



Release Notes

Clavister CorePlus Version 8.80

Clavister AB
Torggatan 10
SE-891 33 Örnsköldsvik
SWEDEN

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

www.clavister.com

Build: 8.80.09
Published 2008-06-13
Copyright © 2008 Clavister AB.

Release Notes Clavister CorePlus Version 8.80

Published 2008-06-13
Build: 8.80.09

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 8.80.09	4
2.2. New Features and Enhancements in CorePlus 8.80.08	4
2.3. New Features and Enhancements in CorePlus 8.80.07	4
2.4. New Features and Enhancements in CorePlus 8.80.06	4
2.5. New Features and Enhancements in CorePlus 8.80.05	4
2.6. New Features and Enhancements in CorePlus 8.80.04	4
2.7. New Features and Enhancements in CorePlus 8.80.03	4
2.8. New Features and Enhancements in CorePlus 8.80.02	4
2.9. New Features and Enhancements in CorePlus 8.80.01	5
2.10. New Features and Enhancements in CorePlus 8.80.00	5
3. Addressed Issues	5
3.1. Addressed Issues in CorePlus 8.80.09	6
3.2. Addressed Issues in CorePlus 8.80.08	7
3.3. Addressed Issues in CorePlus 8.80.07	8
3.4. Addressed Issues in CorePlus 8.80.06	8
3.5. Addressed Issues in CorePlus 8.80.05	9
3.6. Addressed Issues in CorePlus 8.80.04	10
3.7. Addressed Issues in CorePlus 8.80.03	11
3.8. Addressed Issues in CorePlus 8.80.02	13
3.9. Addressed Issues in CorePlus 8.80.01	14
3.10. Addressed Issues in CorePlus 8.80.00	14
4. Installation Instructions	14
5. Known Issues	14
6. Compatibility	15
7. Getting Help	15

1. Version Summary

Version 8.80.09 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 8.80. For a complete list and description of all the features in Clavister CorePlus 8.80, refer to Clavister CorePlus Admin Guide 8.80.

2.1. New Features and Enhancements in CorePlus 8.80.09

No new features were introduced in the 8.80.09 release.

2.2. New Features and Enhancements in CorePlus 8.80.08

No new features were introduced in the 8.80.08 release.

2.3. New Features and Enhancements in CorePlus 8.80.07

No new features were introduced in the 8.80.07 release.

2.4. New Features and Enhancements in CorePlus 8.80.06

No new features were introduced in the 8.80.06 release.

2.5. New Features and Enhancements in CorePlus 8.80.05

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.

2.6. New Features and Enhancements in CorePlus 8.80.04

TCP Stack optimization

The TCP Stack implementation has been optimized to increase the performance of the Application Layer Gateways.

2.7. New Features and Enhancements in CorePlus 8.80.03

Web Authentication: Automatic redirect to originally requested URL upon authentication.

It is possible to set up SAT/NAT rules in combination with user authentication and redirect all http requests to the login page. When the user has successfully logged in, he or she will be redirected to the originally requested URL.

New advanced setting to turn on logging for all packets that pass through the gateway over a connection.

A new advanced setting "LogConnectionUsage" has been added that will log all packets that pass through the gateway over a connection.

2.8. New Features and Enhancements in CorePlus 8.80.02

No new features were introduced in the 8.80.02 release.

2.9. New Features and Enhancements in CorePlus 8.80.01

No new features were introduced in the 8.80.01 release.

2.10. New Features and Enhancements in CorePlus 8.80.00

- **Support for relaying of Bridge Protocol Data Units (BPDUs)** To support transparent mode deployments in scenarios where redundant switches with spanning tree protocol are used, the system is able to relay Ethernet frames containing Bridge Protocol Data Units (BPDUs).



Note

CorePlus does not support Spanning Tree protocol, it just has the ability to forward BPDUs.

