Nipper – Juniper NetScreen, SSG and ISG Firewalls (ScreenOS)

Multiple Award Winning Security Software

Titania Nipper Version 2.6.2
Published November 2019

© Titania Limited 2019. All Rights Reserved

This document is intended to provide advice and assistance for the installation and running of Nipper software. While Titania takes care to ensure that all the information included in this document is accurate and relevant, customers are advised to seek further assistance from our support staff if required.
No part of this documentation may be copied or otherwise duplicated on any medium without prior written consent of Titania Limited, publisher of this work.
The use of Nipper software is subject to the acceptance of the license agreement.

Titania Limited
Security House
Barbourne Road
Worcester
WR1 1RS

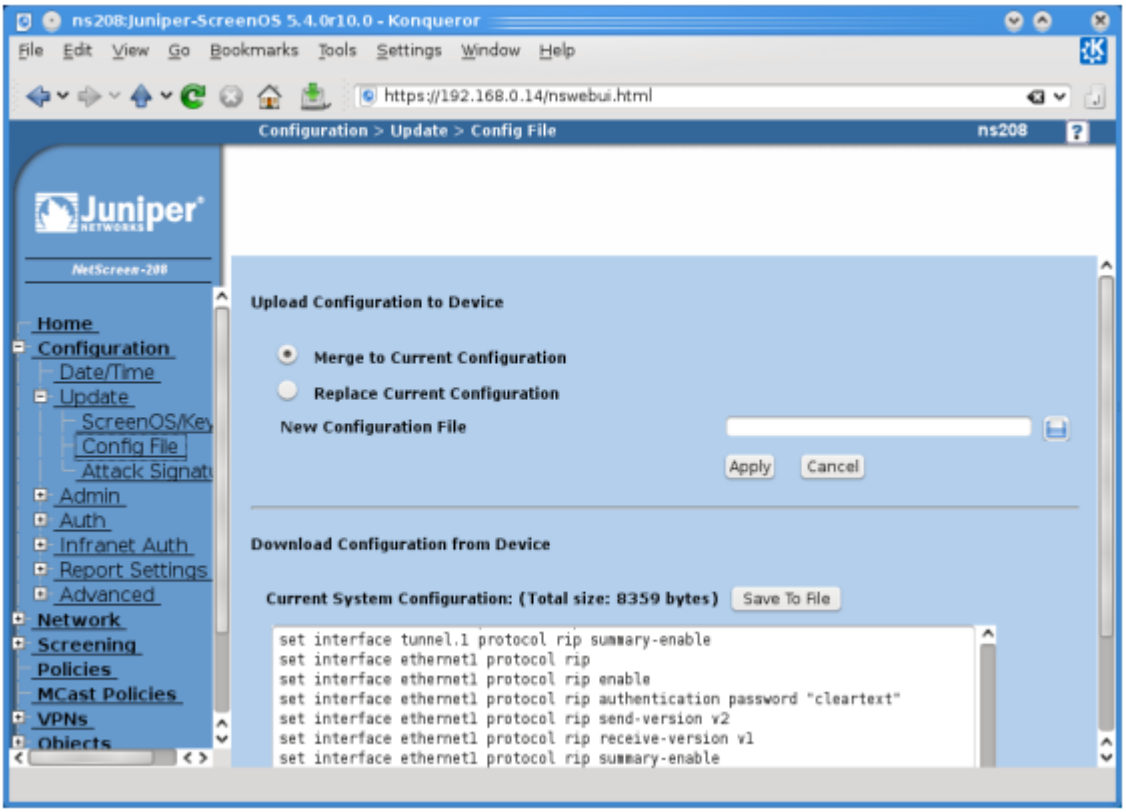
Telephone: (+44)1905 888 785
Technical Support: Support@titania.com
Licensing: Enquiries@titania.com
Nipper Support: https://www.titania.com/support/nipper-support/

There are several different methods of extracting the configuration from from your Juniper NetScreen device and this guide outlines three different methods.

Using HTTP(S)

We would recommend using HTTPS rather than HTTP for transferring your devices configuration as the latter provides no encryption. The procedure for getting the configuration from the device using HTTP(S) is as follows:

1. Using your favorite web browser, connect to the HTTP(S) service provided by your Juniper NetScreen device for remote management. You can do this by entering "https://" (recommended) or "http://" followed by your devices IP address.
2. Logon using your administration username and password. Juniper NetScreen devices default to using "netscreen" for the username and password.
3. Select from the menu on the right; "Configuration", then "Update" and finally "Config File".
4. Click the "Save To File" button to save the configuration to a local file.



