

AMARANTEN

Release Notes

Amaranten CorePlus Version 8.90

9M Oriental Kenzo Mansion, 48 Dongzhimenwai Avenue, Dongcheng District, 100027 Beijing, China
Amaranten Corporation Ltd
<http://www.amaranten.com>

Build: 8.90.13
Published 2011-03-07
Copyright © 2011

Release Notes Amaranten CorePlus Version 8.90

Published 2011-03-07
Build: 8.90.13

Copyright © 2011

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this document nor any of the material contained herein, may be reproduced without written consent of the author.

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL AMARANTEN OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE AMARANTEN PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF AMARANTEN IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, AMARANTEN WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. AMARANTEN WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT AMARANTEN RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

1. Version Summary	4
2. New Features	4
2.1. New Features and Enhancements in CorePlus 8.90.13	4
2.2. New Features and Enhancements in CorePlus 8.90.12	4
2.3. New Features and Enhancements in CorePlus 8.90.11	4
2.4. New Features and Enhancements in CorePlus 8.90.10	4
2.5. New Features and Enhancements in CorePlus 8.90.09	4
2.6. New Features and Enhancements in CorePlus 8.90.08	4
2.7. New Features and Enhancements in CorePlus 8.90.07	4
2.8. New Features and Enhancements in CorePlus 8.90.06	5
2.9. New Features and Enhancements in CorePlus 8.90.05	5
2.10. New Features and Enhancements in CorePlus 8.90.04	5
2.11. New Features and Enhancements in CorePlus 8.90.03	5
2.12. New Features and Enhancements in CorePlus 8.90.02	5
2.13. New Features and Enhancements in CorePlus 8.90.01	6
2.14. New Features and Enhancements in CorePlus 8.90.00	6
3. Addressed Issues	8
3.1. Addressed Issues in CorePlus 8.90.13	8
3.2. Addressed Issues in CorePlus 8.90.12	8
3.3. Addressed Issues in CorePlus 8.90.11	9
3.4. Addressed Issues in CorePlus 8.90.10	9
3.5. Addressed Issues in CorePlus 8.90.09	9
3.6. Addressed Issues in CorePlus 8.90.08	10
3.7. Addressed Issues in CorePlus 8.90.07	11
3.8. Addressed Issues in CorePlus 8.90.06	11
3.9. Addressed Issues in CorePlus 8.90.05	16
3.10. Addressed Issues in CorePlus 8.90.04	17
3.11. Addressed Issues in CorePlus 8.90.03	19
3.12. Addressed Issues in CorePlus 8.90.02	19
3.13. Addressed Issues in CorePlus 8.90.01	20
3.14. Addressed Issues in CorePlus 8.90.00	21
4. Installation Instructions	23
5. Known Issues	23
6. Licensing	24
7. Getting Help	24

1. Version Summary

Version 8.90.13 is the latest version of the Amaranten CorePlus kernel.

2. New Features

The following sections detail new features and enhancements in Amaranten CorePlus 8.90. For a complete list and description of all the features in Amaranten CorePlus 8.90, refer to Amaranten CorePlus Administration Guide 8.90.

2.1. New Features and Enhancements in CorePlus 8.90.13

No new features were introduced in the 8.90.13 release.

2.2. New Features and Enhancements in CorePlus 8.90.12

No new features were introduced in the 8.90.12 release.

2.3. New Features and Enhancements in CorePlus 8.90.11

No new features were introduced in the 8.90.11 release.

2.4. New Features and Enhancements in CorePlus 8.90.10

No new features were introduced in the 8.90.10 release.

2.5. New Features and Enhancements in CorePlus 8.90.09

Connection Rate Statistic Values

The statistics module has been improved with statistic values for the number of opened and closed connections per second. These values can be viewed both using the real time monitor and SNMP. A new MIB file has been created with the new values.

2.6. New Features and Enhancements in CorePlus 8.90.08

Support for relaying DHCP to multiple servers

The DHCP Relay was limited in relaying to only one server. The relay limit has been increased to 3 servers.

2.7. New Features and Enhancements in CorePlus 8.90.07

Improved DNS tunnel handling.

Tunnels with a DNS name as Remote Gateway are not torn down at reconfiguration.

Improved handling of IPsec tunnels during reconfiguration for SG12 and SG15.

Gateways which were not able to act as IKE responders due to license restrictions are now allowed to process incoming IKE connections if there exist an old IKE SA with the peer.

Improved Keep-alive functionality for IPsec tunnels.

IPsec Keepalive does not only remove the IPsec SA but also the IKE SA which allows a tunnel to be reestablished quicker.

2.8. New Features and Enhancements in CorePlus 8.90.06

Improved logging for Anti-SPAM.

Log message "recipient_email_changed_to_drop_address" added for easy tracking of SPAM e-mails that gets forwarded to the DNS blacklist drop address.

Real-time monitoring of system memory usage and TCP windows.

Real-time monitoring has been improved with monitoring capabilities of system memory usage and TCP receive and send window usage.

Real-time monitoring of system timer usage.

Real-time monitoring has been improved with monitoring capabilities of system timer usage.

New log message at failover triggered by linkmon.

A new log event has been added when a failover is triggered by linkmon. The new event is called "linkmon_triggered_failover".

A new advanced setting has been added to control the number of RADIUS communication contexts that can be used simultaneously.

With the new advanced setting MaxRADIUSContexts it is now possible to adapt the maximum number of simultaneous RADIUS communication contexts. The contexts are used in the RADIUS subsystem for both authentication and accounting procedures.

DNS name resolving uses the shared IP in High Availability setups.

In High Availability setups, the active node did not use the shared IP address when resolving DNS names. This could lead to problems in setups where only one, the configured shared IP address, were globally routable. The security gateway will now use the shared IP address when resolving DNS names from the active node. DNS resolving from an inactive node will still be using the private IP.

2.9. New Features and Enhancements in CorePlus 8.90.05

No new features were introduced in the 8.90.05 release.

2.10. New Features and Enhancements in CorePlus 8.90.04

No new features were introduced in the 8.90.04 release.

2.11. New Features and Enhancements in CorePlus 8.90.03

Added support for Hardware Watchdog on SG3200 (Winbond 83627EHF/EHG)

The hardware watchdog on the SG3200 series appliances are now supported.

2.12. New Features and Enhancements in CorePlus 8.90.02

Failed attached interfaces are set to null.

Failed attached interfaces are set to null-interfaces.

SMTP Email Size Limitation

The SMTP-ALG has been improved with an Email Size Limitation feature for limiting the total size of a transferred email.

Improved FineTune performance

The grid control used in the Security Editor has been tuned to improve speed when handling large configurations.

2.13. New Features and Enhancements in CorePlus 8.90.01

X-SPAM headers are added to e-mails considered to be SPAM by DNSBL anti-spam.

The DNS blacklisting functionality in the SMTP ALG now adds X-Spam headers to emails that are considered to be SPAM.

2.14. New Features and Enhancements in CorePlus 8.90.00

NAT Pools

NAT Pools is a new feature that is used together with IP NAT rules. The NAT Pools provide means for NATing using multiple IP addresses.