- **CorePlus sends a gratuitous ARP reply when a route fails in route failover.** CorePlus sends a gratuitous ARP reply to notify other equipment that the MAC address has changed when a route failover occurs.
- **CLI command added to make it possible to send gratuitous ARP replies.** A CLI command is added which makes it possible for the administrator to force the transmission of a gratuitous ARP reply.
- **Protection against IP address conflicts.** To protect against IP address conflicts, CorePlus sends unsolicited ARP replies when it detects that another device sends ARP messages with the Clavister Security Gateway IP as source.
- **Integrated Antivirus.** Integrated Antivirus scanning is implemented as a part of the Application Layer Gateways and is supported for HTTP, FTP and SMTP. The AV scan engine supports on-the-fly decompression of ZIP and GZIP data streams. It also supports decoding of multiple encoding formats. The AV scan engine supports on-the-fly stream based scanning of gigabyte sized files without increased latency.
- **SMTP Application Layer Gateway.** An SMTP Application Layer Gateway has been added to improve the possibility to control mail transactions.
- **Web Content Filtering: Unknown category renamed to Non-Managed.** To correctly describe it's purpose the category is now renamed to **Non-Managed**. All sites that are outside the scope of the other categories will be defined as Non-Managed. In most network environments it is recommended to always allow users to access Non-Managed websites.
- **IDPUpdate functionality moved to UpdateCenter.** To streamline IDP and Antivirus update functionality an UpdateCenter CLI command is added to handle all automatic updates.
- **UpdateCenter functionality now uses the shared IP when communicating with the CSPN network.** To deprecate the need to have public IP addresses for both nodes in an HA scenario the UpdateCenter functionality now uses the shared IP when communicating with the CSPN network.
- **Pseudorandom number generator algorithm in QuickSec changed from Yarrow to ansi-x9.62.** The Pseudorandom number generator in QuickSec has been changed from Yarrow to ANSI X9.62 to comply with ICSA specifications.
- **Extended IkeSnoop logging** IkeSnoop has been updated with timestamps and a new set of messages describing dropped packets as well as internal errors.

3. Addressed Issues

The following sections detail the addressed issues in Clavister CorePlus 8.80 release.

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

3.1. Addressed Issues in CorePlus 8.80.09

- **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-6045:** IP address with suffixes .0 and/or .255 could incorrectly be assigned to IPsec config mode clients.
- **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-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-6503:** Attachments with very long file names could cause memory corruption.
- **COP-6512:** When restarting an interface using the yukon driver, there has been a theoretical possibility of memory corruption. This has been fixed.
- **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.
 - **FNT-402:** Default IPsec MTU is now 1420

3.2. Addressed Issues in CorePlus 8.80.08

- **COP-3899:** The TCP pseudo reassembly didn't take the window scale option into consideration.
- **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-6045:** IP address with suffixes .0 and/or .255 could incorrectly be assigned to IPsec config mode clients.
- **COP-6124:** Some log strings containing space characters were not quoted as required for proper interpretation by some log receivers.
- **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-6331:** Log id 1800211 contained incorrect English. The typo has been corrected and the revision changed to 2.

3.3. Addressed Issues in CorePlus 8.80.07

- **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-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-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

3.4. Addressed Issues in CorePlus 8.80.06

- **COP-5159:** Hardware acceleration of encryption/decryption on IXP platforms would eventually fail during high IPsec traffic load.
- **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-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-5550:** NAT-T was not fully compliant to RFC 3947.
 - **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-5690:** A fail-over due to reconfiguration could faulty result in two active nodes in a High Availability cluster.

3.5. Addressed Issues in CorePlus 8.80.05

- **COP-2049:** The SGW could use a malformed host name upon contact of a LDAP server for CRL retrieval.
- **COP-4388:** Log message `log_messages_lost_due_to_throttling` was sometimes lost.
- **COP-5194:** Fixed HA issue with the private (instead of the shared) MAC address being used as source for outgoing traffic
- **COP-5236:** A wrong hostname could be used upon DNS lookup as a consequence of LDAP server connections by the SGW.
- **COP-5253:** Old ICMP conns were not removed after a reconfiguration.
- **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-5306:** No log messages were generated if the system runs out of TCP send and receive buffers. Log messages have been added.
- **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-5333:** The default value for max number of SMTP sessions has been lowered to 200 to preserve memory. Please note that this value should be adjusted to fit your organization's need.
- **COP-5337:** SSL version 2.0 client hello messages larger than 127 byte were not handled correctly.
- **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-5386:** In some cases Web Content Filtering failed to parse URLs that contained commas.
- **COP-5422:** The SMTP ALG sometimes handled SMTP traffic incorrectly if the last part of the mail was not received in one chunk.
- **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-5461:** Multicast and broadcast traffic that were logged due to a low TTL, would incorrectly log the minimum TTL setting for unicast traffic.
 - **COP-5464:** Fixed HA resend/failover issue in DHCP Server.
 - **COP-5471:** An invalid IKE certificate payload could cause a service stop when running ikesnoop in verbose mode.
 - **COP-5488:**
 - **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-5501:** 'Updatecenter -status' command did not change from displaying "Initializing...". This defect was only cosmetic and did not affect the auto update functionality.
 - **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-5556:** IP fragmentation could cause TCP sequence number validation to lose track of the transmission window and start to drop all segments.
 - **COP-5638:**
 - **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.

