Release Notes for the Cisco ISA500 Series Integrated Security Appliances Firmware Version 1.2.15

May 2013

These Release Notes describe important information and known issues for firmware version 1.2.15.

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 versions 8, 9, and 10
  - Mozilla Firefox versions 3.6.x, 4, 5, 6, and 17
  - Google Chrome version 23
- 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)

Enhancements

- Enhanced browser support. The currently supported browsers are listed in **Important Notes**.
- Improved logging to include more details for IPSec and WAN PPPoE connections. (CSCub20624)
- Added support for IPS hardware acceleration to improve performance. On the Security Services > Application Control > Application Control Settings page of the configuration utility, you can check the **Enable Hardware Acceleration** box to enable this feature, or uncheck the box to disable it.
- Added blocked signature IDs to the IPS security report. (CSCud13136)

- Added default policies for QoS to make it easier to manage the QoS settings. The user can use the Cisco-recommended policies or can customize them as needed. (CSCty43583)
  - WAN Queue Settings: By default, WAN outbound QoS is configured with Low Latency Queuing (LLQ). Default bandwidth percentages are provided for each queue. The default queue descriptions identify the traffic selectors that are assigned to each queue.
  - Traffic Selector (Classification): Several default Traffic Selectors are configured and are assigned to priority queues. These include Voice, Signaling, routing/VPN Control, Management, Video, and Best Effort.
  - QoS Policy Profile: A default WAN_POLICY is provided and is active on the enabled WAN interfaces.
- Reorganized the listings of applications on the Application Control Policies > Policy Profile Add/Edit page for easier use. After a category is selected, the screen displays an alphabetized list of applications to configure. (CSCtx66551)
- Enhanced the Networking > VRRP page to allow the administrator to enable or disable VRRP preemption. With preemption enabled by default, VRRP chooses a new master any time a router comes online with a higher Priority value than the current master virtual router, even if the master has not failed. If you disable preemption, VRRP chooses a new master only if the current master fails or the original master recovers from a failure. Check the **Enable pre-empty** box to enable this feature, or uncheck the box to disable it. (CSCtx35944)

Resolved Issues

Reference Number	Issues
CSCtr33978	Fixed an issue in which Split Tunneling settings were not correctly saved after the user made changes.
CSCtr58067	Fixed an issue in which the configuration utility did not detect the entry of a duplicate DHCP IP Reservation.

Reference Number	Issues
CSCtr58068	Fixed an issue in which the Status > Interface > DHCP Bindings page did not display a successfully configured DHCP IP Reservation address.
CSCtr76810	Fixed an issue in which a Google Chrome user was unable to editing a profile on the Security Services > Web URL Filter > Policy Profile page.
CSCtu35596	Fixed an issue in which Captive Portal monitored HTTPS requests only through port 443. Other ports can be configured for use.
CSCua30749	Fixed issues with VRRP not always switching correctly between master and backup routers.
CSCub91801	Resolved an issue with SSL VPN connections failing during MTU renegotiation when using AnyConnect 3.1.00496 and later releases.
CSCuc33541	Fixed a QoS issue in which an outbound QoS profile was applied to inbound traffic.
CSCuc47788	Corrected the Bandwidth Usage Report by IP Address to display the SSLVPN client's IP address instead of the server's public IP address.
CSCuc89697	Fixed an intermittent issue with loss of connectivity from mobile phones using AnyConnect Mobile Client.
CSCud06033	Resolved an issue VRRP priority changes were not handled correctly.
CSCud13727	Resolved a certificate issue that occurred when using the Setup Wizard to configure HTTPS-only Remote Management.

Reference Number	Issues
CSCue60607	Fixed an issue in which some users could not upgrade firmware through their Cisco.com accounts due to permissions issues for encrypted images. Now when this situation occurs, the user interface provides a descriptive message and a link for registration.
CSCue74463	Corrected a system message that contained incorrect information about VPN configuration. Multiple site-to-site VPN tunnels are supported.
CSCue76832	Fixed an issue in which a site-to-site VPN tunnel failed if one of the routers was behind Network Address Translation.
CSCuf81594	Fixed an issue in which a teleworker VPN connection to a Cisco IOS router disconnected after 24 hours.

Known Issues

The following table lists the known issues in version 1.2.15. As with any upgrade, review these known issues before upgrading the firmware.

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:** Disable CDP for ports belonging to STP-enabled VLANs.
CSCuf85568	Daylight Savings Time is not activated on the correct schedule for time zones outside the United States.
CSCug09224	After the Packet Capture utility is used, the log incorrectly indicates that tcpdump failed.

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

78-21234-01