
**NetDefendOS Version:** 2.27.30-RU

**Published Date:** 2015-03-22

Copyright © 2015

*Note: this version is dedicated for Russian territory only.*

## 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 |
|---|---|---|---|
| 2.27.30-RU | Mar. 27 2015 | DFL-260E/860E/1660/2560/2560G DFL-1600/2500 | A1 (FL-860E/1600/2560/2560G) A2 (DFL-260E/1600/2500) |
| 2.27.08-RU | Feb. 02 2014 | DFL-210/800/1600/2500 DFL-260/860 DFL-260E/860E/1660/2560/2560G | A1 (for all models), A2 (for DFL-210/260E/800/1600/2500), A3 (for DFL-210/800/1600), A4/A5 (for DFL-210), B1 (for DFL-260/860) |
| 2.27.07-RU | Apr. 03 2013 | DFL-210/800/1600/2500 DFL-260/860 DFL-260E/860E/1660/2560/2560G | A1 (for all models), A2 (for DFL-210/260E/800/1600/2500), A3 (for DFL-210/800/1600), A4/A5 (for DFL-210), B1 (for DFL-260/860) |
| 2.27.06-RU | Oct. 30 2012 | DFL-210/800/1600/2500 DFL-260/860 DFL-260E/860E/1660/2560/2560G | A1 (for all models), A2 (for DFL-210/800/1600/2500), A3 (for DFL-210/800/1600), A4/A5 (for DFL-210), B1 (for DFL-260/860) |
| 2.27.05-RU | Dec 26 2011 | DFL-260E/860E/1660/2560/2560G | A1 (for all models), A2 (for DFL-2560G) |
| 2.27.04-RU | April 30 2011 | DFL-210/800/1600/2500 DFL-260/860/1660/2560/2560G DFL-260E/860E | A1 (for all models), A2 (for DFL-210/800/1600/2500), A3 (for DFL-210/800/1600), A4/A5 (for DFL-210), B1 (for DFL-260/860) |
| 2.27.02-RU | Sep 13 2010 | DFL-210/800/1600/2500 DFL-260/860/1660/2560/2560G | A1 (for all models), A2 (for DFL-210/800/1600/2500), A3 (for DFL-210/800/1600), A4/A5 (for DFL-210), B1 (for DFL-260/860) |
| 2.27.00-RU | May 14 2010 | DFL-210/800/1600/2500 DFL-260/860/1660/2560/2560G | A1 (for all models), A2 (for DFL-210/800/1600/2500), A3 (for DFL-210/800/1600), A4/A5 (for DFL-210), B1 (for DFL-260/860) |

## 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 v2.27.05 user Manual*.

### Upgrading by using Web-UI

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the *NetDefend Firewall v2.27.05 User Manual.*

## New Features:

| Firmware Version | New Features |
|---|---|
| 2.27.30-RU | **1. True Application Control:**<br>The addition of Application Content Control allows for granular policies using application attributes to control the contents of data streams for applications. This will not only allow for granular policies on an application level, but also on an application content level, such as restricting access to certain usage of application functions such as web browser version control, blocking of DNS queries for certain domains and blocking of mail transfers containing certain keywords in the subject field. This will also allow for granular logging of the contents of data streams generated by the applications and protocols, providing an unprecedented audit view of data that applications in the network transmit.<br>**2. SSL Inspection for Application Control:**<br>This new feature provides D-Link NetDefendOS the capability to identify applications that use the HTTPS protocol. Based on the result, the applications can be bandwidth managed, blocked and/or logged.<br>**3. IKE/IPsec HA synchronization:**<br>Full HA synchronization of established IKE negotiated IPsec tunnels are now supported, providing full redundancy for service critical installations where IPsec tunnels are used. Fully established IKE and IPsec SAs are now synchronized to the inactive HA cluster node, making it possible to keep tunnels up and running throughout a node failure, restart or upgrade, eliminating the need to renegotiate the tunnel after HA system fail-over. Fail-over times should be less than a second and the impact on routed packets over the tunnel is minimal. Note, only available on DFL-1660, DFL-2560 and DFL-2560G.<br>**4. IKE/IPsec Virtual Routing support:**<br>Virtual Routing for IKE/IPsec tunnels is now supported, which allows for flexible usage of IKE/IPsec tunnels in more complex networks with overlapping IP ranges, or where multiple routing tables are used. In practice this means that you can now terminate or initiate IKE and IPsec traffic in any routing table and not only in the main routing table. It also allows for a more flexible configuration of an IKE/IPsec tunnel, where it is possible to configure any ARP or core routed IP to listen on for incoming IKE/IPsec traffic, and not only the interface IP |

address.

**5. Link Aggregation support:**

IEEE 802.1AX-2008 and 802.3ad Link Aggregation for 1 Gbps Ethernet links with static link aggregation and LACP negotiated link aggregation is now supported.

