Release Notes for SA 500 Series Security Appliances Firmware Version SA500-K9-1.1.42

April 15, 2010

These release notes describe the known and resolved issues in firmware version SA500-K9-1.1.42.

Contents

This document includes these topics:

Recommended Practices

Recommended Upgrade Steps

When upgrading from version 1.0.15, 1.0.17, or 1.0.39, the firmware will reset the router to its factory default and you will need to back up the configuration. When upgrading from 1.1.21, these steps are not required.

CAUTION Do not try swap images if a secondary firmware image is not present. Doing so can cause the to router to not boot up.

To upgrade the SA 500 follow these steps.

STEP 1 Back up the existing configuration using the SA 500 Configuration Utility.

If you need to revert to the previous firmware version, this allows you to restore the configuration associated with the prior version.

To access the configuration back-up options, click **Administration** on the menu bar, then click **Firmware & Configuration > Network** in the navigation tree.

Follow the instructions in the *Cisco SA 500 Series Security Appliances Administration Guide* to back up the configuration.

STEP 2 Write down or take screenshots of your existing configuration settings. After upgrading to firmware version SA500-K9-1.1.42, you must manually re-enter these settings by using the SA 500 Configuration Utility.

This is necessary because the SA 500 is reset to factory defaults as part of the upgrade process and the previous configuration back-up file format is incompatible with the format required for firmware version SA500-K9-1.1.42.

STEP 3 Perform the upgrade by using the Configuration Utility. To access the upgrade options, see the **Upgrade Firmware** section of the Getting Started (Basic) page of the Configuration Utility.

STEP 4 Manually re-enter the configuration settings you recorded in Step 2.

STEP 5 Verify that the installation is working properly.

If the upgrade is not successful, you can revert to the previous firmware version and restore the configuration from the backup that you created in Step 1.

Limitations and Restrictions

These are the limitations and restrictions for the SA 500. These are known limitations that will not be fixed and there is not always a workaround.

- When performing a factory default reset, the updated IPS signatures (newer than the image's built-in signatures) are erased and fall back to the built-in signature in the image.

  The workaround is to reinstall the latest signatures.

Important Notes

These are important notes related to firmware version SA500-K9-1.1.42.

- If the LAN LEDs remain down for more than 10 minutes, or if the Diagnostic LED is up, press the reset button (with the router powered on) for 10 seconds and release. During that time, do not power off the device.
- Upgrading the firmware over wireless or over slow internet connections is not recommended. When upgrading, always connect to the LAN. Do not exit the browser window or interrupt the process in anyway until the operation is complete.

Known Issues

The following table lists the known issues in firmware version SA500-K9-1.1.42.

Ref Number	Description
CSCtc15599	The router's optional port cannot be configured in VLAN trunk mode (Only applies to the SA 540). **Symptom** Changing the optional port from Access mode to Trunk mode does not allow traffic to pass though. **Workaround** Use other LAN ports for VLAN trunking.
CSCtd83237	Firewall rules and positions in the Available Firewall Rules table are not the same number. **Symptom** Index numbers begin counting with 0 (zero), and positions begin counting with 1 (one). This can cause confusion when using the "Move to *<index number>*" button. **Workaround** Use the **Move Up** button to move the rule up the list.
CSCte60926	Unable to access IPv6 internet addressing when using 6 to 4 automatic IPv6 tunneling. **Workaround** None.
CSCtf07090	A "server is down" error message sometimes appears when ProtectLink Web threat protection is set to high. **Workaround** None.

