Release Notes for the Cisco 7600 Wireless Security Gateway, Release 4.4.8

January 2017

This document explains features, requirements, and caveats for the Cisco 7600 Wireless Security Gateway (WSG), Release 4.4.8.

Contents

This document has the following:

Features

The WSG is a high-density IPSec gateway for mobile wireless carrier networks. IP Security (IPSec) is an open standards set. IPSec gives confidentiality, integrity, and authentication for data between IP layer peers. The WSG uses an IPSec-protected tunnel to connect outside endpoints.

The WSG runs on the Cisco Service and Application Module for IP (SAMI), a new-generation high performance service module for the Cisco 7600 series router platforms.

For more information about the WSG, see the *Cisco 7600 Wireless Security Gateway Configuration Guide, Release 4.4.8*. For more information about the Cisco SAMI, see the *Cisco Service and Application Module for IP User Guide*.

WSG Release 4.4.8 supports the following features:

Cisco Systems, Inc.
www.cisco.com

- Minor enhancement to detect the PPC-IXP HM failure within 15 seconds.
- Minor enhancement to allow user to configure HA timeout value.
- HA_TRACE file enhancement.
- Minor enhancement to generate SNMP trap if authentication failures are found during decryption of encrypted packets.
- Support to generate SNMP trap on configured tunnel creation/deletion rate.
- Support to Configure the Facility parameter in the syslog messages.
- Asymmetric division of clear traffic between 2 IXPs.
- Both TCP and HTTP are supported as CMPv2 Transport protocols.
- DHCPv6 address allocation.
- IKEv2 redirect.
- High Availability Active-Active Redundancy Mode.
- Path MTU.
- SSH authentication using RADIUS.
- Reverse DNS lookup for IKE peers.
- S2S blacklisting.
- IPv6.
- Virtual Routing and Forwarding (VRF).
- Data Plane Routing.
- SSH server.
- Per Peer IP tunnel debug.
- Reverse Route Injection (RRI).
- Peer authentication through EAP-MD5, EAP-AKA and EAP-SIM.
- RADIUS Accounting.
- Traffic-based Phase 2 rekey.
- Blacklisting remote peer.
- Multiple IKE proposals.
- Multiple DH groups, EAP authentication algorithms, and transform sets.
- DHCP address allocation.
- High Availability Active-Standby Redundancy Mode.
- Site-to-Site scalability improvements.
- Certificate Management Protocol.
- Online Certificate Status Protocol.
- IKEv1 and IKEv2 and Public Key Infrastructure (PKI).
- Both remote access and site-to-site type profiles cannot be used in combination on a SAMI.
- The DPD initiation feature allows the WSG to send DPD to peers at a regular interval. This allows WSG to detect and remove dead connections or peers.
- WSG supports the extended form of traffic selectors.

- Multiple Child SAs—For a single IKE association with a peer, multiple child IPSec SAs can be created, each with its own traffic selector rules.
- DNS to AP feature allows the WSG to pass the DNS server IP address to the remote peer.
- The WSG supports platform traps for PPC CPU congestion and memory exhaustion.
- The OAM traffic routing feature allows the WSG to do static routes on the PPC to carry OAM traffic directly to a local network through a VLAN interface.
- Single Entity configuration allows you to configure the SAMI from a single login interface rather than going to each of the 6 PPCs individually and configuring them.
- All traps, syslog and SNMP stats are sent from a single PPC. For SNMP stats, the external SNMP manager goes to the single PPC to retrieve stats for all the PPCs.
- The PPC Traffic Throttle feature, throttles the number of IKE INIT messages sent to the PPC. This prioritizes the DPD traffic over new tunnel requests, and allows existing tunnels to remain intact.
- WSG supports debugs using the CLI.
- Diffie-Helman (DH) Groups 14, 15, 16, 17, and 18 are added to groups 1, 2 and 5.
- WSG adds Extended Sequence Number (ESN) support as longer lifetimes are expected in customer deployments. Additionally, higher traffic is expected in site-to-site setups. Extended Sequence Number (64 bit sequence number) implementation is required in such cases.
- Processes Internet Key Exchange version 2 (IKEv2) initialization requests from endpoints.
- Creates IPSec tunnels.
- Exchanges information with endpoints.
- Authenticates endpoints.
- Assigns IP addresses to endpoints.
- Does cryptographic algorithm negotiation.
- Rekeys security associations (SAs).
- Does traffic selector negotiation.
- Supports network address translation (NAT) traversal.
- Encrypts, decrypts, authenticates, encapsulates, and decapsulates packets.Capacity and performance limit recognition, providing system wide throughput capacity characteristics and helping to identify the traffic load for future expansion.
- Fresher IKE/IPSec statistics will be delivered via SNMP. In earlier releases, the same statistics could be up to 10 minutes stale. Now user can configure the freshness to be adjusted dynamically based on number of SAs, or be set to a fixed interval between 1 and 300 seconds.
- Load balancing in support of 100% uni-directional ESP or clear traffic.
- Upgrade support from release 3.1.1. to release 4.x.
- Performance and throughput indicators to provide system wide throughput capacity characteristics of WSG.
- Persistent IKE/IPSec tunnel index for SNMP during a tunnel’s lifetime.