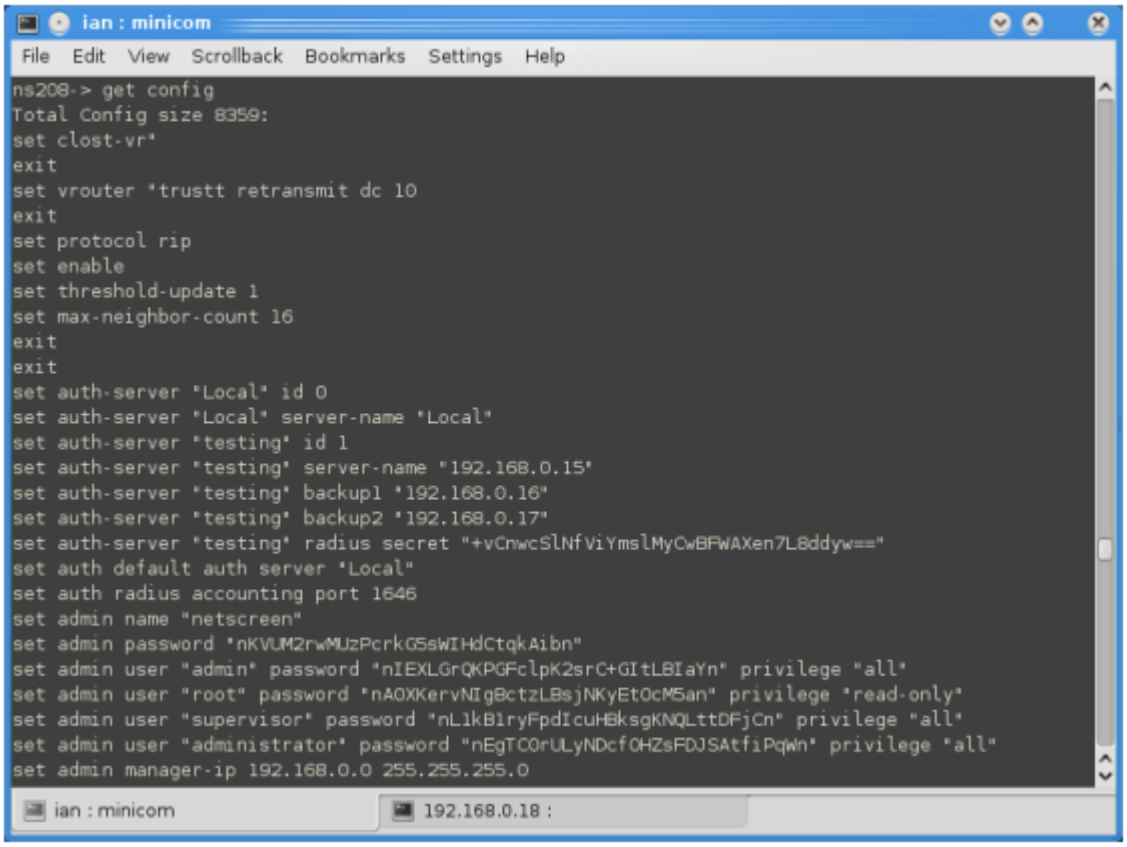
Using SSH, Telnet Or The Console

For this procedure you will be using the Command Line Interface (CLI) of your Juniper NetScreen device using an SSH client (such as OpenSSH or Putty), Telnet or through the console port. We would recommend using either SSH (for remote connections) or using a direct connection to the console port. Telnet provides no encryption of the communications and therefore your authentication credentials and configuration would be vulnerable if a malicious user were to monitor your connection.

1. Connect to the Juniper NetScreen using your favorite SSH client, Telnet or a direct console connection.
2. Logon using your administration authentication credentials.
3. Execute the following CLI command and capture the output (possibly using the cut and paste facility):

```
get config all
```

4. Save the captured output to a file and remove any visible page lines (i.e. --More--).



Using TFTP

We have included TFTP in order to be complete, but we don't recommend using this method for two reasons:

1. it provides no authentication;
2. it provides no encryption of the network communications.

However, if you want to make use of TFTP to transfer the configuration from your NetScreen device then the procedure is as follows:

1. Connect to the Juniper device using SSH, Telnet, ASDM, PDM or through a Console connection.
2. Login.
3. Transfer the configuration using the TFTP command:

```
save config to tftp <ip-address>:<filename> from interface
<interface>
```