NetDefendOS Version: 2.26.01

Published Date: 2010-01-29

Copyright © 2010

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, 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 D-LINK 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 D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

Content:

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
2.26.01	Jan 29 2010	DFL-160 DFL-210/800/1600/2500 DFL-260/860/1660/2560/2560G	A1/A2 (for all models), A3/A4/A5 (for DFL-210/800/1600/2500),B1 (for DFL-260/860)
2.26.00	Sep 15, 2009	DFL-210/800/1600/2500 DFL-260/860/1660/2560/2560G	A1 (for all models), A2/A3/A4/A5 (for DFL-210/800/1600/2500)
2.25.01.28	July 15, 2009	DFL-210/260/800/860/1600/2500	A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500)
2.25.01.22	Jun 11, 2009	DFL-210/260/800/860/1600/2500	A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500)
2.20.03	Oct 21, 2008	DFL-210/260/800/860/1600/2500	A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500)
2.20.02	Jul 10, 2008	DFL-210/260/800/860/1600/2500	A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500)

Upgrading Instructions:

Upgrading by using CLI via SCP protocol

SCP (Secure Copy) is a widely used communication protocol for file transfer. No specific SCP client is provided with NetDefendOS distributions but there exists a wide selection of SCP clients available for nearly all workstation platforms. SCP is a complement to CLI usage and provides a secure means of file transfer between the administrator's workstation and the NetDefend Firewall. Various files used by NetDefendOS can be both uploaded and downloaded with SCP. This feature is fully described in *Section 2.1.6, "Secure Copy" of NetDefend Firewall v2.26.01 user Manual*.

Upgrading by using Web-UI

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the *NetDefend Firewall v2.26.01 User Manual.*

New Features:

Fireware Version	New Features
2.26.01	1. The name of the authenticated user is logged together with the requested URL in HTTP ALG log messages 2. DFL-160 only: DHCP relaying through the firewall in transparent mode is supported 3. DFL-160 only: DH Group and PFS can be configured on IPsec interfaces

2.26.00	1. The name of the authenticated user is logged together with the requested URL in HTTP ALG log messages 2. DFL-210 and DFL-800 support anti-virus and dynamic web content filtering
2.25.01.28	No new features in this version. This firmware version is positioned to replace v2.25.01.22 because the v2.25.01 will cause device into cycle reboot when IPSec encapsulation was set as "Both".
2.25.01.22	1. Added version check for external language files 2. Improved logging for Anti-SPAM 3. New log message at failover triggered by linkmon 4. A new advanced setting has been added to control the number of RADIUScommunication contexts that can be used simultaneously 5. DNS name resolving uses the shared IP in High Availability setups 6. Added support for Host Monitor for Routing 7. Added command to handle language files on disk 8. Improved LDAP functionality 9. Redesign of the tuple value controller in the webUI 10. Display of network objects 11. Extended route monitoring capabilities 12. The IPsec status page has been improved 13. PCAP Recording 14. New advisory link in virus found log messages 15. The webUI has been extended to handle child objects in a tab 16. Support of custom monitor interval in Linkmonitor 17. ZoneDefense now supports DGS-3200 series switches 18. Anti-Virus triggered ZoneDefense 19. LDAP Authentication 20. Route Load Balancing 21. Extended SIP Application Layer Gateway supporting new scenarios 22. TCP transport added to the SIP Application Layer Gateway 23. Multiple media connections for SIP Application Layer Gateway 24. PPTP server support for multiple PPTP clients behind the same NAT gateway 25. PPTP server and client have been extended to support stateful MPPE 26. Improved verification of IP4 values 27. IDP Triggered Traffic Shaping 28. AVSE_MaxMemory setting has been removed 29. Relayer IP address filter at DHCP Server 30. Support for VLAN priority derived from IP DSCP precedence 31. Gigabit Traffic Shaping Support

	32. The PPPoE client has been changed to support unnumbered PPPoE 33. Improved server monitoring for Server Load Balancing 34. The ping CLI command has been improved 35. The schedule page has been improved 36. SSL/TLS Termination
2.20.03	1. No new features were introduced in the 2.20.03 release.
2.20.02	1. MTU can be configured for PPPoE Interfaces 2. MTU can be configured for PPTP/L2TP Client Interfaces.

Changes of Functionality:

Fireware Version	Modified Features
2.26.00	1. DFL-210 and DFL-800, remove IDP Maintenance Service

Changes of MIB & D-View Module:

Support memory usage and TCP buffer usage monitoring.

