Juniper Networks

NetScreen Engineering notes for ScreenOS special release 5.2.0r3a

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, Wireless, ADSL), NS-HSC

Version: Engineering release 5.2.0r3a

Document version: V1
Date: 2-28-06

Note: This Engineering Note is an addendum to the ScreenOS 5.2.0r3 Release Notes. Additionally, this version of ScreenOS is based in ScreenOS 5.2.0r3 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 5.2.0r3a

Bug ID	Description
07033, 07490	Loopback interface can be set as source interface from cli or gui for Auth, but upon reboot, the command was removed from the config
07510	In some cases with DI enabled, an internal error caused the device to fail
07806	When adding or deleting an interface or sub-interface, packet drop was observed with high rates of multicast traffic
08164	In some cases a mishandled internally buffered packet caused the device to fail
08073	5.2.0r3 has an internal task which incorrectly increased the CPU usage
07472	In some cases phase 2 proposals were not cleanly releasing resources
07539	Removing a user did not take effect until the device was reset
08113	In some cases using 5.2.0r3 the device management would slow down after about an hour
07178	In some cases IPSEC sessions were not cleaned up in the session table
08032, 08184	Internal mishandling of radius traffic could cause the device to fail
07660	Passive FTP traffic was not being translated correctly
07928, 08301	Time stamp was incorrect in the Websense log report
08117	LDAP CRL retrieval was case sensitive
08178	Radius Auth via SSH would fail
07772, 08126	Internal mishandling of h323 traffic could cause the device to fail
08183	SSH login attempts stops debugging
08161	Syn cookie mechanism not working correctly on logical interfaces
07623	Inter vsys routing was not being handled properly
07913	Internal resources being held too long caused the device to fail
08077	Large number of VPN tunnels and traffic caused the device to fail
07753	Authentication resources were not being freed correctly and affecting administration