Support for Multiple IP Rule Sets.

CorePlus can now handle multiple sets of IP rules. Instead of having all rules in a big list, the entire collection of rules can be broken down into smaller logical units. Although not limited to this, the main target of the feature is to ease configuration of virtual routers (where each Virtual Route may have its own set of rules).

SIP Application Layer Gateway

A SIP Application Layer Gateway has been implemented.

TFTP Application Layer Gateway

A TFTP Application Layer Gateway has been added to make it possible to secure TFTP transfers through the gateway.

POP3 Application Layer Gateway

A new POP3 Application Layer Gateway with support for Anti-Virus has been added.

DNSBL Anti-Spam

The SMTP Application Layer Gateway has been extended with support for DNS Blacklisting as a Anti-Spam mechanism.

PCAP Recording

It is now possible to capture network traffic directly at the gate using the new "pcapdump" console command.

Broadcom Network Adapters.

Two new network drivers have been added to CorePlus; B5700 for the Broadcom Gigabit Ethernet type network adapters (sometimes referred to as Broadcom Netextreme), and BNE2 for the Broadcom NetXtreme II type network adapters.

Extended SNMPv2c Support

SNMP support has been extended to support all statistical counters in CorePlus.

Real-Time Monitor Alerts

The Real-Time Monitor Alerts function makes it possible to generate alerts when a specific RTM value exceeds the defined limit.

Support for MPLS Pass through.

The security gateway can now be configured to allow MPLS packets to be forwarded in transparent mode.

Diagnostic Console

The diagnostic console is an extension to the now obsolete "crashdump" console command and its output should be accompanied when submitting troubleshooting reports. The diagnostic console can be accessed through the "dconsole" console command.

Extended ping command

The ping console command has been extended to support both "TCP Pings" (three way handshakes) and "UDP Pings".

Improved Virtual Routing support in the Link Monitor

Link monitor can now be used in Virtual Routing scenarios as it has been extended to support configuration of which PBR table to use when monitoring the host.

New Log Category for Anti-Virus Related Events

It is now easier to find Anti-Virus related log events since they have been grouped into a separate log category.

Enhanced support for managing log categories for a log receiver

It is now possible to exclude, include and change severity on a log category level for a log receiver. Behavior for a specific log message has higher priority and will override category behavior.

Server Load Balancing Extended with Capability to Rewrite Destination Port

The SLB (Server Load Balancing) functionality now has the possibility to specify a new destination port.

FineTune is now Certified for Windows Vista

The 8.90.00 release of Amaranten FineTune is now Certified for Windows Vista.



Note

Before installing 8.90.00, older versions of FineTune must be uninstalled.

Rules and Routes Locations Changed

A new "Rules" folder is added, under which you can add custom rule sets. The main rule set is also moved under this folder and is called "Main". The folder "Policy-Based Routing Tables" (under the "Routing" folder) is renamed to "Routes". The main routing table is also moved under this folder and is called "Main".

FineTune Supports Exporting of IP Rule Sets to Microsoft Excel Format.

It is now possible to export IP Rule Sets in Microsoft Excel XML spreadsheet format.

Copy or move items between different nodes in the Security Editor treeview.

Now it's possible to copy or move items between different nodes in the Security Editor treeview.

You can, for example, cut one or more rules from the main rule set and paste them into a sub rule set.

3. Addressed Issues

The following sections detail the addressed issues in Amaranten CorePlus 8.90 release.

COP items refer to issues in Amaranten CorePlus and **FNT** items refer to issues in Amaranten FineTune.

3.1. Addressed Issues in CorePlus 8.90.13

- **COP-8653:** References to UserAuth privileges for authenticated users could change when modifying the number of configured privileges.
- **COP-9087:** ACK messages for non 2xx PBXs responses were not forwarded by the SIP ALG.
- **COP-9249:** It was impossible to monitor the HWM values since they were of the unsupported float type. SNMP has been updated to round the value to an integer.
- **COP-9400:** Incoming SIP traffic routed through an IPsec tunnel was discarded by the SIP ALG.
- **COP-9418:** The reception of 255.255.255.254 as Framed-IP-Address in a RADIUS negotiation was not handled correctly in all installations. Now this will always lead to an IP being assigned, to the PPTP-/L2TP-client, from the configured IP pool.
- **COP-9467:** In certain scenarios, the voice transmitted through the SIP ALG terminated suddenly two minutes after the call was established.
- **COP-9561:** The HTTP ALG failed to load web pages from certain web servers correctly. The HTTP ALG will now respond with a TCP RESET should the server continue to send packets after the client has closed the connection.
- **COP-9591:** Anti-virus scanning of zip files containing files with a large compressed size could sometimes lead to unexpected behavior.

3.2. Addressed Issues in CorePlus 8.90.12

- **COP-8100:** Certain SIP server scenarios in REGISTER transactions made the gateway reject incoming SIP calls.
- **COP-8261:** Certain SIP PBX configurations blocked media transmission on calls established between devices located on the same interface of the gateway.
- **COP-9135:** The POP3 ALG did not reset its state after a failed authentication. This could cause the next login attempt to fail.
- **COP-9152:** The DHCP Server did not send DHCP NAK messages in all scenarios. For example when Windows XP DHCP clients moved to a new subnet and requested their previous address again. This change speeds up the process of receiving a new IP address lease in these scenarios.
- **COP-9195:** Restarting a GRE interface did sometimes trigger an unexpected restart of the gateway.
- **COP-9223:** The POP3 ALG did not allow Digest-MD5 authentication.
- **COP-9253:** There was no log message indicating that an ARP resolve query failed. A new log message has been added.

-
- **COP-9285:** The SIP ALG could forward malformed SIP messages if a range 0-65535 was used as destination port in the SIP service configuration.
 - **COP-9339:** The HTTP ALG MIME type check did not have support for OpenDocument Text Documents (odt).
 - **FNT-449** Since the change to the new Clavister company website, license registrations no longer work from within FineTune. A warning message now informs the user that licenses must be registered manually.

3.3. Addressed Issues in CorePlus 8.90.11

- **COP-8364:** Certain SIP option messages with high values for the "expires" header field failed to be properly parsed. When that occurred incoming calls to phones placed behind the gateway failed.
- **COP-8488:** Some HTTP headers could cause HTTP connections through the HTTP ALG to be closed down prematurely.
- **COP-8598:** Some specific high stressed Intrusion Detection and Protection scenarios using a hardware accelerator could drain the memory of the gateway.
- **COP-8802:** The SMTP ALG did not accept response codes that only contained numeric data.
- **COP-8862:** Directly after a reconfiguration using a HA configuration the interface synchronization list for the Inactive node contained invalid interface references which could cause problems when connections were synchronized before the list was rebuilt. The references are now properly cleared during a reconfiguration.

3.4. Addressed Issues in CorePlus 8.90.10

- **COP-8397:** The CLI command 'dns -query' only returned one IP address even though the DNS Record contained multiple entries.
- **COP-8924:** When using services with the SYN flood protection (SYN Relay) functionality enabled, reconfigurations could result in unexpected behavior.