Problems Fixed:

Firmware Version	Problems Fixed
2.26.01	1. A configuration that contains a routing table loop could lead to the watchdog being triggered. Now the configuration will fail to be activated with the following message: "Dynamic routing configuration error, possible configuration loop". 2. Setting both "IKE Lifetime" and "IPsec Lifetime" to 0 seconds in an IPsec tunnel triggered a warning message on the console referring incorrectly to another property. 3. Proposal lists were not properly listed in command line "ipsectunnel -iface" output. 4. When using a user authentication rule for HTTPS with LDAP, an SSL socket was sometimes not closed, possibly resulting in instability. 5. It was not possible to use certificates that had no alternative name set. 6. Due to memory corruption occurring in some setups, the internal timers caused the firewall 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. 7. DFL-160: It did not work to have DHCP assigned IP on the WAN interface and at the same time relay DHCP requests to hosts on the LAN or DMZ in transparent mode. 8. The establishment of SYN flood protected TCP connection could be unnecessarily delayed due to the firewall dropping all the packets sent by the client side while waiting for the completion of the three-way handshaking between the firewall and the server. 9. Updates of the Anti-Virus database could only be done when the Anti-Virus functionality was enabled. The database can now be updated even though no Anti-Virus functionality is enabled 10. The license page showed an incorrect value for maximum number of PPP tunnels. 11. Running certain sequences of CLI commands (or performing corresponding actions in the Web User Interface) involving multiple "reject" commands, could cause a critical malfunction in some cases. 12. After running the CLI command "reject" with a configuration object as parameter, activation of configuration changes could fail with an error message, but "show -errors" would say that there were no errors. The "show -errors" command has been updated to correctly display these errors. 13. 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. 14. The console 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. 15. The system information slides on the front panel display could stop after showing the first sensor under certain conditions when Hardware Monitor was enabled. The system information slides can now loop through all pages without getting stuck. Only affected hardware models with front panel display. 16. There was a critical defect in the Web Content Filter functionality that could cause the firewall to reboot unexpectedly. 17. DFL-160: If the Internet connection had dynamic IP address (DHCP enabled) and transparent mode was used on LAN or DMZ, the IP address on the LAN / DMZ interface was set to 0.0.0.0.

2.26.00	1. PPP negotiations were sometimes slower than necessary. 2. Deploying a configuration during heavy traffic load could cause a watchdog reboot. 3. It was possible to enable the anti-spam feature DNSBL on an SMTP-ALG without specifying any DNSBL servers. Configuring DNSBL without specifying any servers will now give an error. 4. Some errors in IPsec tunnel configuration were not correctly treated during the firewall start up process, resulting in IPsec tunnels not properly being set up. Now most of those errors make the tunnel be disabled and a warning message be displayed. For the most severe ones the configuration will be rejected by the system. 5. Running FTP-ALG in hybrid mode could result in the first packet being dropped when the connection to the server isn't established, and this leads to a three seconds delay. The connection from the ALG to the client will now not be initiated until the server connection is established towards the ALG. 6. It was not possible to move a rule up or down in the list if the rule was disabled. 7. The command "ipsecstats" could in some circumstances not show all tunnels when a tunnel name was given as an argument. The command now displays all the tunnels when tunnel name is given as an argument. 8. The command "ipsecstats" only listed the first matching IPsec SA when a tunnel name was given as an argument. The command now displays all IPsec SAs that are connected to the specified tunnel name. 9. 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. 10. The "ippool - show" CLI command output showed all configured pools, which could be a very long list. Now only the first ten are listed by default. The "-max <num>" option can be used to display more items. 11. The SIP-ALG didn't handle "183 Session Message" when initiating a new SIP call. 12. 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. 13. Tab completion in the command line interface (CLI) did not work on IPsec tunnels when using the "ipsecstats" command. Tab completion is now possible to use in the "ipsecstats" command. 14. The firewall did not accept certificates signed with RSA-SHA256.

