CISCO

Release Notes for Cisco RVS4000 4-Port Gigabit Security Router with VPN Firmware Version 1.3.0.5

6/15/2009

These Release Notes describe the new features and enhancements in the RVS4000 firmware version 1.3.0.5.

Contents

This document includes the following topics:

- **Changes Since RVS4000 Firmware Version 1.2.11**
- **Related Information**

Changes Since RVS4000 Firmware Version 1.2.11

New features were added, and problems were fixed.

New Features

The router's web-based configuration utility now has a new user interface based on the Cisco Small Business style.

Other Updates

The following problems were fixed in firmware version 1.3.0.5:

- In the VPN > Summary window, the VPN Tunnels Available field sometimes shows an incorrect number.

- The domain name cannot be entered in the Syslog Server field.

- Duplicate user names can be entered in the Router Access list.

- PPTP Passthrough on RVS4000 fails to interoperate with Cisco PPTP server.

- DHCPv6 server crash issue.

- IP-based ACL rules could prevent forbidden domains or keywords defined in the Firewall > Internet Access Policy window from functioning correctly.

- The router allows the saving of invalid LAN IP address.

- Users can configure and save an invalid character string in the Syslog Server field.

- Traceroute on the Administration > Diagnostics window does not check for valid input before executing the command.

- QuickVPN DoS vulnerability.

- In the Setup > LAN window, the drop-down menu does not list the netmask 255.255.255.252.

- DNS Cache Poison attack vulnerability.

  To avoid the DNS Cache Poison attack, RVS4000 now changes the DNS source port number randomly in the network address port translation.

Known Issues

The following are know issues in firmware version 1.3.0.5:

- QuickVPN Client running on Windows Vista cannot transfer more than 70MB of file to a remote RVS4000 over a QuickVPN tunnel before the tunnel disconnects. The issue will be fixed in the next firmware version which will be posted on cisco.com.

- Saving the configuration of port forwarding or port triggering rules causes the router to restart the firewall module which can cause a temporary lockup of the router for 10 to 15 seconds.

- QoS Rate Control has no effect when IPS is disabled. As a workaround, use QoS Priority instead.

- DHCP Relay is not supported when multiple VLANs are created.

- There is a known issue with Windows XP SP2 Firewall. ICMP packets are always dropped by the firewall when the firewall is enabled.

   This issue causes the QuickVPN client to be unable to establish a tunnel with the remote QuickVPN server successfully.

   Microsoft has released a patch to fix this issue, which you can get from:

   http://support.microsoft.com/kb/889527/en-us

   After you install the patch, the issue should be resolved. You can also fix this issue by upgrading Windows XP to SP3.

- IPS cannot block eMule 0.48a.

- During firmware upgrade, the router finishes loading the firmware and reboots before the progress bar shows 100% completion.

   It is recommended that you wait until the router finishes rebooting before attempting to access the router's web-based configuration utility.

Related Information

Support	
Small Business Support Community	www.myciscocommunity.com/community/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads, and enter the model number in the Software Search box.
Product Documentation	
Technical Documentation	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

OL-20177-01