3.5. Addressed Issues in CorePlus 8.90.09



Note

It is recommended to update the Loader to the 1.07.14 version supplied in the upgrade package, as a number of the addressed issues are dependent on resolved issues in the Loader.

- **COP-8533:** Due to memory corruption occurring in some setups, the internal timers caused the gateway to restart unexpectedly. Depending on the traffic load, the reboots occurred periodically from a few hours up to several days. This issue has been corrected together with fixes in the loader.
- **COP-8792:** Keep-alive SIP pings were not handled correctly and would generate drop logs. The SIP pings are now handled correctly and a response pong is sent.
- **COP-8832:** The dconsole command always printed that it showed the events for the last 30 days even though nothing had happened. The command has been updated so it will print the date of the oldest entry. If entries exist that are older than 30 days it will print 30 days and truncate, if less than 30 days, date of last entry will be printed.

-
- **COP-8840:** There was a critical defect in the Web Content Filter functionality that could cause the gateway to reboot unexpectedly.
 - **COP-8859:** If the DHCP Relay option "DHCP Server to relay to" is set to broadcast or zero and action is set to BOOTPForward, then the DHCP Relay triggered incorrectly on incoming packets. The DHCP Relay now correctly handles broadcast and zero address packets.
 - **COP-8965:** During HA fail-over, some server load balancing (SLB) servers could end up in inactive state. With this fix, all SLB monitor states are reset to online on HA fail-over and the servers' status are updated in the next server status poll.

3.6. Addressed Issues in CorePlus 8.90.08

- **COP-5250:** A configuration that contains a routing table loop could lead to the watchdog being triggered. Now the configuration is failed with the following message: "Dynamic routing configuration error, possible configuration loop".
- **COP-7744:** Some errors in IPsec tunnel configuration were not handled correctly during the gateway start up process, which resulted in the incorrect setup of IPsec tunnels. Now that sort of error result in a disabled tunnel and a warning message is displayed. For the most severe cases the configuration will be rejected by the system.
- **COP-7853:** Policy based routing was not previously handled by SIP-ALG and would incorrectly use the main routing table.
- **COP-7894:** Running FTP-ALG in hybrid mode could result in the first packet being dropped when the connection to the server was not established, and this led to a three seconds delay. The connection from the FTP-ALG to the client will now not be initiated until the server connection is established towards the FTP-ALG.
- **COP-8286:** The reconfiguration process took a long time, when using multiple IDP rules. Now this time has been shortened in cases where the configuration changes do not impact the Deep Inspection rules and / nor its signatures.
- **COP-8351:** The gateway did not accept certificates signed with RSA-SHA256.
- **COP-8363:** A race condition could previously occur in the state machine handling the IKE traffic when execution of a packet thread was preempted due to time restrictions. The problem arose when other timeouts that assumed the completion of a packet thread were executed before a packet thread had finished. The packet threads is now guaranteed to be executed first until it reaches a valid state for preemption.
- **COP-8380:** The SMTP-ALG incorrectly blocked emails sent using the CHUNKING (BDAT) extension. The SMTP-ALG has been modified to remove the CHUNKING capability from the server's EHLO response. This allows the emails to pass through the SMTP-ALG.
- **COP-8402:** The gateway could unexpectedly restart when disabling automatic updates of anti-virus and IDP updates.
- **COP-8445:** IPsec tunnels with a DNS name as remote endpoint would cease to function after a remote endpoint IP address change.
- **COP-8521:** There was a problem when multiple IPsec SAs referenced the same XAuth context.
- **COP-8525:** The UDP checksum was not correctly updated when the multiplex rule was used together with address translation (SAT SETDEST / NAT).
- **COP-8644:** The Web Content Filtering (WCF) protocol could in high latency networks get out of sync with the server. When this happened, the local URL cache failed to build up correctly and an unnecessary amount of lookup requests were sent to the server. Users trying to connect to web sites experienced abnormally long delays. This fix solves the protocol synchronization

issues. The local URL cache builds up correctly at a rate corresponding to the latency to the WCF server. The local cache has also been increased to 50,000 URLs for systems running with 1024 Mb RAM or more. With this fix, the 'httpalg -wcfcache' CLI command has been extended to show statistics of the WCF cache.

- **COP-8674:** The establishment of SYN flood protected TCP connection could be unnecessarily delayed due to the SGW dropping all the packets sent by the client side while waiting for the completion of the three-way handshaking between the SGW and the server.
- **COP-8792:** Keep-alive SIP pings were not handled correctly and would generate drop logs. The SIP pings are now handled correctly and a response pong is sent.

3.7. Addressed Issues in CorePlus 8.90.07



Note

It is recommended to update the Bootmenu to the 1.05.05 version supplied in the upgrade package, as a number of the addressed issues are dependent on resolved issues in the Bootmenu.

- **COP-6986:** Deploying a configuration during heavy traffic load could cause a watchdog reboot.
- **COP-7535:** In some setups, there was a problem in internal timer functionality that occasionally could cause an unexpected reboot.
- **COP-8013:** The HTTP-ALG blocked web pages with malformed charset statement in HTTP headers.
- **COP-8112:** The command "ipsecstats" only listed the first matching IPsec SA when a tunnel name was given as an argument. "ipsecstats" now displays all IPsec SAs that are connected to the specified tunnel name.
- **COP-8124:** CorePlus could perform an unexpected abort when it failed to probe PCI devices through BIOS. CorePlus is now probing PCI devices directly without relying on BIOS functionality.
- **COP-8138:** Adobe Illustrator (.ai) files (saved by recent versions of Illustrator) did not pass the MIME type check performed by the Application Layer Gateways since they were identified as PDF files.
- **COP-8145:** Removing the use of DHCP on multiple interfaces could in some rare cases during reconfigure cause the gateway to perform an unexpected abort. Protection has been added to the timeout handling routine of DHCP.
- **COP-8155:** The FTP-ALG virus scanner triggered an unexpected restart if the virus signature database was updated while files were being processed by an FTP-ALG configured with fail-mode set to allow.
- **COP-8181:** Informative error pages generated by the HTTP-ALG could get incorrectly cached by downstream proxy servers.
- **COP-8206:** Running HA cluster and using user authentication could cause access to uninitialized memory when sending updates to the inactive node.
- **COP-8328:** The return traffic for ICMP messages received on an IPsec transport mode interface was wrongly routed to the core itself and then dropped. The return traffic is now passed back using the same connection as it arrived on.

3.8. Addressed Issues in CorePlus 8.90.06



Note

It is recommended to update the loader to the 1.07.09 version supplied in the upgrade package, as a number of the addressed issues in the list below is dependent on resolved issues in the loader.

