

Juniper Networks

NetScreen Engineering notes for ScreenOS special release
5.2.0r3d

Product(s): NS-5000 MGT1, NS-5000 MGT2, ISG-2000, NS-500, NS-204, NS-208, NS-25, NS-50, NS-5XT, NS-5GT (Standard, ADSL), NS-HSC

Version: Engineering release 5.2.0r3d

Document version: V1

Date: 12-12-06

Note: This Engineering Note is an addendum to the ScreenOS 5.2.0r3 Release Notes. Additionally, this version of ScreenOS is based in ScreenOS 5.2.0r3c and may only be available until the next public mainline release which will contain these fixes. The notes below do not contain all included fixes, known issues and other information available in the mainline release notes. Therefore it should be used as an addendum to the current 5.2.0r3 release notes and previous engineering notes.

1. Addressed issue(s) in Special Engineering release 5.2.0r3d

Bug ID	Description
NSCcs04649	When using RADIUS Auth and local IP Pool, VPN users could receive the error message No more IP address in pool.
NSCcs06021	NSRP A/P transparent mode device may incorrectly handle VPN decrypted packets; causing the device to reload with an error.
NSCcs06410	FW device configured for NSRP in transparent mode may experience high CPU and/or reset with an error due to an incorrect session handling. [Reported in 5.0 and 5.3 Beta]
NSCcs07010	After a network re-route, DHCP relay performance could suffer.
NSCcs07030	Some L2TP connections using passwords could lead to device failure.
NSCcs07422	In some cases, large amounts of specific fragmented traffic could cause the device to reset
NSCcs11360	In some cases the NetScreen device failed to send the upstream load balancer device the correct MAC address upon a failover.
NSCcs11918	WebUI prompted error when adding/editing VSYS interface.
NSCos66805	Update internal Daylight Savings Time (DST) tables for new USA 2007 schedule