	15. Timezone setting could make the minimum date limit in scheduling to wrap and become a date into the future. The minimum and maximum dates in scheduling have been modified to be between the years 2000 and 2030 which will not trigger the incorrect behavior. 16. The SMTP-ALG incorrectly blocked emails sent using the CHUNKING (BDAT) extension. The ALG has been modified to remove the CHUNKING capability from the server's EHLO response. This allows the emails to pass through the ALG. 17. It was not possible to connect to the firewall using SSH if lots of public keys were registered in the SSH client. 18. The firewall could unexpectedly restart when disabling automatic updates of anti-virus and IDP updates. 19. IPsec tunnels with a DNS name as remote endpoint would cease to function after a remote endpoint IP address change. 20. Blacklist could potentially write to media up to five times each minute. The delay between possible writes has been increased to two hours. 21. It was not possible to configure "maximum authentication retries" for the SSH server in the web user interface. Configuration support has now been added. 22. There was a problem when multiple IPsec SAs referenced the same XAuth context. 23. If a DHCP lease of a reserved IP address was manually released in the DHCP server and the host requested a new lease, the host was not given the reserved IP again. 24. The UDP checksum was not correctly updated when the multiplex rule was used together with address translation (SAT SETDEST / NAT). 25. On some models, a data alignment error in the Route Load Balancing system could cause the firewall to malfunction. 26. Old configurations had an incorrect definition of the all_tcpudp service. Upgrading from an older version to a newer version could cause problems. This problem has now been fixed and the old service will be converted during the upgrade. 27. In some scenarios, login attempts using the web user interface failed with the error message "Error 500 - Internal Server Error". No new login attempts were allowed until the system had been restarted. A synchronization lock for an internal buffer failed to reset during reconfigure and caused this issue. 28. Scripts created by "script -create" could previously have problems to run even when executed with "script -execute -force", because the generated script would sometimes incorrectly reference an object before it had been added. This

	has been solved in such way that "script-create" always generates a script that will not reference an object before it has been created. Circular dependencies are resolved by first adding the objects without the problematic references, then later modifying the object to its final state. 29. Since the web user interface uses UTF-8 encoding, a PSK containing ASCII characters with value of 128-255 would be stored as UTF-8 characters. UTF-8 characters are now converted back to ASCII characters when it is possible.
2.25.01.28	1. If the IPSec encapsulation was configured as "Both" then upgrade firmware to v2.25.01.22, it will cause device into cycle reboot. 2. The WCF tab is shown on Non-UTM Firewall models. Basically, Non-UTM firewalls don't support dynamic WCF feature. It is no longer visible on non-UTM firewall models after upgrade to firmware v2.25.01.28. 3. Startup Wizard is not displayed after reset configuration to default via WebGUI.
2.25.01.22	1. The advanced setting Block0000Src{Drop, DropLog, Ignore, Log} has been renamed toLog0000Src{Drop, DropLog}.The actions Log andIgnore have now been converted into DropLog and Drop. 2. UpdateCenter caused problems in HA setups, sometimes locking up an HA node. HA alsocaused some problems for pseudo-reassembly 3. The behavior of the TCP reassembly has been changed slightly to avoid causing orcontributing to ACK loops 4. The firewall could generate multicast_ethernet_ip_address_mismatch log messages if itwas 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. 5. Configuration errors in SSH management setup were not reported to the user. 6. 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. 7. Log messages regarding denied update of anti-virus or IDP signatures were incorrectly generated when no valid subscription existed for that service. The log messages have been removed. 8. Redirecting HTTP users to the web authentication login page did not work correctly. 9. A change of an interface's name could lead to the drainage of free buffers that eventually caused the firewall to stop handling traffic. The root cause of the

	leakage has been identified and fixed. 10. The functionality of the CLI command 'urlcache' has been moved into the 'httpalg-wcfcache' command. The new 'httpalg' flag '-wcfcache' lists the hosts which have overridden the content filter. 11. A predefined list of file types were missing in the configuration for ALG file integrity and anti-virus scan exclusion. Specifying the file extensions can now be done with support of a list of extensions. 12. The arguments to the CLI command "arpsnoop" have been changed. To enable snooping on all interfaces "all" should now be used instead of "*" and "none" instead of "disable". 13. Some malformed HTTP URLs 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). 14. Previously, ARP monitoring would be disabled if there was no gateway to monitor. 15. Previously a route could not be configured to include its own gateway among hosts to monitor, if the gateway address was obtained via DHCP. 16. 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. 17. At shut down of the unit, connected SSH clients were not disconnected 18. The interface status page could show corrupted driver / hardware output when viewing VLAN interfaces. VLAN interfaces have no driver or hardware information so this field is now left empty. 19. Executing commands which used object arguments from within a script file did not work. It is now possible to execute such commands from within script files. 20. IP4HAAddress peer address was not shown in the WebUI and CLI address book views. The HA peer address is now displayed in address book listings. 21. Idling system backup download for more than 5 seconds aborted the download. It is now possible to idle up to two minutes without having the download being aborted. 22. 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.