**6. Improved anti-virus scanning:**

The anti-virus engine has been improved to support the latest streaming based technologies from Kaspersky, improving protection for malicious scripts, URLs and files transported through the system.

**7. 6-in-4 Tunneling:**

The new 6-in-4 Tunneling feature is a transition mechanism that enables customers that lack native IPv6 connectivity to setup a tunnel towards a Tunnel Broker using IPv4 and thereby be able to access IPv6 hosts and offer services on IPv6. This feature greatly simplifies configuring mixed networks and enables customers to continue to use IPv4 only services in a more transparent way.

**8. Support for IEEE 802.1ad (QinQ) Service VLAN:**

NetDefendOS already provide fine granularity for configuring 802.1q tagging, enabling customers to configure the same 802.1q tag on different Ethernet Interfaces. With the addition of 802.1ad it is now possible to configure QinQ, using 802.1q VLANs on top of Service VLANs (802.1ad VLANs). This new feature is very useful in service provider scenarios or for larger enterprises.

**9. PCAP support in the Web User Interface:**

A PCAP tool has been added to *Status->Tools* to allow control over packet capturing from the web user interface. Some of the more common filters and options are available to specify and it is possible to start, stop and download packet captures.

**10. Added Diagnostic Console Page in the Web User Interface:**

The Diagnostic Console collects system critical logs and is used to help troubleshooting of internal problems within the system. To ease access to the Diagnostic Console, it is now available under *Status->Maintenance->Diagnostic Console* in the web user interface.

**11. DHCP Client Enhancements:**

The DHCP Client is now supported on VLAN interfaces.

**12. PPPoE Client Enhancements:**

It is now possible to use the PPPoE client over VLAN as well as Ethernet Interfaces.

**13. RADIUS Enhancements:**

This release has added support for the Framed-IP-Netmask attribute. This

attribute together with the Framed-IP attribute can be combined to generate a route. This enables customers to set up VPN tunnels using RADIUS authentication with L2TPv2/IPsec.

**14. Command-Line Interface (CLI) Enhancements:**

The Command-Line Interface (CLI) now supports viewing and filtering the Memory Log using CLI commands.

**15. User Identity Awareness Enhancement:**

The User Identity Awareness Agent has been updated with a protocol that supports a larger number of group memberships for a user.

Note: NetDefendOS 10.21.02 and up is required for use with this new 1.01.00 Agent version.

**16. ZoneDefense with Universal MIB:**

ZoneDefense now supports switches that use the Universal MIB.

**17. Diagnostics & Quality Improvements:**

To improve the quality of the product, anonymous usage information is sent to the manufacturer. The data sent is encrypted and contains information such as firmware version, UTM database versions, uptime and memory usage. The type of diagnostic data sent can be tuned in the configuration and can also be completely disabled.

**18. Source IP selection for RADIUS requests:**

The RADIUS server configuration has been enhanced with the possibility to manually specify the source IP for RADIUS requests.

**19. DHCPv6 Server support:**

The system now includes support for DHCPv6 Server, which can be used to configure IPv6 hosts with IP addresses, IP prefixes and/or other configuration required to operate on an IPv6 network.

**20. RADIUS Relayer:**

The system now supports acting as a RADIUS Relayer, which can provide user information and DHCP IP provisioning for RADIUS-based authenticated users, for example, when a user roams over from a cellular network to an Enterprise WiFi network for data access. This is useful as it allows for granular user and group based policing of traffic, controlling access to network resources.

**21. ARP Authentication:**

A new authentication agent has been added that makes it possible to authenticate users based on the MAC address in the firewall's ARP cache as username. Supported authentication sources are external RADIUS and LDAP databases.

