Release Notes for the Cisco ISA500 Series Integrated Security Appliances Firmware Version 1.1.14

December 2012

These Release Notes describe important information and known issues for firmware version 1.1.14.

IMPORTANT:
As with any firmware release, please read these release notes before upgrading the firmware.

- You should install the latest available firmware when setting up a newly purchased device.
- Upgrade your firmware when a new version is available.
- As a standard practice, you should back up your configuration before any firmware upgrade.

Important Notes

- The ISA500 Series Configuration Utility supports the following web browsers:
  - Microsoft Internet Explorer 8 and 9
  - Mozilla Firefox 3.6.x, 5, and 6
- Please update the Anti-Virus and IPS signatures to the latest version when using the Anti-Virus and IPS features. For more information, see the *Cisco ISA500 Series Integrated Security Appliance Administration Guide* or the help pages for Security Services > Anti-Virus > General Settings and

Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection.

- The following Cisco AnyConnect Security Mobility Client Software versions are recommended with the ISA500 and are available on the Cisco ISA500 product documentation and software CD.
  - anyconnect-EnableFIPS-win-3.0.2052.exe
  - anyconnect-linux-3.0.2052-EnableFIPS.tar.gz
  - anyconnect-linux-64-3.0.2052-EnableFIPS.tar.gz
  - anyconnect-macosx-i386-3.0.4235-EnableFIPS.tar.gz
  - anyconnect-macosx-i386-3.0.4235-k9.dmg
  - anyconnect-predeploy-linux-3.0.2052-k9.tar.gz
  - anyconnect-predeploy-linux-64-3.0.2052-k9.tar.gz
  - anyconnect-win-3.0.2052-pre-deploy-k9.iso
- Some Firefox add-ons and plug-ins are incompatible with the firmware. If you are using Firefox, Cisco recommends disabling the following add-ons and plug-ins before installing firmware:
  - Adblock Plus (add-on)
  - bitcomentAgent (plug-in)
  - WinZipBar (browser toolbar)

Resolved Issues

Reference Number	Issues
CSCud08322	Fixed an issue in which spam filtering processes caused the ISA to reboot.
CSCud10160	Fixed an issue in which UPNP processes caused the CPU to run at 100 percent.

Reference Number	Issues
CSCud14009	Fixed an issue in which SSL VPN processes caused CPU to run at 100 percent.
CSCud17101	Fixed an issue in which blocked requests were missing from the Web Security Report.

Known Issues

The following table lists the known issues in version 1.1.14. As with any upgrade, review these known issues before upgrading the firmware.

Reference Number	Issue
	Remote users are sometimes unable to re-establish an SSL VPN session through AnyConnect v3.1.x after disconnecting from an earlier SSL VPN session. **Work Arounds:** ▪ Disable Idle Timeout or choose the maximum value in the range. ▪ Alternatively, use AnyConnect 3.0.2052, which is included on the DVD that was shipped with the security appliance.
CSCua43844	The Usage Report may display the public IP addresses instead of the private IP addresses on the LAN. Typically this issue occurs after topology changes, especially for WAN Interfaces.
CSCub91801	With AnyConnect 3.1.00496 or above releases, SSL VPN connection may fail during MTU renegotiation. **Work Around:** Change the MTU size to default value of 1500 on the PC.

Reference Number	Issue
CSCuc40174	Interaction between Spanning Tree Protocol (STP) and Cisco Discovery Protocol (CDP) can cause a traffic outage when STP blocks a port due to a physical loop in the network. **Work Around:** Remove the physical loop, or disable STP, CDP, or both features.
CSCuc47788	The Bandwidth Usage Report by IP Address displays the server's public IP address instead of the SSLVPN client's IP address.
CSCuc89697	Sometimes a mobile phone using AnyConnect Mobile Client loses connectivity. **Work Around:** Disable the client dead peer detection by entering 0 for the Client DPD Timeout value on the VPN > SSL Remote User Access > SSL VPN Configuration page.
CSCud06033	When the VRRP priority is changed, the update is not sent to the PC. For example, after adjusting the priority to make one router act as a backup, both routers may act as the master. **Work Around:** Disable STP.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc

Cisco Small Business Firmware Downloads	www.cisco.com/go/isa500software
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Documentation	
Product Documentation	www.cisco.com/go/isa500resources
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

78-21079-02 Jan. 2013