Requirements

For hardware requirements, such as power supply and environmental requirements, as well as hardware installation instructions, see the *Cisco Service and Application Module for IP User Guide*.

WSG Release 4.4.8 software application ships preloaded on the Cisco SAMI processors with fully-functional default settings. During an image upgrade, the image is automatically loaded onto each SAMI processor.

WSG Release 4.4.8 requires the following hardware and software:

- Any module with ports connected to the network.
- Cisco 7600 Series Supervisor Engine 720 (WS-SUP720-3BXL) with a Multilayer Switch Feature Card 3 (WS-SUP720) or Policy Feature Card 3 (WS-F6K-PFC3BXL) running Cisco IOS Release 12.2(33)SRC or later,

  or

  Cisco Supervisor Engine 32 with a Multilayer Switch Feature Card 2A (MSFC2A) or Policy Feature Card 3 (PFC3B) running Cisco IOS Release 12.2(33)SRC or later.

  The Cisco Supervisor Engine 32 requires LCP ROMMON version 12.2[121] or later on the Cisco SAMI.

  For details on upgrading the Cisco IOS release running on the SUP, refer to the "Upgrading to a New Software Release" section in the Release Notes for Cisco IOS Release 12.2SR.

  For details on verifying and upgrading the LCP ROMMON image on the Cisco SAMI, refer to the *Cisco Service and Application Module for IP User Guide*.
- Cisco Service and Application Module for IP (Cisco Product Number: WS-SVC-SAMI-BB-K9) with the 2 GB memory option (Cisco Product Number: MEM-SAMI-6P-2GB[=]).

To find out which IOS version your system is running, log in to the SUP and enter the **show version** command.

To find out which WSG version your system is running, establish a session with a PPC, and enter the **show version** command.

Caveats

Caveats are unexpected behavior in Cisco software releases. Severity 1 caveats are the most serious caveats, Severity 2 caveats are less serious, and Severity 3 caveats are moderate. Typically, only Severity 1, Severity 2, and select Severity 3 caveats are included in the caveats lists.

If you have an account with Cisco.com, you can use the Bug Navigator II tool to find the current list of caveats of any severity for any software release. To access the Bug Navigator II tool, go to http://www.cisco.com/support/bugtools.

WSG Release 4.4.8—Open Caveats

The following caveats are unresolved and newly opened in this release:

- CSCvc32967—when enabling multiple debugs commands, its not showing in "Show debug cryprto" cli cmd.

Description: The "**show debug crypto**" CLI command output does not show that multiple debug commands are enabled. However, there is no functional impact in enabling multiple debug commands.

Workaround: None.

- CSCvc39008—"show crypto throughput" show diff values across WSG PPCs

  Description: The "**show crypto throughput**" CLI command shows different values across SAMI WSG PPCs.

  This condition occurs when different PPCs are used in remote-access mode,

Workaround: None.

Open Caveats Prior to WSG Release 4.4.8

The following caveats are unresolved in this release:

- CSCus87746—DHCP relay function not working with VRF on SAMI

  Description: DHCP relay function is not working on SAMI card.

  This condition occurs when VRF is configured.

  Workaround: Remove VRF configuration.

- CSCut40563—WSG: PPC4 alone is missing when polling “hrProcessorLoad” on SAMI

  Description: PPC4 alone will be missing when a snmpwalk is done for “hrProcessorLoad” on WSG.

  This issue is specific to Active-Active scenario wherein the primary Active PPC4 SAMI is reloaded, and once it comes back after the SYNC is successful between the Active PPC4 and Standby PPC4, the issue is seen with the standby PPC4.

```
Node#  /opt/local/bin/snmpwalk -c <> -v 2c -r 0 -t 10 <IP add>1.3.6.1.2.1.25.3.3.1.2
host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad.274727680 : INTEGER: 2
-> PPC3
host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad.278921984 : INTEGER: 1
-> PPC5
host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad.281019136 : INTEGER: 3
-> PPC6
host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad.283116288 : INTEGER: 3
-> PPC7
host.hrDevice.hrProcessorTable.hrProcessorEntry.hrProcessorLoad.285213440 : INTEGER: 3
-> PPC8
```

  This condition occurs on WSG with Active-Active scenario with below mentioned conditions:

  - Active-Active on WSG
  - Primary Active PPC4 reloads
  - Comes Backup as Active

  Now, PPC4 will not report to SNMP polling for “hrProcessorLoad”.

  Workaround: Reloading only the affected WSG.

- CSCug93071—An Invalid IPV6 address can be configured for gateway

  Description: The gateway address should be verified as routable before being accepted. If it fails then an error code should be returned.

  Workaround: None.

