notice**

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.
ATTN: General Counsel
1194 N. Mathilda Ave. Sunnyvale, CA 95014

**FCC Statement**

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

**Caution:** Changes or modifications to this product could void the user’s warranty and authority to operate this device.

**Disclaimer**

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.
Contents

Preface ....................................................................................................................................... V

Organization ......................................................................................................................... v

CLI Conventions .................................................................................................................. vi

Juniper Networks Publications ........................................................................................... vi

Chapter 1 Troubleshooting ............................................................................................... 1

General Troubleshooting .................................................................................................. 1

Chapter 2 Resetting the Device .................................................................................... 3

Chapter 3 Enabling Event Messages .......................................................................... 5
Preface

The Juniper Networks NetScreen-Hardware Security Client (NS-HSC) provides IPSec VPN and firewall services for a broadband telecommuter, a branch office, or a retail outlet. The NS-HSC uses the same firewall, VPN, and traffic management technology as Juniper Networks’ high-end central site products.

NS-HSC is designed for management by NetScreen-Security Manager (NSM) 2004, the integrated management system for all NetScreen FW/VPN devices. Although the NSM administrator handles most of the day-to-day administration of the NS-HSC device, the local device admin can perform basic troubleshooting techniques and, if necessary, reset the device to its factory defaults.

Specifically, this Administrator’s Guide is intended for:

- **Non-technical users (Chapters 1 & 2).** Non-technical users can identify basic system problems and reset the NS-HSC device.
- **IT administrators with networking experience (Chapter 3).** IT administrators can enable event messages on the NS-HSC device to help them identify and resolve more complex system problems.

**Organization**

This guide has three chapters:

- **Chapter 1, “Troubleshooting”,** describes troubleshooting techniques for the NetScreen-Hardware Security Client.
- **Chapter 2, “Resetting the Device”,** describes how to reset the NetScreen-Hardware Security Client to factory default settings.

**CLI Conventions**

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces {} is required.
- If there is more than one choice, each choice is separated by a pipe ( | ). For example,
  
  ```
  set interface { ethernet1 | ethernet2 | ethernet3 }
  manage
  ```
means “set the management options for the ethernet1, ethernet2, or ethernet3 interface”.

- Variables appear in italic. For example:

  `set admin user name1 password xyz`

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in italic). For example: “Use the **get system** command to display the serial number of a NetScreen device.”

---

**JUNIPER NETWORKS PUBLICATIONS**

To obtain technical documentation for any NetScreen product, visit [www.juniper.net/techpubs/](http://www.juniper.net/techpubs/).

To obtain the latest version of NetScreen software, visit [www.juniper.net/support/](http://www.juniper.net/support/). Before you can perform such downloads, you must register as an authorized user.

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

  techpubs@netscreen.com
This chapter describes troubleshooting procedures for the NetScreen-Hardware Security Client. If your device is not working as expected, you can use the procedures in this section to help perform some initial checks and procedures that can solve basic device problems.

Before you begin the troubleshooting procedures, remember that improperly connected cables are often the source of connectivity or power problems. You should make a quick check of all the cable connections and ensure that they are secure. Additionally, you should also verify that the external peripherals connected to the device are functioning as expected:

- Is the Internet gateway device (router, DSL modem, or cable modem) that connects to the device working properly?
- Is the hub or switch that connects to the device working correctly?
- Are your workstations working properly?

**General Troubleshooting**

Use the following information to help you resolve basic device problems:

- The device is not receiving power.
  a. Ensure that a power cable is attached to the power connector on the device back panel.
  b. Disconnect the power cable from the electrical outlet.
  c. Reconnect the power cable to the electrical outlet. If the device is still not receiving power, plug the power cable into another electrical outlet.
- The default username and password do not work.
  - Ensure that the device is using the default settings. If you are unsure, reset the device to restore default settings and attempt to access the WebUI again. For details, see “Resetting the Device” on page 3.
  - Ensure that the username and password are correct. The username and password are case sensitive—ensure that Caps Lock is disabled and attempt to log in again.
- The WebUI wizard does not appear.
  - Ensure that the device is using the default settings. If you are unsure, reset the device to restore default settings and attempt to access the WebUI again.
  - Ensure that the PC you are using to access the WebUI is on the same subnet as the device.
- Ensure that the workstation you are using to access the WebUI is configured to receive an IP address (via DHCP) from the device, or uses a static IP address that is on the same subnet as the Trusted interface on the device.