3.6. Addressed Issues in CorePlus 8.80.04

- **COP-3162:** SNMP Interface OperStatus was only updated during startup and reconfiguration, resulting in a non trustable status.
- **COP-3533:** The L2TP server failed in some cases to send traffic over an L2TP tunnel to the client, forcing the client to reconnect in order to send traffic over the tunnel.
- **COP-4261:** VPN-Tunnels that were configured without a Remote Gateway caused the ipsectunnel command to show the Remote Net instead of Remote Gateway.
- **COP-4847:** The DHCP Relay MaxLeaseTime was previously 24 hours, causing problems if the DHCP lease time was higher. The MaxLeaseTime is now increased to 68 years.
- **COP-4950:** Under certain circumstances there was not possible to establish new IPsec tunnel because the IPsec engine falsely reported that it had run out of Phase-1 SA:s.
- **COP-5068:** The following SNMP Advanced settings was previously limited to 32 characters: SNMPSysContact, SNMPSysName and SNMPSysLocation. The new limit is 255 characters.
- **COP-5072:** SMTP commands were under certain circumstances incorrectly parsed, allowing blacklisted addresses to faultily pass through the SMTP ALG.
- **COP-5087:** NAT keep-alive messages for all IPsec SAs was sent in a single burst, causing heavy load on the CPU when having a large number of active SAs.
- **COP-5166:** The 'Outer Interface Filter' specified on an 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-5181:** The HTTP-ALG failed to forward data to the receiver if the HTTP server announced a content-length value larger than the actual file size to be transmitted.
- **COP-5258:** SSL/TLS handshake with the gateway failed if 4096 bit keys were used.
- **COP-5295:** Dynamic route synchronization for IPsec tunnels caused issues with disconnected clients when multiple L2TP/IPsec clients were behind the same NAT gateway.
- **FNT-254:** After deleting an object in a sorted list, wrong object was selected.

3.7. Addressed Issues in CorePlus 8.80.03

- **COP-3198:** The SNMPv1 ifSpeed counter was of the wrong data type (Counter32 changed to Gauge32).
- **COP-3201:** SNMP statistics for bps in and out per interface showed unrealistically high values during reconfiguration.
- **COP-3275:** The MAC addresses were earlier displayed in a non standard notation. They are now displayed using the following notation: xx-xx-xx-xx-xx-xx.
- **COP-3392:** IKE SAs were removed when a SGW goes from active to inactive in a HA cluster. Previously, the IKE SAs remained at the inactive member and could cause tunnel establishing problems when it got active again.
- **COP-3464:** Routes added by IPsec was not synced between cluster members.
RESULT: Connections that were synchronized to the cluster member and that had the tunnel as an endpoint would be removed on the inactive node. When a fail over occurred the active node did not have any state of connections going through the IPsec tunnel.
- **COP-3984:** User web authentication redirection did not work if a file path was requested. It is possible to set up SAT/NAT rules in combination with user authentication and redirect all http requests to the login page. This did not work if the specified request was a request with a file path e.g. "www.domain.com/somepath".
- **COP-3998:** IPSec tunnels were dropped upon reconfiguration. Configuration deployment caused all established IPSec tunnels to be dropped even though the change did not affect the configuration of the IPsec tunnel.
- **COP-4229:** The Multiplex rule did not previously work in NAT scenario.
The multiplex rule (used to handle multicast traffic) did not work correctly with NAT'ed traffic.
RESULT: With this fix, NAT rules will correctly rewrite source IP even with multiplexed traffic. Normal IP NAT rules are honored, as well as NAT/SETSRC rules. This does NOT include support for PORT-NAT/SAT.
- **COP-4342:** Sender and recipient e-mail addresses were missing in the SMTP log messages.
- **COP-4343:** The zip decompression functionality (used by the Anti Virus functionality) failed to decompress certain types of zip files.
- **COP-4517:** The security gateway rebooted indefinitely when a configuration was uploaded that contained a VLAN interface that had a NULL interface as a physical interface. This only happened in HA scenarios.
- **COP-4519:** The PPP/CCP implementation used by PPTP/L2TP could not handle the case when a peer rejects the MPPE/MPPC option.
- **COP-4526:** Threshold rules connection rate limiting included connections that would not be