Ref Number	Description
CSCtf07567	Sometimes there is no audio for a voice call, when a UC 500 is behind the router. **Symptom** The UC 500 sends out 2 C lines (media and session level addresses) in the SIP header, but the router only translates the media level address. **Workaround** Configure the UC 500 to send only the media level addresses in the SIP header by entering these commands from the CLI: voice class sip-profiles 1 request ANY sdp-header Connection-Info remove response ANY sdp-header Connection-Info remove ! voice service voip sip sip-profile 1
CSCtf37764	Bandwidth profiles do not restrict the following: ▪ HTTP traffic when content filtering is enabled ▪ Passive FTP sessions **Workaround** For HTTP traffic, disable content filtering. For passive FTP sessions, there is no workaround.
CSCtf40495	After modifying the default VLAN IP and DHCP pool addresses, sometimes the PC cannot obtain a DCHP address. **Symptom** The PC connected to the LAN port can no longer obtain a DHCP address, even after release/renew or by plugging and then unplugging the power cable. **Workaround** Configure a static IP address in the newly configured network to regain access to the router. For example, if you changed your default VLAN to 192.168.10.x, you will then need to configure a static IP address for your PC to 192.168.10.5.
CSCtf58458	SSL VPN tunnel installation sometimes fails on certain Windows 7 Home Premium 64-bit PCs. **Symptom** An error message occurs during an SSL VPN tunnel adapter installation. **Workaround** None.

Ref Number	Description
CSCtf62341	If you cannot establish an SSL VPN tunnel, this might indicate that the previous VPN client did not uninstall correctly from your PC. **Workaround** Clean up the previous client installation by following these steps: ▪ In Internet Explorer, on the **Tools** menu, click **Internet Options**. ▪ On the **General** tab, click **Settings**. ▪ Click **View Objects**. ▪ Delete all object files then relaunch the browser. If this workaround does not resolve the problem, do the following: ▪ Click **Start** and then click **Control Panel**. Double-click **System**. ▪ On the **Hardware** tab, click **Device Manager.** ▪ Double-click Network Adapters**.** Right-click the **Vpn Tunnel ssldrv** adapter and click **Uninstall.** ▪ Restart your system.
CSCtf63339	The interface statistics for Tx Pkts (send) and Rx Pkts (receive) are not accurate between LAN and WAN. **Workaround** None.
CSCtf72391	Voice is not supported on the DMZ interface. **Workaround** None.

Resolved Issues

The following table lists the problems that were fixed in firmware version SA500-K9-1.1.42.

Ref Number	Description
CSCtd92770	BYE messages are blocked by the router from the WAN and LAN if the call is longer than 3 minutes.
CSCte53632	When configuring remote management for SSL VPN, remote access for QuickVPN will not work properly.
CSCte62822	The IPS license expiry date only shows the expiration period of the current license. It does not show the cumulative expiry date when multiple licenses are installed.
CSCte62836	Enabling Universal Plug and Play (UPnP) causes a memory leak.
CSCte84080	QuickVPN client on Windows 7 behind NAT does not work properly.
CSCte84080	QuickVPN client cannot connect to server again once the connection is lost.
CSCte84127	The router locks up when multiple IPSec tunnels are added.
CSCte91638	SSL VPN does not work when running Windows 7 Home Premium 64-bit.
CSCte93076	The router's IPSec tunnels go down sometimes and do not come back up.
CSCte93153	Remote desktop sessions intermittently don't work when site-to-site VPN is connected.
CSCte93163	Intermittently, PPPoE does not work on optional WAN port.
CSCte95846	WAN and optional port LEDs take some time to come up after the router connection is established.
CSCte99377	If you swap images when there is only a single image present, the router fails to boot up, even if there is no secondary image on the flash.
CSCte87995	Automatic signature updates fail after certain retries. When this occurs, the GUI is grayed out and reports that IPS is not enabled
CSCtf40932	Auto-Rollover does not work under certain conditions.
CSCtf57792	IPSec VPN is not stable after rebooting the router.

Release Notes

Ref Number	Description
CSCtf58467	Redundant VPN gateway does not work when the primary tunnel fails.
CSCtf58471	IPS Peer-to-Peer (P2P) detect and prevent does not block access to the BitTorrent application.
CSCtf58475	The router crashes sometimes when connected to a Tandberg C20 system.

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/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Small Business Products. No login is required. Downloads for all other Cisco Small Business products are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
Open Source Publication Tarball link Offer Letter	ftp://ftp-eng.cisco.com/pub/opensource/smallbusiness/sa500/1.1.42/readme_OpenSource_Offer.rtf
Quick VPN Software	www.cisco.com/go/qvpnsoftware
Product Documentation	
SA 500 Technical Documentation	www.cisco.com/go/sa500resources
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

OL-20046-01