- CSCug79787—crypto ipsec-fragmentation configuration issue

Description: Following configuration issues observed in crypto ipsec-fragmentation configuration.

- User unable to know the default path MTU since both following configuration are consider as default but not in running configuration, though the configuration successful.
- After crypto ipsec-fragmentation none configured and saved to start configuration, then after sami reload, then new tunnel established, the path MTU is 1400 instead 0.
- Path MTU is changed in CLI output but function does work for existing tunnel.

Workaround: None.

- CSCtw67551 — SNMP walk of the ipv6 Interface table doesn't return any information

  Description: WSG doesn't provide ipv6 interface and address information via SNMP get or snmpwalk. This is seen with ipv6 interface and address information.

  Workaround: None.

- CSCtz68085 — PMTU set to 0 when CLI "no cry ipsec-fra be MTU 1300" applied on WSG

  Description: This issue may be observed when the above mentioned CLI is executed on the WSG instance. Upon execution:

  - It allows sending the traffic up to size 1300.
  - Traffic gets dropped and no error is reported when the traffic size is between 1300 and 1400.
  - "Destination un-available (Fragmentation needed) error is reported when the traffic size exceeds 1400

  Workaround: It is possible to mitigate this issue by reconfiguration.

- CSCtr89117 — Observe the softirq-timer stack trace while WSG is idle

  Description: This issue may be observed when WSG is in the idle state and no profile is selected. In some scenarios following trace is observed:

  [7ffc9d00] [40005cc0] show_stack+0x58/0x198 (unreliable)

  [7ffc9d50] [40287488] yield+0x54/0x68

  [7ffc9d60] [401abe2c] netlink_broadcast+0x32c/0x35c

  [7ffc9db0] [401ac45c] nlmsg_notify+0x60/0xa0

  [7ffc9dd0] [401a36b4] rtnl_notify+0x48/0x58

  Workaround: None

WSG Release 4.4.8—Resolved Caveats

The following caveats are resolved in WSG Release 4.4.7:

- CSCuy31639—Disabling qconn process in WSG-SAMI xscale

  Description: In a rare occurrence, QNX QCONN process crashed and SAMI card had reloaded. QCONN core was seen in the LCP core directory after the SAMI restarted.

- CSCuy95677—Nitrox always fragments the IPv6 packets to 1400

  Description: Nitrox was fragmenting the IPv6 packets to the default IPv4 MTU (1400) fragmented value or with the configured IPv4 fragment value. For example, when both the IPv4 and IPv6 fragment MTUs were set to 1500 and 1600 respectively, Nitrox was fragmenting the IPv6 packets with IPv4 MTU value (1500). And, when only the IPv6 fragment MTU was set, the Nitrox fragmented the IPv6 packets with default IPv4 value (1400).

- CSCva67189—R3.1.1 SAMI WSG eNB unable to pass traffic with IPSec auth failures

  Description: When the faulty enodeB (with hmac error) was connected to the SAMI WSG, the ESP packets were dropped reporting authentication decryption failures, not only for the faulty peer but for other peers too, which were working appropriately before they were connected to the faulty enodeB.

- CSCvc15732—WSG crashes due to mem leak during "Could not export IKE SA"

  Description: Due to improper handling of error condition “Could not export IKE SA”, the WSG leaked small amount of memory over a period of time leading it to reload.

- CSCvc46840—SAMI : crypto profile configuration on WSG module missing after upgrade to sw 4.4.7

  Description: Part of the SAMI configuration was erased without any external intervention. The SAMI module was active and all sites connected to it were reported to be down. All crypto profile information were missing. Reloading the module fixed the issue and the card retrieved all the configurations from the RSP bootdisk.

Resolved Caveats Prior to WSG Release 4.4.8

The following caveats were resolved in WSG Release 4.4.7:

- CSCuv56122—SAMI should reload when Nitrox error happens on Itasca baseboard

  Description: The following error appears on SUP syslog indicating a Nitrox failure:

  ```
  ERROR: Failure to read SA from nitrox
  ```

  This condition impacted traffic and service.

- CSCuz79833—IKE create exports fail on Active SAMI WSG caused redundancy insync

  Description: Count of IPSec tunnels differed between Active and standby WSGs. Error counters incremented in "**show crypto ha stats**". The following error message was found in syslogs/show eventlog:

  ```
  ERROR: Could not export IKE SA
  ```

  This condition is dependent on customer environment and also when redundancy is configured.

The following caveats were resolved in WSG Release 4.4.6:

- CSCux12961—WSG 4.x "service interface vlan" limit of only 10 - more loopbacks need

  Description: Cannot use more than 10 service VLAN interfaces - loopback interfaces. There was no such limitation in WSG 3.x. While upgrading to WSG 4.x, the VLANs exceeding 10 service VLAN interfaces are placed in shutdown state after configuration migration. The exceeding VLANs were not saved in startup-config.