**22. RADIUS server retry:**

| | |
|---|---|
| | Configuration options have been added to make the firewall able to retry contacting the primary RADIUS server if failing to contact the backup servers configured.<br>**23. Web Content Filtering update:**<br>Web Content Filtering category 31 has been changed from "Spam" to "Remote control/desktop".<br>**24. Improved certificate information in the CLI:**<br>The CLI has been improved to show more detailed information about the IPsec certificate cache.<br>**25. Alias for routes**<br>It is now possible to use "route" as an alias to the CLI command "routes".<br>**26. High Availability Status in the Web User Interface**<br>The current High Availability status is now visible in the "System Information" list on the main status page in the web user interface. |
| 2.27.07-RU | 1. Added the DHCP server when used with MAC address authentication to enable automatic logout of users. When an IP address is being reused from the DHCP server and the old user was logged in via MAC authentication, the DHCP server sends a logout message to log out the old user from the system.<br>2. Added "IPA" as recognized MIME type.<br>3. Support for hardware acceleration of IKE negotiations for DFL-2560/2560G to offload the CPU and make IPsec setup faster. |
| 2.27.06-RU | No new features were introduced in the 2.27.06 release of NetDefendOS. |
| 2.27.05-RU | 1. The WebUI page "Reset" now also contains a method for normal shutdown (same action as the CLI command "shutdown"). This method will gracefully close down tunnels, hand over to other HA unit (in HA scenarios) and so on.<br>2. The cache size for the Web Content Filtering (WCF) feature has been increased. The size is now doubled on all hardware models.<br>3. The drop down menu for services has been enhanced to show port numbers. |
| 2.27.04-RU | 1. The File Integrity tab for ALGs has been re-arranged with a more logical view for MIME type check.<br>2. Added possibility to sort data grids. Sorting on anything except column index will hide grouping.<br>3. New setting for High Availability failover timeout value that specify the timeout before HA failover is triggered. |
| 2.27.02-RU | 1. The D-Link DES-3528 switch can now be used by ZoneDefense.<br>2. A new log message has been added indicating that an ARP resolve query failed. |

| | |
|---|---|
| | 3. The following browsers are now supported: Firefox 3+, Opera 10.5+, Safari 3+, Internet Explorer 7+ and Chrome 4+.<br>4. A confirmation question will be prompted if the user attempts to execute a CLI command that may cause system delays. |
| 2.27.00-RU | 1. Grouping configuration objects into logical groups makes it easier to manage large number of configuration objects. It is also possible to add a descriptive description and custom color to distinguish what these objects do. This grouping functionality is only for presentation and does not affect the existing functionality.<br>2. Logging enabled by default on rules for the following objects: Access, DHCP Server, DHCP Relay, Routing Rule, Dynamic Routing Policy Rule, IDP Rule Action, IP Rule, OSPF Router Process, Threshold Action and User Authentication Rule.<br>3. Static configuration objects default to their default values if the objects contain configuration errors. This will prevent the firewall to misbehave due to configuration errors on static objects.<br>4. The script command has been updated to handle adding objects with dependencies between each other.<br>5. User authentication has been updated with a new authentication source that will grant access to the user without checking any credentials. This functionality can be used to authenticate users from within login scripts etc, to make auditing easier.<br>6. All rule page layouts have been updated for how to enter the interface and network combination to be more intuitive.<br>7. The data grid in the Web User Interface now displays information for simple objects as tooltip (an example is a reference to an IP4Address which would show the address value as a tooltip). |

## Changes of Functionality:

| Firmware Version | Modified Features |
|---|---|
| 2.27.xx | 1. RU firmware version doesn't support over 56bit encrypted algorithm according to regulatory restriction. |

## Changes of MIB & D-View Module:

Support memory usage and TCP buffer usage monitoring.

## Problems Fixed:

| Firmware Version | Problems Fixed |
|---|---|
| 2.27.30-RU | 1. Source Address Translation 'Auto' would not result in correct behavior when configuring IPPolicies.<br>2. Fragmented traffic sent through an IPsec tunnel was sometimes dropped.<br>3. No error was generated when configuring HTTPS management without selecting an HTTPS certificate.<br>4. The Router Advertisement related settings had inconsistent naming. The names have been updated and a configuration converter has been added so that existing behavior is kept after upgrade.<br>5. IPsec interfaces could not be used by OSPF to communicate with a neighbor.<br>6. Connections using the secondary route in a route monitor setup where the primary route had failed were incorrectly closed during reconfiguration.<br>7. A firewall with User Identity Awareness configured could in rare scenarios reboot unexpectedly.<br>8. Memory consumption could in rare circumstances increase when an authenticated user timed out from a RADIUS server.<br>9. Configuring OSPF to run on top of VLAN interfaces did not set the VLAN's Ethernet base interface's receive mode parameter to accept OSPF multicast packets, causing OSPF communication fail in some scenarios.<br>10. The Web User Interface selection box was not wide enough, which made long object names not being displayed in full.<br>11. Error messages output by the "time -sync" command were in some failure cases not informative enough to describe the problem.<br>12. On rare occasions, the firewall could perform an unexpected restart after reconfiguring a PPTP server that used LDAP authentication.<br>13. Configuring an IPv6 core route would always cause a configuration warning.<br>14. Traffic passing through an IPsec tunnel was sometimes incorrectly dropped if there was fragmentation of the packets.<br>15. Valid UTF-8 characters were in some logs not shown properly.<br>16. UDP packets sent from the firewall when using the ping CLI command always had the same Fragmentation ID or Identification field set.<br>17. The output from the "time -sync" command was shown in all active CLI |