	23. An HA node sometimes froze and had to be physically rebooted after updating IDP signatures via updatecenter. 24. The authentication method for IPsec tunnels was set to PSK as default value. When adding such tunnels from the CLI this was unclear. When using the CLI to create IPsec tunnels, the user must now explicitly specify the wanted authentication method. 25. Microsoft Windows LT2P over IPsec sessions could fail in the sequence of re-keys. 26. When using the CLI it was possible to add objects to already disabled folders. It is no longer possible to add objects to disabled folders. 26. The User Authentication logs sometimes contained faulty authentication information. Log events were also missing in some authentication scenarios 27. A file transfer scanned by the HTTP ALG with anti-virus activated could be aborted after a WindowZero event from the client. 28. 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'. 29. PCAP captures on non-Ethernet interfaces were missing Ethernet headers causing Wireshark to fail opening the files. 30. The configuration user and session stored for the configuration changes sometimes indicated that the wrong user session stored the configuration. Now, the correct user session parameters are stored. 31. In rare cases, the Web Content Filtering feature could trigger an unexpected restart of the firewall. 32. A lease for a static host 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. 33. The webUI memory logger search fields used partial matching. The search fields are now using strict matching with the possibility to use the wildcards '*' and '?'. 34. Outdated information was sometimes used when generating log events from the ALGs which could cause the device to restart. 35. It was not possible to select Local ID for certificates. Added configuration support for Local ID. 36. 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 that 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. 37. Route Fail Over status information was faultily printed on the console every time the state of the route changed. These printouts are now removed and only the log events remain. 38. Changing the high availability setting "use unique shared MAC" could make both nodes of a high availability cluster go active. 39. There was a dependency between link monitors which resulted in that the effective ping interval was reduced for each new link monitor configured. 40. The CLI was missing a quick and easy way to list the available runtime services. A 'services' CLI command has been added. This command lists the runtime values of configured services. 41. 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 firewall and a peer. 42. Netobject groups were not updated if the groups contained a dynamically changed (DHCP, PPPoE etc.) address. 43. IPsec-tunnels using DNS resolving of the remote gateway could sometimes not be established. The dynamic routes are now set properly for tunnels using DNS resolving of remote gateway. 44. Certain device parameters, such as the device name, were previously synchronized between the members of a HA cluster. To make it easier to distinguish between the members of a HA cluster; these parameters are no longer synchronized. 45. Route load balancing method spillover didn't take disabled routes into account. 46. 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. 47. When activating HA in the WebUI, the browser was redirected to the shared IP address of the management interface. Now, the web browser is redirected to the private IP of the management interface. 48. 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.

	49. 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. 50. The CLI command "arp -flush <interface>" did not work. It has now been corrected. Flushing the ARP cache on all interfaces using "arp -flush" did work though. 51. The firewall did not respond to TCP Keep-Alive packets. 52. Management sessions to the WebUI could on low throughput links timeout before the web pages have been fully loaded. The timeout of the sessions has been increased in order to better handle this scenario. 53. 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. 54. IPsec config mode configured with a static IP pool did not, in general, hand out the last address in a range to clients. 55. 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. 56. 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. 57. 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. 58. The HTTP-ALG blocked web pages with malformed charset statement in HTTP headers. 59. A misconfigured IPsec tunnel could in some scenarios cause the firewall to malfunction. 60. The firewall sometimes restarted unexpectedly when using IDP Pipes. 61. The LDAP client now handles authentication using PPP with CHAP, MS-CHAPv1 and MS-CHAPv2. 62. 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. 63. Removing the use of DHCP on multiple interfaces could in some rare cases during reconfigure cause the firewall to perform an unexpected abort. Protection has been added to the timeout handling routine of DHCP.

