

New Features for ScreenOS 2.6.1

This overview describes the following new features added to ScreenOS 2.6.1:

- [“Resetting the Device to the Factory Default Settings” on page 1](#)
- [“Automatically Creating a Bidirectional VPN Policy” on page 2](#)
- [“Disabling an Access Policy” on page 2](#)
- [“FIPS Certification” on page 3](#)

Resetting the Device to the Factory Default Settings

If the admin password is lost, you can use the following procedure to reset the NetScreen device to its default settings. The configurations will be lost, but access to the device will be restored. To perform this operation, you need to make a console connection, which is described in detail in the *NetScreen CLI Reference Guide* and the installer’s guides.

Note: By default the device recovery feature is enabled. You can disable it by entering the **unset admin device-reset** command. Also, if the NetScreen-100 is in FIPS mode, the recovery feature is automatically disabled.

1. At the login prompt, type the serial number of the device.
2. At the password prompt, type the serial number again.

The following message appears:

```
!!! Lost Password Reset !!! You have initiated a command to reset the device to
factory defaults, clearing all current configuration, keys and settings. Would
you like to continue? y/[n]
```

3. Press the **y** key.

The following message appears:

```
!! Reconfirm Lost Password Reset !! If you continue, the entire configuration
of the device will be erased. In addition, a permanent counter will be
incremented to signify that this device has been reset. This is your last chance
to cancel this command. If you proceed, the device will return to factory
default configuration, which is: System IP: 192.168.1.1; username: netscreen;
password: netscreen. Would you like to continue? y/[n]
```

4. Press the **y** key to reset the device.

You can now login in using *netscreen* as the default username and password.

Automatically Creating a Bidirectional VPN Policy

To allow both ends of a VPN tunnel to initiate traffic, the administrators at both gateway devices need to create inbound and outbound access policies. When the incoming/outgoing policies or todmz/fromdmz policies (NetScreen-10, -100, and -500) constitute a matching pair (that is, everything in the inbound and outbound policy configurations is the same except that the source and destination addresses are reversed), you can configure one policy and then select the **Create matching incoming (outgoing/toDMZ/fromDMZ) VPN Policy** check box to create a second policy automatically for the opposite direction. For the configuration of a new policy, the bidirectional VPN policy check box is cleared by default. For the modification of an existing policy that is a member of a matching pair, the check box is selected by default, and any changes made to one policy are propagated to the other. (Note that this option is only available through the WebUI.)

Disabling an Access Policy

With ScreenOS 2.6.1 and later, NetScreen provides a means for enabling and disabling access policies. By default, an access policy is enabled. To disable it, do the following:

WebUI

Policy >> Incoming | Outgoing | To DMZ | From DMZ: Select the **Disable** option from the Configure column for the policy that you want to disable.

The row containing the policy information is shaded grey to indicate that the policy is disabled.

CLI

1. set policy id <id_num> disable
2. save

Note: To enable the policy again, click **Enable** in the Configure column for the policy that you want to enable (WebUI), or type **unset policy <id_num> disable** (CLI).

FIPS Certification

The NetScreen-100 device complies with the Federal Information Processing Standards (FIPS) set forth by the National Institute of Standards and Technology (NIST). For further information on FIPS compliance and instructions on setting the NetScreen-100 in FIPS mode, see the *NetScreen-100 Cryptographic Module Security Policy*.