- **COP-3346:** UpdateCenter caused problems in HA setups, sometimes locking up an HA node. HA also caused some problems for pseudo-reassembly.
- **COP-3995:** The behavior of the TCP reassembly has been changed slightly to avoid causing or contributing to ACK loops.
- **COP-4126:** The security gateway may generate `multicast_ethernet_ip_address_mismatch` log messages if deployed in setups where another HA cluster was present. The heartbeats from the other HA setup were not recognized and triggered a log message. Heartbeats from other HA setups are now identified and silently dropped.
- **COP-5013:** Ability to configure a source port for a NAT rule has been removed. This could be configured but would be ignored and the source port would still be randomly selected.
- **COP-5500:** Redirecting HTTP users to the web authentication login page did not work correctly. It is now possible to configure three different redirect scenarios. A) A user surfing to e.g. `http://www.<some site>.com` will be redirected to a login page. After successful login, the user is automatically redirected to the originally requested web page. B) A user surfing to e.g. `http://www.<some site>.com`, will be redirected to a login page. After successful login, the user is redirected to a configurable static web site e.g. `http://www.<my company>.com`. C) A user surfing to e.g. `http://www.<some site>.com`, will be redirected to a login page. After successful login, the user will be greeted with a "You have been granted access" welcome page. A requirement for this fix is that the custom web pages must be updated with the `%REDIRURL%` keyword.
- **COP-5601:** A change of an interface's name could lead to a drainage of free buffers that eventually caused the Security Gateway to stop handling traffic. Scenarios where the Security Gateway goes from being an HA member to stand alone (and vice versa) were also affected since the name of the sync interface is changed. The root cause of the leakage has been identified and fixed.
- **COP-6108:** Some malformed HTTP URIs were always blocked when scanning with IDP. It is now possible to configure the way malformed HTTP URIs should be treated (log, drop, droplog, ignore).
- **COP-6139:** IDP and Anti-virus signature databases were not automatically downloaded when upgrading the license. The IDP and/or Anti-virus databases are now automatically downloaded as soon as the gateway is upgraded with a license supporting these services.
- **COP-6190:** Previously, ARP monitoring would be disabled if there was no gateway to monitor. This behavior would cause an erratic behavior when the gateway address had been obtained via DHCP, causing the route to be permanently enabled if ARP monitoring was the only monitor selected. For the problem to manifest, the route would need to have a statically configured network range (because if the network range also had been obtained via DHCP, the route would be completely removed in the case of a lease timeout). This fix will cause ARP monitoring to disable the `*route*` if there is no gateway to monitor, rather than the monitor itself.
- **COP-6204:** Previously a route could not be configured to include its own gateway among hosts to monitor, if the gateway address was obtained via DHCP. This limitation has now been lifted.
- **COP-6486:** CorePlus was sending heartbeats during the shutdown phase, prolonging the time before the inactive cluster member declares the peer as dead. This led to unnecessary packet loss at fail over due to shutdown. The active node now stops sending CHB earlier in the shutdown phase.
- **COP-6582:** A missing anti-virus signature database or a license file not allowing anti-virus

scanning, resulted in all traffic sent through an anti-virus enabled Application Layer Gateway to be blocked. Even though this behavior guaranteed that un-scanned traffic never passed through the gateway, it could lead to unexpected interrupts in traffic flows. With this fix, the fail-mode setting for each ALG will be consulted before blocking the traffic. If fail-mode is set to allow, the traffic is still allowed and log messages will indicate that the data is passed through the gateway without being scanned.

- **COP-6884:** Synchronization of DHCP leases could fail if DHCP relay or server is configured with local host (core interface). The inactive node interpreted the synchronization message incorrectly, making the interface of a lease to become invalid.
- **COP-6890:** Addressed a series of problems in the Marvell Yukon NIC driver for the SG5500 RTM interfaces which resulted in the reception unit becoming unresponsive.
- **COP-6985:** The "max sessions" value configured for H.323 services limited the total number of concurrent ALG sessions for the whole system. If the max sessions value for an H.323 ALG was set to e.g. 100, a total limit of 100 concurrent ALG sessions would have been shared by all ALG types (HTTP, SMTP, FTP etc.) There would also not be any log message indicating that the limit had been reached. The max sessions setting for an ALG service has been fixed to reserve the requested amount of sessions for the ALG service, independently of other ALG services.
- **COP-7002:** When the SMTP-ALG anti-virus engine detected multiple infected files within a single ZIP file, the name of the zip file was incorrectly added to the BlockedAttachments.txt file each time a virus was found. The zip file name is now only added once, no matter of the number of infected files within the zip file.
- **COP-7027:** HA node froze and had to be physically rebooted after updating IDP signatures via updatecenter.
- **COP-7081:** The TCP stack did not always send segments in sequence number order when it had multiple segments to send at once.
- **COP-7094:** MS Windows LT2P over IPsec sessions could fail in the sequence of re-keys.
- **COP-7131:** The User Authentication logs sometimes contained faulty authentication information. Log events were also missing in some authentication scenarios.
- **COP-7141:** A file transfer scanned by the HTTP ALG with anti-virus activated could be aborted after a WindowZero event from the client.
- **COP-7156:** The 'active' column of 'updatecenter -servers' command showed misleading information. The column shows which server that is the recommended server to use by the UTM services (Anti-virus, IDP and Web Content Filtering). The column has been renamed to 'Precedence' and a server is either marked as 'Primary' or 'Backup'.
- **COP-7231:** PCAP captures on non-ethernet interfaces were missing Ethernet headers causing Wireshark to fail opening the files.
- **COP-7269:** In rare cases, the Web Content Filtering feature could trigger an unexpected restart of the security gateway.
- **COP-7320:** Lease for a static hosts in a DHCP server was removed if a new lease with the same MAC-address was created. A lease is now removed if the new lease is within the same DHCP server and has the same MAC-address.
- **COP-7354:** The Web Content Filtering connection to the content server did not close down when a high availability gateway switched role from being active to inactive. The web content filtering connection is now closed on inactive units.
- **COP-7363:** RFO with only HostMon did not enable the primary route when it came back up again. ARP triggered by RFO Host Monitors under this circumstances are now treated so the route can come up again.

