



NetScreen-Security Manager

Release Notes

Release: Forward Support for ScreenOS 5.4
7-18-2006

Contents

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Installation Instructions on page 3
- 4 Addressed Issues on page 4
- 5 Known Issues on page 4
- 6 Getting Help on page 6

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1817-000

1 Version Summary

This Forward Support package enables you to use Juniper Networks NetScreen-Security Manager to manage specific features on security devices running ScreenOS 5.4. NSM is a comprehensive security management solution designed to manage device, network, and security configuration for integrated firewall, intrusion detection and prevention, and virtual private network (VPN) appliances, sensors, and systems.

2 New Features

This Forward Support package provides the following levels of support for ScreenOS 5.4:

- **Full Support for the following features in ScreenOS 5.4:** “Full Support” enables you to manage devices using the new ScreenOS version. In addition, you can also configure all the new features in that version of ScreenOS.
 - Internal Antivirus Extended to the SSG Platforms
 - IDP Functionality
 - Wide Area Network Support: T1, E1, T3 interfaces
 - XAuth with Internet Key Exchange Mode Enhancements
- **Forward Support (Blended) for the following features in ScreenOS 5.4:** “Forward Support (Blended)” enables you to manage devices using the new ScreenOS version. In addition, you can also configure all the new features in that version of ScreenOS using Supplemental CLI.
 - External Antivirus
 - Integrated Web Filtering and Anti-spam Extended Support
 - DI Signature Pack Selection Enhancements
 - Configuring Next-Server-IP
 - Authentication
 - Hard Authentication Timeout
 - Source Interface Option for Domain Name Services (DNS)
 - General Packet Radio Service (GPRS)
 - Router Discovery Protocol
 - Passport Policy Support
 - Policy Based Routing
 - Virtual Systems Enhancements

- Voice Over IP Enhancements
- Wireless Enhancements
- **The following features in ScreenOS 5.4 are not supported:**
 - Internet Protocol Version 6 (IPv6)
 - Wide Area Network Support: ISDN interface

3 Installation Instructions

Install this Forward Support release with NSM 2006.1 only.

Forward Support for ScreenOS 5.4 Installation Files

The Forward Support for ScreenOS 5.4 installation package includes the following files:

- nsm2006.1_schema_update_server.zip
- nsm2006.1_schema_update_ui_win.zip
- nsm2006.1_schema_update_ui_linux.zip

Installing the Schema Update on the Management System

To install the schema update on the management system (standalone configuration - GUI Server and Device Server on the same computer):

1. Login to the management system computer as root.
2. Navigate to the directory where you saved the management system installer file and load the schema update file. It is recommended that you save the schema update file in the /tmp subdirectory.
3. Unzip the schema update. For example, type the following command:

```
unzip nsm2006.1_schema_update_server.zip
```

4. Run the schema update. For example, type the following command:

```
sh nsm2006.1_schema_update_server.sh
```

The update begins automatically. During the update process, the installer stops and restarts the management system.

If you are running NetScreen-Security Manager on a management system in the extended configuration - GUI Server and Device Server on separate computers, you must load and run the schema update on both computers where you have installed the GUI Server and Device Server. You can use the same procedure described previously to update the GUI Server and Device Server.

Installing the Schema Update on the UI

After you have installed the schema update, you must install the schema update on all your UI clients.

To install the schema update on the UI:

1. Login as an Administrator user on the computer where you are installing the UI.
2. Download the schema update file in the same location where you have installed the UI.
3. Unzip the schema update file.
4. Run the schema update.
 - a. If you are upgrading the UI on a Windows-based PC, then double-click on the installer executable.
 - b. If you are upgrading the UI on a Linux-based computer, then launch it from a command line using the following command:

```
sh nsm2006.1_schema_update_ui_linux.bin
```

Verifying that Forward Support is installed properly

To verify that you have installed forward support properly, view NSM UI client login window and verify that the installed version number is displayed. You can also use the Help menu option to view the installed patch version number.

4 Addressed Issues

None.

5 Known Issues

The following are known deficiencies at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:”.