allowed by the threshold rule in the rate computations.

- **COP-4530:** Whitelisted hosts were allowed to exceed the threshold of protect actions that triggers blacklisting.
- **COP-4535:** Anti Virus updates were downloaded even though no Anti Virus was configured.
- **COP-4539:** HTTPS User Auth. was not able to use 4096 bit certificates
- **COP-4549:** Anti Virus log messages did not use a standardized format.
- **COP-4562:** IDP and Antivirus signature downloads was not terminated correctly when the download was aborted by a reconfiguration.
- **COP-4573:** The security gateway could under some circumstances hang if the Anti Virus scanning was enabled.
- **COP-4592:** HTML encoded e-mails could in some circumstances be corrupted when passing through the SMTP-ALG
- **COP-4639:** If one or more interfaces was configured with 0.0.0.0 as IP address the SGW would use it as local IP address in IKE negotiations.
RESULT: IKE negotiations failed in phase 2.
- **COP-4650:** Small files were sometimes passed through the HTTP-ALG without being scanned by the AntiVirus engine.
- **COP-4674:** Problem to establish multiple IPsec tunnels with a remote peer using ID lists.
It was not possible to establish more than one tunnel to a remote peer if ID lists were used.
- **COP-4683:** Problems with the ServerFilter in IPPools.
If the server filter was specified together with a server ip address, it was not properly enforced until a reconfigure of the SGW took place.
RESULT: After a reconfigure previously accepted leases could become disallowed and be released.
- **COP-4689:** The TCP stack did not announce a zero-sized receive window when the receive buffer was full.
- **COP-4698:** The SMTP-ALG blocked server-to-server SMTP transactions.
E-mails were incorrectly discarded by the SMTP-ALG. The sending server received no indications of that the transaction had failed.
- **COP-4702:** The IDP engine was previously limited to 8000 signatures.
- **COP-4728:** HTTP-ALG blocks traffic from web-servers that generate erroneous HTTP-headers.
Some web-servers did not terminate HTTP headers correctly which resulted in blocked data transfer. The ALG now accepts these http-headers.
- **COP-4793:** Problem in certificate validation during IKE negotiation
There was a problem with the certificate validation in the IKE negotiation that under certain circumstances caused the gateway to stop responding.
- **COP-4821:** Web Content Filtering stopped working if the connection to the current CSPN server was lost.
- **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-4865:** A problem with the pattern matching engine (used by the UTM functionality) could cause the SGW to restart under certain extreme conditions.
- **COP-4907:** No logging were previously done when the SGW failed to resolve the IP addresses from the update servers.