-
- **COP-7364:** If a reconfigure was issued when the primary route was in state down, the monitored route was incorrectly declared as up, when reconfigure completed. Route Fail Over now tracks the previous state of failing routes so they are properly resumed after a reconfiguration.
 - **COP-7379:** The SNMP table CLAVISTER-MIB::clvIfVlanStatsTable was not populated correctly. This could result in watchdog reboots and that some OIDs were unavailable when using many Vlans.
 - **COP-7504:** Outdated information was sometimes used when generating log events from the ALGs which could cause the device to restart.
 - **COP-7512:** EFWLog data was not sent with the correct header when using other routing tables than the main table. The EFWLog header is now correctly set based on the routing table.
 - **COP-7528:** The SMTP-ALG could in some scenarios incorrectly block e-mails with virus infected attachments. When an email was blocked, the client received an error message saying: "Badly formatted command (pipelining not supported)".
 - **COP-7533:** Linkmon reconfigure didn't properly detach all interfaces
 - **COP-7548:** Configuring the static IPsec config mode IP pool with an address range where the least significant byte of the last address in the range is smaller than the least significant byte of the first address in the range would cause the device to reboot when several tunnels are established. One example of such a range is 172.16.1.240-172.16.2.40.
 - **COP-7558:** Route Fail Over status information were faulty printed on the console every time the state of the route changed. These printouts are now removed and only the log events remain.
 - **COP-7573:** The e1000 NIC could lose its link during reconfigure due to an incorrect triggering of the Transmit (TX) timeout handler. Addressed by changing the conditions for when the Transmit timeout handler is triggered.
 - **COP-7588:** A problem with using more recent SCP clients (built on OpenSSH) resulted in a failed SCP connection. This problem has now been resolved and verified to work with OpenSSH_5.1p1, OpenSSL 0.9.8h.
 - **COP-7598:** Tearing down an IPsec tunnel configured with XAUTH authentication could lead to an unexpected restart of the system.
 - **COP-7600:** Restarting an interface through the CLI or alternatively via ping/link monitor would not always set receive mode correctly. Addressed by securing that reset of Receive Mode is always performed upon interface restart.
 - **COP-7621:** Changing the high availability setting "use unique shared MAC" could make both nodes of a high availability cluster go active.
 - **COP-7664:** There was a dependency between link monitors which resulted in that the effective ping interval was reduced for each new link monitor configured.
 - **COP-7675:** Hardware accelerated IDP scanning sometimes failed after a signature update.
 - **COP-7693:** It was not possible to send IKE messages through an IPsec interface. The result was that a pair of hosts could not establish an IPsec tunnel with each other using IKE if the negotiation needed to pass through an IPsec tunnel established by the Security Gateway and a peer.
 - **COP-7710:** The HTTP-ALG statistic counters, e.g. the number of requests per web content filtering category, were always reset when the unit reconfigured. When using automatic updates for IDP and anti-virus, these counters were reset quite often. The statistic counters are now kept during reconfigure, as long as there is no change in the number of configured HTTP-ALG definitions. If an HTTP-ALG definition is added, removed or renamed, the counters are reset.

-
- **COP-7725:** Netobject groups weren't updated if the groups contained a dynamically changed (DHCP, PPPoE etc.) address
 - **COP-7728:** IPsec-tunnels using DNS resolving of the remote gateway didn't get established. The dynamic routes are now set properly for tunnels using DNS resolving of remote gateway.
 - **COP-7765:** Dynamic Web Content Filter, IDP and Anti-Virus updates did not always try to use the closest server. This lead to unnecessary long delays when using WCF and downloading IDP and anti-virus databases.
 - **COP-7803:** When reclassifying a Web Content Filtering blocked site, the new category for the site was not immediately updated in the local cache. It could take up to five hours before the cached entry was updated. The local cache is now immediately updated once a site has been reclassified.
 - **COP-7837:** Using the CLI, it was possible to manually connect to the Web Content Filtering server from an inactive HA member. Connection attempts to the WCF servers from an inactive HA member are now denied.
 - **COP-7842:** The HTTP-ALG could fail to reconnect to Web Content Filter servers after a HA fail-over. The unit will now reconnect to the server when URLs need to be resolved.
 - **COP-7855:** The Security Gateway could run into a state with unexpected behavior when the advanced settings for interface ring sizes or "HighBuffers" were changed. The configuration change caused the packet buffers to be freed without notification to subsystems that made use of the buffers and there by causing the unexpected behavior. CorePlus now needs to be restarted before the settings above will come into effect.
 - **COP-7857:** The TCP stack used by TCP-based ALGs, web-based user authentication and remote management did not respond to SYNs with the window set to zero.
 - **COP-7893:** The E100 transceiver could under some circumstances become unresponsive. Addressed the problem by introducing an internal interface monitor which recovers the interface when these circumstances occur.
 - **COP-7896:** The Security Gateway did not respond to TCP Keep-Alive packets.
 - **COP-7909:** A leak of addresses in the static IPsec config mode IP pool caused the number of addresses available to clients to shrink over time. It could also cause the device to reboot itself.
 - **COP-7910:** IPsec config mode configured with a static IP pool did not, in general, hand out the last address in a range to clients.
 - **COP-7919:** Log messages were not throttled correctly when the configured log receiver was offline and in return sent ICMP destination unreachable packets to the gateway. This made the gateway trigger more log messages which could lead to drained CPU resources. Log messages are now throttled for a time period of five seconds once it receives a ICMP destination unreachable as reply to a log message. It will then continue to send log messages again.
 - **COP-7938:** The gateway incorrectly discarded log messages for remote FWlog receivers. The FWlog (not Syslog) messages were discarded by the internal log queuing functionality used when a log message could not be immediately sent, e.g. during early startup or reconfigure.
 - **COP-7950:** IPsec config mode, configured with multiple subnets or a static IP pool with multiple ranges of addresses, falsely treated unchanged configurations as changed during reconfiguration and disconnected all tunnels.
 - **COP-7951:** Using Web Content Filtering, users were incorrectly displayed the "access has been denied" page if their HTTP request was generated while the WCF server connection was establishing. The URL category lookup request is now silently queued and sent to the WCF server once the connection has been established.
 - **COP-8072:** A misconfigured IPsec client made the Security Gateway to reboot while SA

handling.

3.9. Addressed Issues in CorePlus 8.90.05

- **COP-4053:** Fixed issue with DHCP NAK reception during initial phase of reconfiguration
- **COP-4524:** Fixed issue in OSPF where an LSA could be incorrectly deleted after being reoriginated
- **COP-4848:** The interface listings for Marvell Yukon interfaces showed incorrect IRQ values.
- **COP-5630:** The amount of memory used by the IDP engine was too high. The memory consumption has now been reduced.
- **COP-5904:** E-mails from e-mail addresses in the whitelist were blocked if they were classified as spam messages. Now all e-mails sent from whitelisted addresses will be let through, even if they are classified as spam.
- **COP-6311:** Fixed leap year problem where leap year day was added to January instead of February
- **COP-6513:** Fixed problem in HA where one of the cluster members could be in lockdown and prevent its member from going active.
- **COP-6546:** A configured external log receiver that does not accept log messages might send ICMP destination unreachable packets to the security gateway. These packets would trigger new log messages resulting in high CPU utilization. Logging is now connection-based and the sending rate of log messages will be decreased by the security gateway when it receives ICMP destination unreachable packets regarding log receiver connections.
- **COP-6568:** Fixed problem resulting in the IDP/AV license being expired prematurely.
- **COP-6656:** Unnecessary DynDNS and HTTP-Poster re-posts were triggered during reconfigure. This is now avoided by always considering if the local interface IP address has been changed or if the HTTP-Poster/DynDNS configuration has been changed.
- **COP-6854:** Broadcom Netextreme II NICs were not automatically detected.
- **COP-6917:** The identification of IPsec clients during reconfigure was not correct when they were behind NAT.
- **COP-6980:** The value of the advanced IP setting MulticastIPEnetOnMismatch was ignored; Packets would be dropped and logged regardless of the configuration.
- **COP-7047:** An internal buffer alignment error in the SIP-ALG could lead to a restart of the system.
- **COP-7048:** Emails did not get forwarded by the SMTP-ALG. The sending client received an error message saying that the email could not be delivered.
- **COP-7084:** HTTP Web Content Filter override functionality can cause an unexpected restart when timing out users that have clicked the override button. Users that have clicked the override button have access to blocked content for a specific amount of time. When this time expires, an unexpected restart may occur.
- **COP-7101:** It was not possible to manually force media or duplex for Marvell Yukon interface types.
- **COP-7124:** Pattern matching in the blacklist and whitelist in the SMTP-ALG has been extended to be more dynamic.
- **COP-7139:** Both members in the HA cluster did not log their change of state when roles were

changed (active to passive and passive to active).