  The following error is seen if "**no shutdown**" the service VLAN interface is attempted:

  ```
  ERROR: exceed the maximum number of service vlan interfaces: 10
  ```

  This condition was seen while upgrading from WSG 3.x to 4.x and, when more than 10 VLAN interfaces with loopback /32 ip addresses are used before migration.

- CSCux02981—WSG CLI "no service interface vlan x" removes interfaces later in config

  Description: After removing an interface with **no service interface vlan <*x*>**, all the subsequent interfaces are also deleted. However, the IP addresses of the deleted interfaces responds to the ping and the VPNs using them as source works fine.

The following caveat was resolved in WSG Release 4.4.5:

- CSCuv99544—Sub commands under 'service interface' lost after reload of WSG r4.4.4

  Description: All sub-commands under **service interface** are lost after reload.

  This condition occurs if VRF/MTU configuration exists under **service interface vlan**.

The following caveats were resolved in WSG Release 4.4.4:

- CSCte53922—Show logging internal facility command causes SAMI reset

  Description: SAMI card reset occurs after command execution.

  This condition occurs when at the SAMI LCP CLI prompt, the command **show logging internal facility** is executed.

- CSCut62112—WSG encoding v1/v2 Trap OID values incorrectly

  Description: WSG encodes v1/v2 Trap OID values incorrectly.

  All Enterprise trap OIDs were affected by this issue.

The following caveats were resolved in WSG Release 4.4.3:

- CSCus69649—Evaluation of glibc GHOST vulnerability - CVE-2015-0235

  Description: On January 27, 2015, a buffer overflow vulnerability in the GNU C library (glibc) was publicly announced. This vulnerability is related to the various gethostbyname functions included in glibc and affect applications that call these functions. This vulnerability may allow an attacker to obtain sensitive information from an exploited system or, in some instances, perform remote code execution with the privileges of the application being exploited. This vulnerability is documented in CVE-2015-0235.

  A Cisco Security Advisory has been published to document this vulnerability at:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150128-ghost

- CSCus58367—WSG picks up wrong profile if multiple profile types are configured

  Description: When EnB requests for PSK profile, WSG picks up RSA profile instead of PSK leading to failure in tunnel negotiation.

- CSCuc65113—LCP Sysmgr Crash Due To Proc Mem Info Corruption

  Description: Core Dump File will have Proc Memory Info details.

  LCP Sysmgr had crashed due to Proc Memory Info corruption.

The following caveat was resolved in WSG Release 4.4.2:

- CSCur93648—High CPU due to multiple vsh.bin processes

  Description: WSG CPU on SAMI gets overwhelmed with abrupt terminations of script, and thereby hogging up the CPU.

  This issue is seen on WSG running 4.4.

The following caveat was resolved in WSG Release 4.4.1:

- CSCur43484—CLI implementation to manually configure the Facility level

Description: Feature support to Configure the Facility level parameter in the syslog messages.

By default, facility will be set as per the process.

Example: The syslogs related to IPSec will be set to the facility level **4** since all of them are related to the Authentication/Security.

The following caveats were resolved in WSG Release 4.4:

- CSCun58841—WSG data path crash seen intermittently with IPv6 over IPv4 traffic

  Description: WSG data path might crash intermittently. This condition might occur with IPv6 over IPv4 traffic.

- CSCuq23679 — CMP command format modification for UPDATE and ENROLL

  Description: The CMP command UPDATE and ENROLL will fail if HTTP is used as transport Protocol.

  This condition occurs when CMPv2 is executed from Exec mode.

- CSCuq58053 — WSG resets the ESP sequence number when AP changes Port Number

  Description: WSG resets the ESP sequence number when AP changes it's Port Number.

  This issue caused the WSG to put wrong sequence number in the ESP packets and the AP to drop the packets, since the ESP sequence number did not fall in the Anti-replay window.

- CSCuq58115 — WSG rejects the tunnel when sha2 is used without NULL parameter

  Description: Authentication failure is seen when sha2 is used as a signature algorithm.

  This condition occurs when signature algorithms like sha256/512/384 is used while signing the cert.

- CSCuq54287 — LCP debugs for mecores collection from IXP

  Description: IXP mecore files (qnx_1_mecore_ucdump) are not present in crashinfo_collection.

- CSCup74321 — SAMI wsg crashes due to health monitor failure

  Description: Card might crash and reload itself with HM Datapath failure event.

  The crash info file will be collected at LCP core: directory

  Different packet type takes different processing time in the Lookup leading to packet reaching late to Resequencer ME. In case if the specific sequence number packet does reach the resequencer before it's buffers is filled up completely, it can cause the resequencer's threads to hang, leading to WSG crash due to HM failure. Resequencer ME is not robust enough to handle such situations.

Note *CSCup74321 was resolved in WSG Release 4.3.3.*

The following caveats were resolved in WSG Release 4.3.3:

- CSCuq33231 — WSG fail to pick correct private key with two certificates with same SN

  Description: IPsec SA creation fails in WSG with certificates.

  WSG IPsec SA fails to pick correct private key when WSG has two certificates with the same subject name, but signed by two different rootCAs.

