



## Release Notes

---

### ***Clavister CorePlus Version 8.90***

Clavister AB  
Torggatan 10  
SE-891 33 Örnsköldsvik  
SWEDEN

Phone: +46-660-299200  
Fax: +46-660-12250

[www.clavister.com](http://www.clavister.com)

Build: 8.90.05  
Published 2008-10-14  
Copyright © 2008 Clavister AB.

---

## **Release Notes Clavister CorePlus Version 8.90**

Published 2008-10-14  
Build: 8.90.05

Copyright © 2008 Clavister AB.

### **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 CLAVISTER 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 CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER 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 8.90.05 ..... | 4  |
| 2.2. New Features and Enhancements in CorePlus 8.90.04 ..... | 4  |
| 2.3. New Features and Enhancements in CorePlus 8.90.03 ..... | 4  |
| 2.4. New Features and Enhancements in CorePlus 8.90.02 ..... | 4  |
| 2.5. New Features and Enhancements in CorePlus 8.90.01 ..... | 4  |
| 2.6. New Features and Enhancements in CorePlus 8.90.00 ..... | 4  |
| 3. Addressed Issues .....                                    | 6  |
| 3.1. Addressed Issues in CorePlus 8.90.05 .....              | 6  |
| 3.2. Addressed Issues in CorePlus 8.90.04 .....              | 8  |
| 3.3. Addressed Issues in CorePlus 8.90.03 .....              | 9  |
| 3.4. Addressed Issues in CorePlus 8.90.02 .....              | 10 |
| 3.5. Addressed Issues in CorePlus 8.90.01 .....              | 11 |
| 3.6. Addressed Issues in CorePlus 8.90.00 .....              | 12 |
| 4. Installation Instructions .....                           | 14 |
| 5. Known Issues .....  | 14 |
| 6. Compatibility .....                                       | 15 |
| 7. Getting Help .....  | 15 |

---

# 1. Version Summary

Version 8.90.05 is the latest version of the Clavister CorePlus kernel. For a list of appliances that are supported by this version of the Clavister CorePlus, please refer to the Compatibility section.

## 2. New Features

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

### 2.1. New Features and Enhancements in CorePlus 8.90.05

*No new features were introduced in the 8.90.05 release.*

### 2.2. New Features and Enhancements in CorePlus 8.90.04

*No new features were introduced in the 8.90.04 release.*

### 2.3. 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.

### 2.4. 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.

### 2.5. 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.

### 2.6. 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 Clavister 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 Clavister CorePlus 8.90 release.

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

## 3.1. 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.

## 3.2. 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 Clavister 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

### 3.3. 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.
- **COP-6417:** The security gateway could fail to startup after a shut or restart command on Clavister 4200/4400 series devices. The console printed "Failed to execute 'fwcore.cfx'"

### 3.4. 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.

### 3.5. 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.

### 3.6. 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 Clavister CorePlus Admin Guide 8.90.



### **Important**

*The Cores for the Clavister SG10 and SG50 are specific to these hardware models and the correct Core file has a name which includes these model numbers. Do not use the Full version for upgrading the SG10 and SG50.*



### **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.
  - **IPsec: Pure IPsec between Windows Vista and Clavister CorePlus is not supported.**
  - **The advanced setting PPTPBeforeRules is not obeyed in the current version of CorePlus.**

## 6. Compatibility

The following section outlines the direct compatibility considerations as of CorePlus 8.90.05.

- **SG30 Series appliances**
  - Anti Virus service is not available.
  - IDP service is not available.

## 7. Getting Help

### Technical Assistance via Telephone or Email

We offer timely and rapid response to customer inquiries and service requests via telephone or email. Don't hesitate to contact us if you have any questions regarding the upgrade or installation procedure.

Clavister Technical Support  
Phone: +46 (0)660-29 77 55  
E-Mail: [support@clavister.com](mailto:support@clavister.com)  
Web: <http://www.clavister.com/support/>