- **COP-7152:** The SIP-ALG could in some scenarios cause instability of the system when running out of RAM. The issues have been addressed and fixed.
- **COP-7194:** Fixed issue in TCPStack with stalling transfers with peers using a very small send window
- **COP-7238:** The SIP-ALG could in rare occasions fail to setup a call and generate a log message containing "M HEADER NOT FOUND". The issue has been corrected.
- **COP-7302:** SNMP Trap messages could sometimes contain garbage characters.
- **COP-7321:** The hardware accelerated IDP scanning caused "unexpected duplicate match" log messages under certain conditions.
- **COP-7337:** The SNMP logger could in rare circumstances cause the system to malfunction.
- **COP-7345:** Web Content Filtering functionality could fail if the WCF server used for URL lookups stopped responding to queries. The mechanism used for failing-over to secondary servers has been improved. WCF will connect to the second closest server if the primary server fails. If that server also fails, it will continue with the other servers. After 1 hour of using secondary servers, a new attempt will be made to contact the primary server in order to minimize latency.

3.10. Addressed Issues in CorePlus 8.90.04

- **COP-1549:** ICMP Destination Unreachable packets were not sent when UDP packets hit a Reject rule.
- **COP-2193:** Web authentication and wwwsrv connections were closed at reconfiguration.
- **COP-2231:** The DHCP Server did just send replies back on the receiving interface without regarding routing decisions. The DHCP Server now performs a route lookup if the reply is destined for a host address (i.e. not an IP broadcast).
- **COP-3346:** Eats TCP packets on the HA-node which was inactive when IDP was enabled, if fail-/handover occurs. HA for idpupdate now let active node download files. Timestamps are compared after reconfigure and signature files are synchronized between HA-nodes.
- **COP-4964:** Some services were using the private IP in HA setups for communicating. This is now changed to use the shared IP.
- **COP-5385:** The DNS lookup of the IP address to a remote gateway failed under certain circumstances.
- **COP-5847:** The CLI command for displaying updatecenter AV/IDP update status was not showing enough information. It has now been improved.
- **COP-6036:** The SMTP ALG could not tell the difference between the new Microsoft Office 2007 document file types and file type ZIP. This is because there is no difference that can be easily discovered (the new Microsoft Office files are in fact ZIP files with a different extension). An ALG configured to make file integrity checks would therefore signal these files as invalid (wrong mime type, wrong file suffix...). The ALG will now identify Office 2007 files as ZIP files. Anti-virus checks will, if enabled, scan the contents of the new Office 2007 files just like it would with a regular ZIP file.
- **COP-6186:** Nested MIME bodies could in some scenarios be blocked by the SMTP-ALG. For example, the SMTP-ALG could block images inserted as 'inline' with an error message indicating base64 decoding error. The recipient received the email without the attached image but an error message saying: "The attachment xxxx has been blocked by the Security Gateway".

The ALG has been updated with better support for nested MIME blocks.

- **COP-6209:** SMTP ALG statistics are now implemented both for RTM and SNMP and the Amaranten MIB has been updated.
- **COP-6276:** When using the e1000 driver with an 82573-based MAC, link detection could sometimes fail under high load. This affects the SG3200-series appliances.
- **COP-6316:** Capture filters configured for the pcap functionality did not remain the same after a reconfigure.
- **COP-6377:** IPsec tunnel setup could in some scenarios read from uninitialized memory and cause instability problems. The issue has been corrected and together with this fix, the memory used by the IPsec engine has been registered and can now be monitored using the 'memory' CLI command.
- **COP-6406:** DNS Blacklist CLI command showed wrong status of blacklist servers on inactive HA member. Inactive HA member does not perform any anti-spam inspection so the inactive node is unaware of the status of the blacklist servers.
- **COP-6503:** Attachments with very long file names could cause memory corruption.
- **COP-6505:** Log string sent to syslog receivers was not always correctly formatted. Some log arguments were not separated by a whitespace, resulting in invalid parsing by syslog receivers.
- **COP-6512:** When restarting an interface using the yukon driver, there has been a theoretical possibility of memory corruption. This has been fixed.
- **COP-6516:** Will continue scanning even if an IDP hardware scanning error happens if AUDIT mode is used.
- **COP-6521:** In a scenario where one or more IPsec tunnels have been modified and needed to be reconfigured the unchecked use of an IPsec policy rule could cause the gateway to crash.
- **COP-6610:** TCP connections with SYN relay were not synchronized correctly. In case of HA failover, traffic on these connections would freeze.
- **COP-6682:** Some H.323 messages were incorrectly disallowed by the ALG. The H.323 Status Enquiry message is now allowed to be forwarded through the H.323 ALG.
- **COP-6763:** The failmode setting in the HTTP ALG was not honored by the Dynamic Web Content Filtering.
- **COP-6773:** The log message for expired or no valid Web Content Filtering license did only show up once. The log message is now generated every 1 minutes, when HTTP request was parsed, and should be more noticeable to the administrator.
- **COP-6791:** The SMTP-ALG could in some scenarios cause instability to the system by losing track of SMTP state synchronization. The SMTP-ALG has been updated with improved state tracking and email syntax validation.
- **COP-6807:** SLB TCP monitoring did not increase TCP sequence number in reset packet sent to server in case of connection timeout. The sequence number is now increased by 1.
- **COP-6842:** SLB did not use All-To-One for port numbers, when using a range on the service the destination port would be the specified port + the offset from the low port number in the service.
- **FNT-389:** The possibility to configure "Max Email Size" in SMTP ALG was missing
- **FNT-402:** Default IPsec MTU is now 1420
- **FNT-408:** Cut'n'Paste didn't work on objects used by other objects