- CSCup74321 — SAMI wsg crashes due to health monitor failure

  Description: Card might crash and reload itself with HM Datapath failure event.

The crash info file will be collected at LCP core: directory

Different packet type takes different processing time in the Lookup leading to packet reaching late to Resequencer ME. In case if the specific sequence number packet does reach the resequencer before it's buffers is filled up completely, it can cause the resequencer's threads to hang, leading to WSG crash due to HM failure. Resequencer ME is not robust enough to handle such situations.

- CSCtr31717 — To collect ixp core in case of PPC-IXP HM failures

  Description: Whenever HM failure occurs, Core dumps are not being collected for the IXPs in the crash-info tar of LCP.

  When “exception ixp <no>” is not present in the LCP configuration, core dumps are not being collected.

  Workaround: Configure “exception ixp <no>” in the LCP

The following caveat was resolved in WSG Release 4.3.2:

- CSCuo78663 — DNS option support for DHCPv4

  Description: WSG is not able to retrieve DNS server IP from DHCPv4 server.

  While IPSec tunnel creation, FAP expects DNS IP from WSG. However, WSG is not able to retrieve DNS server IP from DHCPv4 server.

The following caveat was resolved in WSG Release 4.3.1:

- CSCuo64958 — WSG: Authentication failure seen due to certificate cache issue.

  Description: When the AP has two different certs with the same subject name and tries to create two different tunnel with WSG, Authentication failure is seen.

The following caveats were resolved in WSG Release 4.3.0:

- CSCtc98394 — WSG S2S profile with overlapping traffic selectors : traffic path issue

  Description: Packet drops in traffic of Site to Site tunnels with overlapping addresses in traffic selectors.

  This condition occurs when overlapping traffic selector addresses are present on WSG configuration.

- CSCtu90531 — LCP: On Sysmgr crash, multiple cores are created in /var/tmp directory

  Description: Session to LCP from SUP may not work at times showing the following message:

  ```
  Error: context name (id:0) cannot be determined.
  ```

  If the sysmgr cores in LCP, without this DDTS fix, core will not be copied to dir core: In LCP and sysmgr, core will not result in SAMI reload. Also, sysmgr will keep generating core files in **/var/tmp** directory leading to **/var/tmp** getting full.

- CSCum18161 — Address-pool config not getting activated after removing DHCP config

  Description: Removed the DHCPv6 configs, de-activated and also removed from the profile, however, new address-pool config fails with the cause “**Remove DHCP server configuration before adding address pools**”.

  When the DHCPv6 config is removed and the profile de-activated, configure the address-pool config and activate the profile. Profile should get activated.

- CSCun35470 — Not able to remove local address pool config on deactivating the profile

Description: Address pool configs cannot be removed even after de-activating the profile.

This condition is seen when an address pool is configured with an active profile. WSG wont allow un-configuring address pool when the profile is in active state.

- CSCun04001 — Removing validation for IP/IPv6 addresses to allow graceful upgrade

  Description: WSG blocks user from configuring 0.0.0.0 as access-permit IP address

  This condition occurs when user tries to configure 0.0.0.0 as access permit under any profile.

- CSCtj29848 — SME crash on LCP while trying to collect coredump

  Description: During the unexpected reload of any of the SAMI processors possibly due to a software defect, the SAMI LCP attempts to collect debug information that will help determine the cause of the unexpected reload. On rare occasions, the LCP itself can undergo an unexpected reload during such information collection with the following error message:

  ```
  %SAMI-2-SAMI_SYSLOG_CRIT: SAMI <CmdArg>slot<noCmdArg>/0: %SAMI-2-443001: System
  experienced fatal failure.Service name:sme(<CmdArg>pid<noCmdArg>) crashed, could not
  save last core,mv command failed, code 256,reloading system
  ```

- CSCuc65113 — LCP Sysmgr Crash Due To Proc Mem Info Corruption

  Description: Core Dump File includes Proc Mem Info Details. LCP Sysmgr crashes due to Proc Memory Info Corruption.

The following caveats were resolved in WSG Release 4.2:

- CSCtz76617 — ipsec proc stuck 99% after "clear cry ips sa" then setup 16k tunnels

  Description: In this scenario there are 16k and 8 k IPv6 tunnels on different profiles and VRF. When WSG initiated P2 re-keys fail due to TS lookup failure on any of the profile. The active WSG IpSec process hangs after 99% completion, after execution of clear cry ips sa – command. Then it again initiates the set-up of 16 k IPv6-VRF tunnels for both profiles. It also requires to load both the active as well as stand-by WSG for recovery.

- CSCtn16495 — Bad result when snmp getnext queries two/more OIDs from ipAddressTable

  Description: This issue is observed when a single SNMP getnext request tries to query two objects from the ipAddress Table. The OID of the second result is incorrect in most cases. This issue is observed only when there are more than two queries in a single getnext request.

  Workaround: Whenever the SNMP getnext is used, the request should be split into single OID queries.