	64. HTTP-ALG generated information pages, e.g. Restricted site notice, could get incorrectly cached by downstream proxy servers. This could lead to proxy servers returning a cached error message even though no error page should be seen. 65. The OSPF Interface was missing the 'network' configuration parameter. This caused problems in certain setups where IPsec tunnels configured with 0.0.0.0/0 as remote or local network. If the network parameter is not set, the network parameter is copied from the configured interface. 66. The PPPoE client option "Force Unnumbered PPPoE" did not force Unnumbered PPPoE to be used. 67. Under certain Traffic Sapping settings, lower precedences stop forwarding traffic when higher precedences start forwarding traffic. 68. Configurations containing names or comments using certain special characters could cause the firewall to fail reading the configuration during startup.
2.20.03	1. ICMP Destination Unreachable packets were not sent when UDP packets hit a Reject rule. 2. Web authentication and web server connections were not closed correctly at reconfiguration. 3. 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). 4. HA setups with IDP scanning enabled, packets could be lost during a failover. 5. Some services were using the private IP in HA setups for communicating. This is now changed and the shared IP is used. 6. The DNS lookup of the IP address to a remote gateway failed under certain circumstances for IPSec interfaces. 7. The CLI command for displaying updatecenter AV/IDP update status did not show enough information. It has now been improved. 8. TCP connections could sometimes fail due to an incorrect sequence number check. 9. A missing Content-Transfer-Encoding header field in e-mails could sometimes cause the SMTP-ALG session to malfunction. 10. 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.

11. 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.
12. IP address with suffixes .0 and/or .255 could incorrectly be assigned to IPSec config mode clients.
13. 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.
14. A user logging in via Web based user Authentication, when configured to handle user credentials via one or several RADIUS servers, it could cause an unexpected abort if no RADIUS server was reachable. This issue has been fixed.
15. The web user interface, the properties in "Dynamic Black Listing" were incorrectly enabled when action was set to something else than "protect".
16. The icon for removing IKE SA was missing, hence making it impossible to remove an IKE SA using the web user interface.
17. 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.
18. Email attachments with very long file names could cause memory corruption in the SMTP-ALG.
19. 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.
20. When restarting an interface on the DFL-1600 or DFL-2500, there has been a theoretical possibility of memory corruption. This issue has been fixed from

	F/W v2.20.02 and later. 21. Connections were, under certain circumstances, incorrectly dropped by the IDP scanning engine when audit mode was used. 22. After IPSec tunnels were modified, the reconfiguration of the gateway was not done correctly. The result was that the gateway could go into unexpected abort state. 23. A configured external log receiver that does not accept log messages might send ICMP destination unreachable packets to the firewall. 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 firewall when it receives ICMP destination unreachable packets regarding log receiver connections. 24. TCP connections with SYN relay were not synchronized correctly. In case of HA failover, traffic on these connections would freeze. 25. 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. 26. 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. 27. The Fail Mode setting in the HTTP-ALG was not honored by the Dynamic Web Content Filtering. 28. The log message for expired or no valid Web Content Filtering license did only show up once. There is now a log message generated once a one minute. This should be more noticeable to the administrator. 29. 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. 30. It was not possible to configure the primary NBNS server for L2TP/PPTP server interfaces in the web user interface. 31. The TCP monitoring of Server Load Balancing did not increase TCP sequence number in the reset packet sent to server in case of connection timeout. The sequence number is now increased by one. 32. Server Load Balancing did not use All-To-One for port numbers. When using a range on the service, the destination port would be the specified port plus the offset from the low port number in the service. 33. One of the log messages had an incorrect format. When the log message was

	placed first in the log table, the web user interface memlog would display an empty page. 34. The description text for IP Pools incorrectly specified that IP Pools could be used by L2TP and PPTP. 35. A confusing Anti-Virus status message was visible in status page on non UTM capable devices. The message has been removed.
2.20.02	1. ICMP Destination Unreachable packets were not sent when UDP packets hit a Reject rule. 2. Web authentication and web server connections were not closed correctly at reconfiguration. 3. 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). 4. HA setups with IDP scanning enabled, packets could be lost during a failover. 5. Some services were using the private IP in HA setups for communicating. This is now changed and the shared IP is used. 6. The DNS lookup of the IP address to a remote gateway failed under certain circumstances for IPSec interfaces. 7. The CLI command for displaying updatecenter AV/IDP update status did not show enough information. It has now been improved. 8. TCP connections could sometimes fail due to an incorrect sequence number check. 9. A missing Content-Transfer-Encoding header field in e-mails could sometimes cause the SMTP-ALG session to malfunction. 10. 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. 11. 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.