-
- **COP-4915:** User Authentication failed when HTTPS was used in conjunction with a RADIUS server configured to use challenge response authentication.
 - **COP-4925:** The wrong type of log event was generated when the SGW received an invalid IPsec proposal.
 - **COP-4947:** UDP encapsulated ESP packets are dropped after HA failover. EAP-SIM clients behind NAT cause problems in case of HA failover. After a failover will the new active node fail to lookup incoming UDP encapsulated ESP packets and as a consequence drop the packets.
RESULT: Calls are dropped upon failover.
 - **COP-4953:** SMTP-ALG blocking transactions missing content-transfer-encoding. The gateway used fail-mode parameter to handle smtp transactions missing the content-transfer-encoding. Transactions not specifying content-transfer-encoding is now according to RFC 2045 assumed to be 7bit.
 - **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.
RESULT: Route failover did not work properly for monitored routes that pointed to a PPTP client as a disconnected tunnel wouldn't be restored again.
 - **COP-4986:** The DHCP Server did not support DHCP release requests from clients.
 - **COP-4995:** GZIP decompressor can give erratic virus detection results
The GZIP decompressor can in some cases give false positives and mark a file as infected even though the file is actually clean.
 - **COP-4999:** Update servers are pinged even when AV/IDP updates and WCF are disabled
The update servers are no longer pinged if none of the services anti-virus automatic updates, IDP automatic updates or web content filtering is enabled.
 - **COP-5002:** IPPool reusing DHCP client problem
Reused DHCP clients in the IP pool will under certain circumstances be treated as a new client by the DHCP server
RESULT: The dhcp server will create a new instance for the client (no problem unless full usage of the ip span)
 - **COP-5004:** HWM stat values are displayed correctly.
HWM stat values were incorrectly sent as integer numbers without proper conversion.
RESULT: The values are now set as proper integer numbers.
 - **COP-5023:** SMTP-ALG fails to discover viruses in e-mails encoded using quoted-printable
The SMTP-ALG failed to correctly decode quoted-printable encoded e-mails.
 - **COP-5037:** DHCPRELEASE problem in IPPools
The DHCP client in IPPool did not always send DHCPRELEASE when removing clients

3.8. Addressed Issues in CorePlus 8.80.02

- **COP-3427:** DNS update of IPsec tunnels can cause a dead lock.
- **COP-3518:** The console command "ipsecstats -num 0" failed to show all tunnels as intended.
- **COP-3962:** There were routing problems when trying to establish L2TP tunnels from Microsoft Windows Vista due to a changed behavior in the NAT traversal functionality.
- **COP-3983:** Files larger than 4GB could not be handled by the HTTP ALG.
- **COP-4104:** Incorrect value of internal severity in the log message for some IPsec SA events.

The value for internal severity called `int_severity` will be incorrect for `ipsec_sa_event` log messages. RESULT: `in_severity` in the `ipsec_sa_event` log message will be incorrect.

- **COP-4175:** A problem with the MIME type recognition caused the integrity check to faulty block some files.
- **COP-4371:** Empty IDP signature groups were erroneously shown.
- **COP-4409:** IP-packets with high protocol numbers would not be forwarded through the system when using Allow or NAT rules. Allowing the traffic using FwdFast rules would however work.
- **COP-4435:** HTTP-ALG: When configured to strip scripts like activeX in combination with anti-virus scanning, data transfer can be interrupted resulting in corrupted downloaded files
- **COP-4486:** There was a problem in collecting statistical data from several concurrent Netcon connections due to a fixed limit in the number of sessions allowed. An advanced setting (`NetConMaxChannels`) is added to control the maximum amount of concurrent connections.
- **FNT-198:** Double clicking on a removed rule in the usage box made FineTune crash.

3.9. Addressed Issues in CorePlus 8.80.01

- **COP-4347** The scan engine that is used for both Anti-Virus and IDP scanning is not working correctly under some circumstances.
- **COP-4327** The security gateway might hang during heavy load when using mime type validation or Anti-Virus scanning.
- **COP-4283** ARP traffic must be accepted by an access rule to make the gratuitous ARP functionality work properly.
- **COP-4234** ALGs configured with the setting "Verify MIME-type against File Content", might block files due to MIME type mismatch even though the files are authentic.
- **COP-4238** The configuration system accepts email blacklist entries that are incorrectly formatted.

3.10. Addressed Issues in CorePlus 8.80.00

- **HA synchronization problems of IPSec tunnels on SG50 appliances.** HA synchronization of IPSec tunnels did not work correctly on SG50 appliances, leading to problems renegotiating tunnels after an HA hand-over.
- **HA heartbeats are not sent often enough if many interfaces are configured.** HA cluster heartbeats are not sent often enough on each interface on security gateways with many configured interfaces.

4. Installation Instructions

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the Clavister CorePlus Admin Guide 8.80.

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.
- **SMTP ALG limitation.** The SMTP-ALG will deny relaying of e-mails if the e-mail user agent has been configured to use "TLS if available". A fall back to non-encrypted transfer is not possible.

6. Compatibility

The following section outlines the direct compatibility considerations as of CorePlus 8.80.09.

- **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
Web: <http://www.clavister.com/support/>