The following caveats were resolved in WSG Release 4.0.3:

- CSCsy93899—Small Number of IPSec Tunnels are Deleted After a Phase-2 Re-key

  After a phase-2 re-key, a small number of IPSec tunnels (approx. 10-20) may be deleted.

  This has been seen with large number of tunnels (8500 tunnels on each PPC) established at a high rate and the lifetime was set to a short value in an engineering environment.

  Workaround: None.

- CSCud46630—Deleting a root certificate does not remove it from the WSG database

  Description: After removing a root certificate from the WSG configuration, the removal appears to be successful. However, the root certificate is not deleted from the WSG database.

  – Attempting to remove a root certificate while crypto profiles are active.

  - Attempting to update an existing root certificate while crypto profiles are active.

  Workaround: Deactivate all crypto profiles when deleting or modifying root certificates.

- CSCtx84326—Removal of BGP related config off WSG may result in abnormal SAMI reload

  Description: With a BGP related configuration for the WSG Reverse Route Injection (RRI) feature, the removal of the BGP configuration off the WSG may result in an abnormal SAMI reload.

  Workaround: Block the BGP neighbors from sending any routes to the WSG. Remove the BGP neighbor configurations one by one before removing the BGP configuration.

- CSCty03287—WSG returns incorrect values for Enhanced-Ipsec-Flow SNMP MIB objects

  Description: This occurs if a SNMP getnext is the first operation performed on the objects after the tunnel is established.

  Workaround: Do not perform getnext immediately after establishing the tunnel. If the getnext operation is the first one performed, the returned values will be correct after the tunnel has been established for at least 15 minutes.

- CSCtx87552—BGP peer session stuck in “Clearing” state

  Description: This occurs after connectivity is lost with the BGP neighbor for more than 3 minutes.

  Workaround: Remove and re-add the BGP neighbor configuration.

- CSCts72607—Tunnels torn down after copy start run

  Description: Normally, the “copy start run” command is used at the beginning of setup. In a case where the user used this command after the tunnels were created, we observed all of the tunnels were torn down (e.g. the start and running configurations were the same). This bug was filed to find a way to avoid it.

  Workaround: None.

- CSCts80965—SNMP walk on some global stats does not show correct value

  Description: The values returned by snmpwalk on ceipSecGlobalStats and some cikeGlobalStats objects are not accumulated across all PPCs.

  Workaround: None.

- CSCth84463—HA: snmpwalk on CISCO-ENHANCED-IPSEC-FLOW-MIB stops abruptly on switchover

  Snmpwalk on CISCO-ENHANCED-IPSEC-FLOW-MIB stops.

  The HA switchover occurs during the snmpwalk.

  Workaround: Re-run the snmpwalk after the switchover is complete. The required statistics are not available immediately after the switchover.

- CSCua56545—Crypto debugs trigger process restart depending on configured timezone

  Description: Output from crypto debugs is displayed incorrectly. SAMI resets after enabling crypto debugs and debug messages are displayed. WSG is configured with a timezone consisting of at least four characters.

  Workaround: Ensure that the configured timezone is less than four characters.

The following caveats were resolved in WSG Release 3.0:

- CSCtg36835—Assertion on Attempting ssh-compliant INITIALIZE

  The **CMP initialize** command returns error when executed.

This occurs when the access method (as indicated in the URL) to the CA server is TCP.

Workaround: Use the HTTP access method (http://...) in the **CMP initialize** command to communicate with the CA server.

- CSCtg65867—snmpd on Secondary PPC Gets Stuck

  sh run in entity-all fails on one or another secondary PPC. snmpd does not respond to configuration request and times out with SAPS-->28 error.

  This condition occurs when you execute snmpwalk on UDP-MIB in continuos loop with sleep 200 secs in between two successive iterations. In entity-all mode execute the **show running-config** command. snmpd on one or more secondary PPCs timeouts with SAPS-->28 error.

  Workaround: On the bash shell of the secondary that got stuck, issue **killall -9 snmpd** command. This causes snmpd to re-spawn again.

- CSCth53865—HA: WSG Deletes Tunnels After Switchover

  The WSG deletes tunnels after an HA switchover.

  This conditions rarely occurs when there are 100,000 remote-access tunnels established. With 100,000 tunnels established, 12 were deleted.

  Workaround: None.

- CSCth86683—snmpwalk, snmpget Misses Data From Secondary Periodically

  SNMP walk may periodically fail to poll MIB instances/elements on secondary WSGs.

  SNMP walk fails to poll data from secondary WSG/PPC periodically. This situation occurs when CPU utilization on primary WSG increases considerably. However, the CPU utilization on secondary WSG always remain normal. High CPU utilization situation remains for very brief time period. The whole issue is not observed on tunnels established on primary WSG.

  Workaround: None.

- CSCti00586—HA: StandbyWSG Cannot Recover From Failed SA Import

  In the rare instance where a tunnel is not fully imported on the standby card, the standby cannot recover the tunnel from this issue.