12. IP address with suffixes .0 and/or .255 could incorrectly be assigned to IPSec config mode clients.
13. 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.
14. A user logging in via Web based user Authentication, when configured to handle user credentials via one or several RADIUS servers, it could cause an unexpected abort if no RADIUS server was reachable. This issue has been fixed.
15. The web user interface, the properties in "Dynamic Black Listing" were incorrectly enabled when action was set to something else than "protect".
16. The icon for removing IKE SA was missing, hence making it impossible to remove an IKE SA using the web user interface.
17. 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.
18. Email attachments with very long file names could cause memory corruption in the SMTP-ALG.
19. 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.
20. When restarting an interface on the DFL-1600 or DFL-2500, there has been a theoretical possibility of memory corruption. This issue has been fixed from F/W v2.20.02 and later.
21. Connections were, under certain circumstances, incorrectly dropped by the IDP scanning engine when audit mode was used.
22. After IPSec tunnels were modified, the reconfiguration of the gateway was not done correctly. The result was that the gateway could go into unexpected abort state.
23. A configured external log receiver that does not accept log messages might send ICMP destination unreachable packets to the firewall. 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 firewall when it receives ICMP destination unreachable packets regarding log receiver connections. 24. TCP connections with SYN relay were not synchronized correctly. In case of HA failover, traffic on these connections would freeze. 25. 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. 26. 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. 27. The Fail Mode setting in the HTTP-ALG was not honored by the Dynamic Web Content Filtering. 28. The log message for expired or no valid Web Content Filtering license did only show up once. There is now a log message generated once a one minute. This should be more noticeable to the administrator. 29. 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. 30. It was not possible to configure the primary NBNS server for L2TP/PPTP server interfaces in the web user interface. 31. The TCP monitoring of Server Load Balancing did not increase TCP sequence number in the reset packet sent to server in case of connection timeout. The sequence number is now increased by one. 32. Server Load Balancing did not use All-To-One for port numbers. When using a range on the service, the destination port would be the specified port plus the offset from the low port number in the service. 33. One of the log messages had an incorrect format. When the log message was placed first in the log table, the web user interface memlog would display an empty page. 34. The description text for IP Pools incorrectly specified that IP Pools could be used by L2TP and PPTP. 35. A confusing Anti-Virus status message was visible in status page on non UTM capable devices. The message has been removed.

Known Issues:

Fireware Version	Known Issues
2.26.01	1. The Oray.net Peanut Hull client does not work after they changed the protocol 2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance. 3. HA: No state synchronization for ALGs. No aspects 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. 4. 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. 5. Inactive HA member cannot send log events over tunnels. 6. Inactive HA member cannot be managed / monitored over tunnels. 7. 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. 8. 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. 9. 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.
2.26.00	1. The Oray.net Peanut Hull client does not work after they changed the protocol 2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance. 3. 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.

	4. 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. 5. Inactive HA member cannot send log events over tunnels. 6. Inactive HA member cannot be managed / monitored over tunnels. 7. 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. 8. 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. 9. 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.
2.25.01.28	1. The Oray.net Peanut Hull client does not work after they changed the protocol 2. HA: Transparent Mode won't work in HA mode There is no state synchronization for Transparent Mode and there is no loop avoidance. 3. HA: No state synchronization for ALGs No aspect of ALGs are state synchronized. This means that all traffic handled by ALGs willfreeze 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. 4. 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. 5. Inactive HA member cannot send log events over tunnels. 6. Inactive HA member cannot be managed / monitored over tunnels. 7. 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. 8. 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. 9. 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.
2.25.01.22	1. If the IPSec encapsulation was configured as both, when upgrade firmware to v2.25.01.22, it will cause device into cycle reboot. This problem has been fixed in v2.25.01.28. 2. The Oray.net Peanut Hull client does not work after they changed the protocol 3. HA: Transparent Mode won't work in HA mode There is no state synchronization for Transparent Mode and there is no loop avoidance. 4. HA: No state synchronization for ALGs No aspect of ALGs are state synchronized. This means that all traffic handled by ALGs willfreeze 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. 5. 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. 6. Inactive HA member cannot send log events over tunnels. 7. Inactive HA member cannot be managed / monitored over tunnels. 8. 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. 9. 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. 10. 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.
2.20.03	1. The Oray.net for Peanut Hull DDNS client does not work after supplier changed the protocol. 2. HA: Transparent Mode won't work in HA modeThere is no state

	synchronization for Transparent Mode and there is no loop avoidance. 3. HA: No state synchronization for ALGsNo 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. 4. HA: Tunnels unreachable from inactive nodeThe 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. 5. 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. 6. 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.

Related Documentation:

- NetDefend Firewall User Manual v2.26.01
- NetDefend Firewall CLI Reference Guide v2.26.01
- NetDefend Firewall Logging Reference Guide v2.26.01