- I have configured the device but can't reach the Internet.
  - Ensure that the cable connection to the device Untrusted port is secure and that the link light glows green.
  - Ensure that the device Untrusted interface is configured to receive an IP address via PPOE or DHCP, or is configured with an Internet routable static IP address and gateway.
  - Ensure that the external router connection is secure and active.
  - Ensure that the policies configured on the device do not prevent Internet access from the Trust zone.

- The WebUI does not appear.
  - Ensure that all cable connections to the device Trusted ports are secure.
  - Ensure that the workstation you are using to connect to the WebUI uses an IP address that is on the same subnetwork as the device.

- I cannot enable AV scanning.

  Ensure that the device is registered with Juniper Networks. You must register the device before you can obtain AV entitlement. If the device is registered when it first connects to the Internet, it automatically contacts the Juniper Networks Support site and obtains AV entitlement; if the device is not registered, it cannot obtain AV entitlement.

  You can still register the device after you have configured and connected it to the Internet, but you must manually set the device to contact the Juniper Networks Support site and obtain AV entitlement. For details on entitling your device for AV functionality, see the NetScreen Concepts & Examples ScreenOS Reference Guide.
You can restore the Juniper Networks factory default configuration of the device. Although resetting the device destroys all existing configuration, it safely restores access to the device.

You might need to restore defaults:
- If you experience problems during device configuration
- If you lose the admin password
- If you want to configure a device using RD. For details, see the Getting Started Guide for the NetScreen-Hardware Security Client.

**Warning:** Resetting the device deletes all existing configuration settings and renders existing firewall and VPN service inoperative.

To restore the device to its default settings:

1. Locate the reset pinhole on the back panel:

![Reset Pinhole](image)

2. Using a thin, firm wire (such as a paper clip), push the pinhole for four to six seconds and then release.
   - While pushing, the Status LED blinks amber once every second.
   - After releasing, the Status LED blinks green.
3. Wait one to two seconds.
4. Push the reset pinhole again for four to six seconds. When the Status LED blinks red, release.
5. The device resets to its original factory settings and restarts.

After the device starts up (should take about 30 seconds), ensure that the Power LED and Status LED both blink green.

If you do not follow the complete sequence, the reset process cancels without changing the configuration, and the Status LED blinks green.

If the device did not reset, an SNMP alert is sent to confirm the failure.
This chapter describes how to enable event messages on your NetScreen-Hardware Security Client. Event messages contain all available information about an event, and can help you locate and identify problems with the device.

You can use event log messages to help you debug device problems. The device event log monitors and records system events and network traffic, and contains an event message that displays the date, time, level, and description of each system event.

You can view the following types of event messages for your NetScreen-Hardware Security Client:

- **Alert**: Messages for multiple user authentication failures and other firewall attacks not included in the emergency category.
- **Critical**: Messages for URL blocks, traffic alarms, high availability (HA) status changes, and global communications.
- **Debugging**: All messages.
- **Emergency**: Messages concerning SYN attacks, Tear Drop attacks, and Ping of Death attacks.
- **Error**: Messages for admin login failures.
- **Information**: Any kind of message not specified in other categories.
- **Notification**: Messages concerning link status changes, traffic logs, and configuration changes.
- **Warning**: Messages for admin logins and logouts, failures to log in and log out, and user authentication failures, successes, and timeouts.

To view event messages on your device:
1. Start a Telnet client application to the IP address for the Trust interface.
2. Log in to the device.
3. At the command prompt, type: `get event`

For details on how to filter event messages, see the NetScreen CLI Reference Guide. For details on each event messages, see NetScreen Message Log Reference Guide.
Chapter 3 Enabling Event Messages