  To see if the standby card has a tunnel in this state, issue the **show crypto isakmp summary** command and **show crypto ha db info** command. This will show if a tunnel count mismatch has occurred.

  Workaround: Reboot the standby card to force a new sync of the tunnels.

- CSCti06262—HA: snmpd Process Crashed on Active/SAMI Module

  Observed SNMP crashinfo on SUP related to primary WSG/PPC3.

  This condition occurred when we configured an SNMP related configuration on primary WSG/PPC. Leave these commands configured on the primary WSG for overnight tests. You may observe SNMP crashinfo files (on SUP disk0) due to SNMP process crash and re-initialization.

  Workaround: None.

- CSCtd27881—Site-to-Site IKEv2 Phase 2 Rekey Does Not Happen For All Child SAs

  WSG Initiated IKEv2 Phase 2 rekey happens only for one child SA.

  IKE SA with multiple child IPSec SAs, with Phase 2 rekeys initiated by WSG (client Phase 2 rekey lifetime > the Phase 2 lifetime configured on WSG).

  Workaround: Initiate rekeys from the client side (configure client Phase 2 rekey lifetime < WSG Phase 2 lifetime).

- CSCtd82379—Source Port Field is Not Updated Under **show crypto ipsec sa remote-ip** Display

  The UDP source port is not correctly displayed using the **show crypto ipsec sa remote-ip** command.

  This problem occurs under the following conditions:

  - IPSec tunnel is established via a device performing PAT.
  - A condition triggers a source port change (for example, a timeout).

  Workaround: Use the **show crypto isakmp sa** command to display the UDP source port.

- CSCtd87234—ipsecpm Process Failed With **auto-initiate** and rsa-sig authentication

  The ipsecpm process failed after tunnel failure with auto-initiate.

  The ipsecpm failure is observed with the following conditions:

  - IKEv1
  - authentication rsa-sig
  - auto-initiate
  - IKE ID for the remote peer does not match the DN, and Certificate does not include a subjectALtName extension.

  Workaround: Configure the remote peer to use DN as the ID.

- CSCte17787—Authentication failed sometimes with more than one trustpoint configured

  Authentication sometimes fails when there is more than one trust point configured.

  If you have two trust points configured, two entries of get certificate request in IKE_SA_INIT all point to the certificate in the first trust point.

  Workaround: One trust point works.

The following caveat was resolved in WSG Release 2.2.2:

- CSCtr15452—Tunnel creation fails, "No Certificate Found Anywhere" is logged on WSG

  Description: IPSec tunnel establishment fails when certificate based authentication is used. The messages "Certificate Path Construction Failed" or "No Certificate Found Anywhere" appear in the WSG event log. This symptom occurs when the certificates in use have an entry for "CAIssuers" in the AIA extension.

  Workaround: Use certificates that do not use “CAIssuers” in the AIA extension.

The following caveats were resolved in WSG Release 2.2.1:

- CSCtq87296—WSG sends DHCP release prematurely under certain conditions

  Description: The WSG sends DHCP release prematurely under certain conditions:

  1. Access Point reboot on an existing IPSec tunnel.
  2. The reboot cycle occurs before the WSG can delete the IPSec tunnel via dead-peer-detection. The WSG sends the DHCP release when the old tunnel is deleted.

  Workaround: The client IP address is re-assigned via DHCP when the IKE SA is rekeyed, provided

  the address is still available. Otherwise, the tunnel is torn down, requiring re-establishment by the Access Point.

- CSCtq89837—WSG allows tunnels to be established with remote peer ID not matching the ID in the remote peer certificate

  Description: WSG allows tunnels to be established with remote peer ID not matching the ID in the remote peer certificate. This issue is seen in 2.X images.

  Workaround: None.

The following caveats were resolved in WSG Release 1.2:

- CSCta55527—**show crypto isakmp summary** IKE Error Counters do not Increment Though SA's Deleted

  Description: Some tunnels are deleted by WSG. The corresponding IKE error counters do not show any errors.

  This happens in multiple circumstances:

  1. Immediately after a large number of tunnel creation (For example, when creating tunnels at 90 tunnels per second).
  2. If the client does not respond to the INFORMATIONAL messages (and probably the IKE timeout happens).

  Workaround: None.

- CSCtb18406—Snmpwalk Returned 0 For All Tunnel Instance Statistics

  Description: The **snmpwalk** utility returns zero values for all instance statistics (per tunnel in/out packets and octets) for the cisco-enhanced-ipsec-flow-mib table.

  Workaround: Use the **snmpget** utility to see valid statistics for each specific instance.

- CSCtb30242—Syslogd crashinfo File Created After SAMI Reset

  Description: Crashinfo files for syslogd are created and saved to the SUP. No other problems are observed with syslog after the SAMI comes up. The files are saved to the SUP after the SAMI is reset. This could occur after upgrading the software image (a reset is required to complete the upgrade), or simply resetting the SAMI.

  Workaround: None.