3.11. Addressed Issues in CorePlus 8.90.03

- **COP-3899:** The TCP pseudo reassembly didn't take the window scale option into consideration.
- **COP-5598:** TXT records can be inserted in the e-mail header using X-Spam-TXT-Records header for a SPAM-tagged e-mail
- **COP-5849:** SIP-ALG failed to parse SIP requests based on the predecessor of SIP RFC 3261. Added SIP RFC 2543 compliance.
- **COP-5867:** Pure IPsec-transport mode with multiple clients behind a NAT gateway did not work when the clients used the same port. The port number is now used in the lookup so that the return traffic from the Security Gateway can be sent to the right client.
- **COP-5946:** A missing Content-Transfer-Encoding header field in e-mails could sometimes hang the SMTPALG session.
- **COP-5965:** With TCP sequence validation turned on, closing existing connections would cause all subsequent attempts to reopen the same connection to be dropped with a log message about a bad sequence number. The situation would resolve itself after a timeout of about 50 seconds, but would still cause severe traffic impairment in certain situations (most noticeably HTTP traffic). This change will by default loosen the restrictions when an attempt to reopen a closed connection is received (ValidateSilent, ValidateLogBad), while still enforcing RFC correctness. TCP sequence validation is turned off by the setting "Ignore". New options also exist to keep the original behavior (ValidateReopen, ValidReopenLog) or to completely ignore TCP sequence validation for reopening attempts (ReopenValidate, ReopenValidLog). The difference between these settings only affects how the gateway handles TCP sequence number validation when an attempt to reopen a "not open" connection is made. Also note that reopening closed TCP connections must be explicitly allowed by the gateway, for these settings to make a difference.
- **COP-6039:** The SIP-ALG will allow the user to set max sessions for a service
- **COP-6124:** Some log strings containing space characters were not quoted as required for proper interpretation by some log receivers.
- **COP-6144:** The SIP-ALG supports requests with missing From tag, which is optional in 2543 compliant clients
- **COP-6184:** When configuring an SG3200 HA cluster with Intel 82573L-based Gigabit Adapters, the sync interface would stop responding after the cable was being manually unplugged.
- **COP-6208:** A user logging in via WebAuth, configured to handle user credentials via one or several RADIUS servers, could cause an unexpected abort if no RADIUS server was reachable. This has been fixed.
- **COP-6214:** A possible memory violation in the user authentication module could cause the SGW to abort. Validation of the memory reference has been added to address this issue.
- **COP-6216:** When using L2TP over IPsec the dynamically added route was not removed when using Windows Vista behind a NAT device.
- **COP-6307:** The SIP-ALG did not always send responses to SIP requests to the correct port. The SIP-ALG sent responses to the port from where it received the request. Now, responses are sent to the port advertised by the SIP client.
- **COP-6331:** Log id 1800211 contained incorrect English. The typo has been corrected and the revision changed to 2.

3.12. Addressed Issues in CorePlus 8.90.02

-
- **COP-1908:** Incorrect translation of TCP SACK sequence numbers could result in poor throughput/reliability when used. This issue has been corrected.
 - **COP-5321:** TCP connections that were closed or aborted almost directly after the three way handshake could, in its closing state, still have as high timeout as it would have in the established state.
 - **COP-5468:** Web Content Filter override feature blocks web content even though they have been overridden by user. The WCF override functionality has changed. When a user overrides a "restricted site notice"-page, the user is allowed to browse all blocked sites for a limited amount of time. All blocked URLs requested by the user are still logged.
 - **COP-5582:** IPSec transport mode between two nodes did not function properly. The handling of fragmented packets in IPSec transport mode was incorrect and has been changed.
 - **COP-5604:** The use of certificate revocation lists without a configured DNS could lead to memory corruption.
 - **COP-5687:** The publishing of IDP signatures to FineTune failed for some signatures.
 - **COP-5692:** The logs did not show the full address and port translation if using a rule with NAT or SAT in Syslog and real-time log.
 - **COP-5744:** Connections with one-way UDP traffic could sometimes be closed within a few seconds. Connections where the side opening the connection remained idle longer than the UDP lifetime was closed even if the other side continued to send data. A new advanced setting ("UDP Bidirectional keep-alive") under Connection Timeouts has been added to make it possible to set if both sides are allowed to keep a connection open.
 - **COP-5835:** There were some L2TP incompatibility problems with Cisco routers. Handling of Offset Size and Offset Pad in the L2TP header has been added.
 - **COP-5853:** Crash occurred when using Stateless NATPool in HA
 - **COP-5876:** Single host routes were sorted according to metric and the routes were added last among the routes with the same metric. This became inefficient in a scenario where there are thousands of single host routes with the same metric. The algorithm for adding single host routes has been changed to be more efficient in this scenario.
 - **COP-5899:** IKE and IPSec lifetimes are no longer set to default values in case of incorrect settings. Lifetimes shorter than 300 seconds for IPSec SAs and 600 seconds for IKE lifetimes could cause inconsistency of IKE and IPsec SAs in large systems (>1000 tunnels). Configuration with shorter IKE lifetimes than IPsec lifetimes and with delta time less than 300 seconds between IKE and IPsec lifetimes could also cause inconsistency. In case of invalid settings a cfg warning will be issued.
 - **COP-5923:** The system shutdown process could be prevented from executing fully by the userauth module taking too long time to initiate shutdown of the module.
 - **COP-5937:** The OSPF maxage handling was in some scenarios not able to flush all outdated LSAs
 - **COP-5943:** The pseudo reassembly statistics were removed from the MIB.
 - **COP-5975:** DNSBL anti-spam events are logged in the anti-spam log category.
 - **COP-6019:** SMTP-ALG tried to send the email-headers twice for an email classified as Spam
 - **FNT-380:** It was not possible to change name of a created rule set.

3.13. Addressed Issues in CorePlus 8.90.01

-
- **COP-4626:** The lionic hardware accelerator card did not support all IDP signatures.
 - **COP-4875:** When an IPsec Xauth authenticated session timeout was reached the user was logged out but the IPsec tunnel could remain open.
 - **COP-5194:** In a HA setup, the private MAC address was used as source MAC address for outgoing traffic on the active node, instead of the shared MAC address.
 - **COP-5245:** Certificate revocation lists (CRL) were sometimes wrongly encoded and sent on as certificates during Ipsec negotiation. A patch from Safenet that corrects the issue has been applied.
 - **COP-5461:** Multicast and broadcast traffic that were logged due to a low TTL, would incorrectly log the minimum TTL setting for unicast traffic.
 - **COP-5550:** NAT-T was not fully compliant to RFC 3947.
 - **COP-5563:** The real time monitor could show monotonically increasing curves for "Forwarded pps" and "Forwarded bps".
 - **COP-5606:** The SMTP-ALG incorrectly blocked e-mails if the client was configured to use "TLS if available" and the server supported TLS. The SMTP-ALG will now strip the STARTTLS capability from the capabilities reply sent from server to client.
 - **COP-5612:** GOTO and RETURN rules traversed by the rule lookup are never implicitly logged. However, logging can now be explicitly turned on for these rules. When triggered, one such rule will log a message with severity DEBUG.
 - **COP-5616:** The log message IPSEC: id=01802040 could contain a wrong info field.
 - **COP-5690:** A fail-over due to reconfiguration could faulty result in two active nodes in a High Availability cluster.
 - **COP-5698:** Increased severity-level to 'error' for Web Content Filtering log message, indicating expired or no valid license parameter.
 - **COP-5714:** Using user authentication with an HTTPS agent and Radius as authentication source could cause the device to reboot.
 - **COP-5753:** Linkmon did not care about grace period when failover event was configured.
 - **COP-5931:** DNS servers returning multiple record types in responses got handled improperly. DNS client will now sort out the wanted record type.
 - **FNT-359:** Could not configure static DHCP leases on more than one DHCP server.