- **27815/28053**—Updating a device with AV unsets some of the ICAP AV's configuration on the device (configured using supplemental CLI or directly on the device).
- **28607**—Regulatory domain appears incorrectly for SSG5/SSG20 wireless devices. This is a display issue on the UI only.
- **28627/29162**—ScreenOS 5.4 only allows to use loopback interface as the source interface for a unnumbered WAN interface. The NSM UI does not have this validation and allows you to select other interfaces as the source interface.
- **28837/28962**—Anti-Virus configuration appears in the UI for SSG devices running ScreenOS 5.4 when they do not have anti-virus license key.

W/A: Do not try to configure AV configuration on these devices, if you do not have an AV license key.

- **29026/29117**—ISDN interface can use PPP and multi-link PPP encapsulation. But the NSM UI allows other encapsulation methods such as frame relay.
- **29028**—New interface options introduced only for ISDN interfaces are not managed. NSM UI does not show these options.

W/A: Use supplemental CLI to configure these options.

- **29148/29247/29362**—MTU ranges for different types of interfaces are the same for all types of interfaces.
- **29154**—When configuring OSPF on a WAN interface, by default the NSM UI selects broadcast as the interface link type. This is wrong because WAN interfaces support point-to-point method only. Updating a device may display false verification errors due to this wrong selection. You need to explicitly select the point-to-point link type to make updates not show false errors.
- **29163**—NSM cannot change a sub interface's VLAN ID in device update when the interface has extended bandwidth setting configured.

W/A: Remove the extended bandwidth setting (for example, change the values back to 0, then update can change the interface's VLAN tag). After that, you can set the extended bandwidth setting to the desired values and do another update.

- **29211**—Update fails when changing the t1/e1 interface keepalive settings to non-default values, then moving the interface into null zone.

W/A: Before moving the interface into null zone, change the keepalive settings back to default.

- **29217**—For SSG5/SSG20 devices, the UI displays the wrong ADSL sub interface name format when adding a new ADSL sub interface. So you cannot use NSM to add an ADSL sub interface correctly.

W/A: Add the interface using CLI and then import the configuration.

- **29218**—T1 frame relay sub interface can have sub interface id from 0 to 32. But NSM allows you to configure higher id.
- **29226/29228/29229**—NS-5GT Wireless platforms running ScreenOS 5.4 introduces non-backward compatible changes in the ssid feature. When SSID configurations are imported, the encryption method may show as "none" on NSM and display a validation error. If you manually correct this problem by choosing an encryption method, updates may fail.

W/A: The best practice is to configure the feature using CLI and then import the configuration into NSM. Also, ignore the validation error on the none encryption method and leave it as empty. This way, update device can keep the configuration on the box.

- **29241**—For SSG5/SSG20 devices, the UI provides an empty zone list for wireless interfaces. This prevents you from configuring a wireless interface into any zone.

W/A: Set the zone of a wireless interface using CLI and then import the configuration.

- **29292**—DHCP is not supported on V92 and Aux interfaces on SSG5 and SSG20. But NSM shows the screen.

- **29300**—You can not create a dialer interface.

W/A: Use supplemental CLI to delete a dialer interface.

- **29326**—For SSG5/SSG20 devices, the UI only allows an ADSL interface to be put in untrust or null zone, while ScreenOS allows an ADSL interface to be in any traffic bearing zone such as trust or dmz.

W/A: Set the zone of an ADSL interface using CLI and then import the configuration.

- **29340**—An interface that is a member of a bgroup interface cannot configure its zone. It uses the zone of the bgroup interface. But NSM allows to configure the zone of the interface.

- **29373**—When modeling a 5GT device running ScreenOS 5.4 using a Trend Micro image, the default URL for AV signature update is wrong. You must manually set up the correct AV signature update URL.

- **29388**—When an ISDN interface is in trust zone, import the device and then do update, the update fails with false verification errors, complaining that it still wants to send CLI like: unset interface bri1/0 manage telnet unset interface bri1/0 manage web to the device. This only occurs when the ISDN interface is in trust zone.

W/A: When this problems happens, open the device, edit the ISDN interface, change the zone from trust to DMZ then change the zone back to trust. After this, update works properly.

- **29407**—A multi-link frame relay interface does not support NAT mode. It only supports Route mode. But NSM UI allows to select the NAT mode.
- **29408**—Multi-link frame relay interfaces do not support the secondary IP feature. But NSM shows the secondary IP screen.

6 Getting Help

For more assistance with Juniper Networks products, visit:

www.juniper.net/support

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your NetScreen device with Juniper Networks at the above web address.

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication 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 94089
U.S.A.

www.juniper.net