- CSCub92784—Allow CA root certificates to be added without profile activation

  Description: Adding new trustpoint (i.e. root) certificates to the WSG configuration requires deactivation of all crypto profiles. Additional root certificates are required when tunnels are already established.

  Workaround: None.

- CSCua97225—Unable to configure multiple TS in remote access profiles

  Description: Multiple access-permit statements cannot be configured in remote access crypto profiles.

  Workaround: None.

- CSCub75654—Multiple TS information is not displayed under **show crypto ipsec sa**

  Description: The **show crypto ipsec sa** command does not display all of the traffic selector information. Only the first traffic selector data is displayed. Occurs when:

  - Remote access crypto profile configuration on WSG.
  - Remote access tunnels are established using multiple traffic selectors.

  Workaround: None.

- CSCub43861—Configuring the remote secret requires profile deactivation

  Description: Attempting to configure the remote secret results in the message, "Configuration failed in ipsecpm." Occurs when the user attempts to configure the remote secret parameter while a crypto profile is active.

  Workaround: Deactivate all profiles prior to configuring the remote secret.

- CSCty02108—Wrong next-hop mac-address on standby

  Description: Traffic lost on a particular WSG or the **show arp** command displays the wrong MAC address. Occurs when HSRP WSG active/standby is configured.

  Workaround: Reload the WSG exhibiting this problem.

- CSCtz71369—asciiPending SAP->611 wipes out WSG config

  Description: WSG has no configuration after a reboot. The startup configuration is corrupted. Occurs after these steps:

  – An error condition such as SAP->611 is encountered which prints an error message into the running configuration when it is displayed using the **show running-configuration** command.

  – User saves the running configuration.

  – A WSG reboot occurs.

  Workaround: If an error message is displayed during the execution of the **show running-configuration** command, do not save the running configuration.

- CSCub32115—Standby WSG usurps the primary MAC address

  Description: The standby WSG will sporadically usurp the MAC address of the active WSG and announce itself causing ARP resolution to fail. This issue can also cause a failure to pass traffic on newly added routes. This issue is seen intermittently in a redundant HA setup when there is no traffic for a period longer than 5 minutes.

  Workaround: Configure mac mac-address table timeout to 4 hours on the appropriate VLAN. Adding new routes requires a WSG reload to take effect.

- CSCtz92610—WSG is dropping all traffic in IXP due to wrong HA bit

  Description: ESP packets are dropped on the WSG. This issue occurs when the VLAN currently configured on a PPC was previously configured on a lower numbered PCC, and the SAMI was not reset since that last configuration change. The information pertaining to the previously configured VLAN is not removed from memory when the configuration changes.

  Workaround: Reload the SAMI.

- CSCuc45124—Traffic fails on tunnel after IPSec SA rekey on a neighboring PPC

  Description: Traffic fails on an IPSec tunnel. The tunnel does not pass traffic until a subsequent IPSec SA (phase-2) rekey occurs on the same tunnel.

  – Remote access tunnels are terminated on WSG.

  – Tunnels are terminated on two adjacent PPCs (e.g. 3 and 4, or 7 and 8).

  – Multiple traffic selectors are configured or negotiated for the tunnels terminating on the higher numbered PPC.

  – A phase-2 rekey occurs on a tunnel terminating on the higher numbered PPC. This triggers the traffic loss on a tunnel terminating on the lower numbered PPC.

  Workaround: If remote-access tunnels with multiple traffic selectors are needed, do not terminate tunnels on an adjacent, lower numbered PPC.

- CSCub82872—WSG infra should send the appropriate msg when tearing the PPC VLAN down

Description: Traffic does not pass through the WSG even though the IPSec tunnel is successfully established. This issue has been observed after configuration changes to VLAN interfaces on different WSG instances (i.e. PPCs) on the same SAMI. Typically, the VLANs are reused but moved to interfaces on different WSG instances.

Workaround: Reload the SAMI.

- CSCsq81533—System Manager (core-server) crash - incorrect reloading system syslog

  Description: The following message may appear in the system log. However, the system does not reload:

  ```
  Jun  9 2008 00:53:01: %ACE-2-443001: System experienced fatal failure.Service
  name:System Manager (core-server)(30822) has terminated on receiving signal
  11,reloading system
  ```

  This process is not supposed to initiate a system reset. It is spawned upon demand and will be re-created as necessary.

Related Documentation

For more detailed installation and configuration information, see the following publications:

- *Cisco Wireless Security Gateway Release Configuration Guide for Release 4.4.8*
- *Cisco Service and Application Module for IP User Guide*
- *Application Control Engine Module Server Load-Balancing Configuration Guide*
- *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*
- Cisco 7600 Series Cisco IOS Software Configuration Guide
- Cisco 7600 Series Cisco IOS Command Reference
- For information about MIBs, see:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- Cisco IOS Configuration Guides and Command References, Release 12.2—
  Use these publications to help you configure the Cisco IOS software that runs on the MSFC.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.