3.14. Addressed Issues in CorePlus 8.90.00

- **COP-4388:** Sending of the log message "log_messages_lost_due_to_throttling" could in some situations fail.
- **COP-4657:** The TCPNewSynProtect advanced setting has been removed due to incompatibility reasons.
- **COP-4683:** If the server filter for IP Pools was specified together with a server IP address, it was not properly enforced until a reconfigure of the unit took place.
- **COP-4689:** The TCP stack did not announce a zero-sized receive window when the receive buffer was full.
- **COP-4793:** There was a problem with the certificate validation in the IKE negotiation that under certain circumstances caused the gateway to stop responding.

-
- **COP-4829:** The port used for a listening connection was not properly released when the connection was closed, thus making the port unavailable to be re-used.
 - **COP-4961:** PPTP client failed to reconnect automatically after it has lost the previous connection to the PPTP server. There will be a reconnection attempt if there are packets sent on the PPTP client interface though.
 - **COP-5159:** Hardware acceleration of encryption/decryption on IXP platforms would eventually fail during high IPsec traffic load. Memory leak in driver fixed.
 - **COP-5166:** The 'Outer Interface Filter' specified on a PPTP server could be overridden by normal IP rules. If the rule-set allowed PPTP clients to connect to the PPTP server, that connection could not be prevented by using the 'Outer Interface Filter' parameter. Now the 'Outer Interface Filter' parameter will always have precedence over the IP rules to actually be able to filter incoming connections. The IP rules will now only affect PPTP connections when the PPP_PPTPBeforeRules setting is off.
 - **COP-5236:** A wrong hostname could be used upon DNS lookup as a consequence of LDAP server connections by the SGW.
 - **COP-5258:** SSL/TLS handshake with the gateway failed if 4096 bit keys were used.
 - **COP-5286:** A problem with the HA synchronization of connection timeout values caused zombie connections to not time out on the inactive cluster member.
 - **COP-5319:** TCP traffic over VPN tunnel using NAT-T and AES could cause unnecessary fragmentation. The default value for the advanced setting TCPMSSVPNMax has been lowered from 1400 to 1392.



Note

Please make sure that your configurations are updated to prevent fragmentation in the network.

- **COP-5324:** Negotiation of SSL/TLS version with clients supporting TLS version 1.1 or newer failed.
- **COP-5337:** SSL version 2.0 client hello messages larger than 127 byte were not handled correctly.
- **COP-5344:** Sometimes SSL/TLS records (primarily those containing alerts) were sent with an incorrect Message Authentication Code (MAC).
- **COP-5357:** When automatic database updates were disabled in Update Center, the security gateway could begin to repeatedly reconfigure until the AV/IDP license expired.
- **COP-5381:** Unexpected abort at the inactive HA on non-x86 platforms during synchronisation of dynamically added IPsec routes. Access to unaligned memory has been made safe.
- **COP-5422:** The SMTP ALG sometimes handled SMTP traffic incorrectly if the last part of the mail was not received in one chunk.
- **COP-5428:** The Anti-Virus scan engine could on some systems cause the memory resources to be depleted. A new advanced setting has been added to make it possible to change the algorithm used by the scan engine.
- **COP-5435:** Client web browsers did not get an indication of a terminated file download in case a virus was blocked. Web browser and other HTTP clients will now receive an error message since the client connection will be closed with a TCP Reset packet.
- **COP-5456:** SMTP ALG did not handle SMTP traffic correctly after receiving a plain text mail.
- **COP-5491:** SMTP-ALG setting for "Maximum e-mails per minute and host" has changed.

Default value is now disabled (unlimited amount of e-mails are allowed). The maximum allowed value has also changed from 100 to 65535.

- **COP-5511:** A full IDP/Anti-Virus database update is triggered if the software and hardware signature databases are not synchronized. This can occur when a device has been upgraded with a hardware accelerator card for IDP and Anti-Virus.
- **COP-5544:** Fragmented IP packets that were dropped for some other reason than being fragmented in an illegal way were sometimes still classified and logged as illegal fragments.
- **COP-5547:** NATPool wrongfully asked for a NULL ipaddress if reconfiguring with an uninitialized natpool IP-object
- **COP-5556:** IP fragmentation could cause TCP sequence number validation to lose track of the transmission window and start to drop all segments.
- **COP-5563:** The real time monitor could show monotonically increasing curves for "Forwarded pps" and "Forwarded bps".
- **COP-5651:** Security Gateway no longer crashes if removing IPPool, NATPool and DHCP server from config
- **FNT-224:** A H323 Application Layer Gateway object didn't reflect changes made in IP Address references. It was also possible to delete the references.
- **FNT-254:** After deleting an object in a sorted list, wrong object was selected.
- **FNT-287:** The setting "Source Interface" didn't recognize VLAN.
- **FNT-307:** Some log categories were missing (e.g. THRESHOLD, AVSE, etc)

4. Installation Instructions

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the Amaranten CorePlus Guide 8.90.



Note

The mini core distributed with this version of the CorePlus package should only be used while installing CorePlus on a fixed drive / media.

The mini core is of an older version than the main core and has limited functionality!



Note

Before installing version 8.90.00 of FineTune, older versions must be uninstalled.

5. Known Issues

- **HA: Transparent Mode won't work in HA mode** There is no state synchronization for Transparent Mode and there is no loop avoidance.
- **HA: No state synchronization for ALGs** No aspect of ALGs are state synchronized. This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. If, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.
- **HA: Tunnels unreachable from inactive node** The inactive node in an HA cluster cannot

communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.

- Inactive HA member cannot send log events over tunnels.
- Inactive HA member cannot be managed / monitored over tunnels.
- OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.
- **HA: No state synchronization for L2TP, PPTP and IPsec tunnels** There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.
- **HA: No state synchronization for IDP signature scan states.** No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.
- **HA synchronization with a gateway using CorePlus version 8.81.01 is not supported.** Due to a interoperability problem in the High Availability protocol, HA synchronization with version 8.81.01 of CorePlus is not supported, and will cause stability issues.
- **The advanced setting PPTPBeforeRules is not obeyed in the current version of CorePlus.**

6. Licensing

Amaranten CorePlus 8.90.13 requires a software subscription covering **October 25, 2007**. Make sure that this is covered before trying to upgrade the system, otherwise the system will enter a "License Lockdown" mode.

7. Getting Help

Technical Assistance via Web or Telephone

We offer timely and rapid response to customer inquiries and service requests via our web based support tool or telephone. Do not hesitate to contact us if you have any questions regarding the upgrade or installation procedure.

Amaranten Technical Support (Singapore)

Phone: (65) 6430 9535

E-mail: support@amaranten.com

Amaranten Technical Support (China)

Phone: 010-84476440/41/42/43

E-mail: support@amarantenasia.com