| | |
|---|---|
| | sessions. It will now only appear in the session where the command was executed.<br>18. The description of the Facility parameter in the Syslog Receiver configuration object was incorrect.<br>19. The device could restart unexpectedly when Application Control was disabled on an IPRule matching active IPv6 traffic<br>20. Certain rare certificates could not be added to the configuration.<br>21. Web Content Filtering did not work for HTTPS when the traffic was directed to a proxy.<br>22. Descriptions were missing for some advanced settings alternatives.<br>23. The DHCP Server Custom Option parameter value was possible to leave empty, but gave an error message during Save & Activate. An error message is now shown if the value is left empty when clicking Ok on the Custom Option page.<br>24. Application Control frequently failed to recognize Skype. Changes have been made to improve the classification of Skype.<br>25. Application Control sometimes identified the application as just TCP or just UDP.<br>26. Using an IP4Address object with a DNS name as Remote Endpoint for an IPsec tunnel could lead to IPsec traffic problems.<br>27. In rare occasions, some applications, such as Skype or RDP, could not be allowed by Application Control.<br>28. The background colors of the row on the connection page in the Web UI were not alternating after a filter had been applied.<br>29. Traffic using routing rules with routing tables where the "Ordering" setting was set to "Default" was sometimes routed incorrectly.<br>30. Accessing certain HTTPS sites sometimes failed if the HTTP ALG was configured to do Web Content Filtering.<br>31. The classified value in the Application Control statistics table suffered from duplicate and premature updates. This has been fixed, so, it is normal to expect a lower rate of updates after a firmware upgrade.<br>32. Safe Search configured together with Web Content Filtering sometimes caused system reboot.<br>33. Removing a large number of IPsec tunnels from the configuration could cause the system to restart.<br>34. Application Control Rules would, with certain selected applications, take longer time than necessary to parse during reconfiguration. |
| 2.27.08 | 1. Using SCP to download a file from the firewall whose filename included a |

| | |
|---|---|
| | hyphen would fail with a "Permission denied" error message.<br>2. In some situations the system would send an extra TCP ACK packet when it did not need to.<br>3. When using a service group which contained overlapping services, there was no warning message that this may cause undefined behavior.<br>4. When "arp -notify" was used in an HA setup, the firewall incorrectly used its private MAC address instead of the shared MAC address.<br>5. Changes made to the HTTP normalization parameters on an IDP rule were ignored unless other settings were changed on the same IDP rule.<br>6. A static DHCP lease was not treated as static anymore if the IP had been blacklisted and then being released from the blacklist. The static leases are now always kept static and related temporarily assigned leases during blacklist are cleaned from the lease pool.<br>7. The Log and Event receivers did not support using another routing table than "main".<br>8. Hardware statistics for some Realtek interfaces was incorrectly represented in the CLI and could not be reset.<br>9. The HostMonitor subsystem could cause an unexpected restart during reconfiguration when used together with Server Load Balancing.<br>10. When using a NAT Pool with a large amount of addresses, the performance was affected in a negative way.<br>11. The CLI tab completion when adding a Custom Option for a DHCP Server was confusing and has been improved.<br>12. On rare occasions the system could make an unexpected restart when using the HTTP ALG together with Anti-Virus scanning.<br>13. In rare cases when a heavy load of IPsec traffic was sent through the firewall there could be logs about hardware acceleration failure with performance degradation as a result. Affects: DFL-210/DFL-260/DFL-260E/DFL-800/DFL-860/DFL-860E.<br>14. The internal SSH Server could in rare circumstances use an increasing amount of memory.<br>15. The firewall would always perform automatic updates of IDP and AV databases on startup and HA activation. Automatic updates will now only occur at the configured time.<br>16. Configuration pages with a very large amount of objects could have the last object hidden by Internet Explorer.<br>17. Certain configurations related to one sub system could cause a security vulnerability.<br>18. POP3 ALG log messages would sometimes contain incorrect e-mail |

| | |
|---|---|
| | addresses.<br>19. On rare occasions, the SMTP and POP3 ALGs could not read fields from theDataHeader correctly.<br>20. The DHCP Client did not renew its IP address lease after a link failure had been restored.<br>21. TCP traffic inside an IPsec tunnel using Transport Mode where both peers were located behind a NAT gateway did not work as expected, SYN-ACKs never reached client, when the firewall was configured with SynRelay.<br>22. The community string in SNMP Remote Management was truncated if it was longer than 32 characters.<br>23. Unsolicited ARP reply was not handled correctly according to the UnsolicitedARPReplies setting. The setting for Multiple Username Logins on the User Authentication Rule did not work as intended when selecting to use timeouts from the authentication server.<br>24. Certain SIP PBX configurations caused the firewall to drop INVITE requests.<br>25. It was possible to configure multiple static DHCP hosts with the same IP or MAC address without getting a configuration warning.<br>26. The system would set the BROADCAST flag in DHCP Discover and DHCP Request messages, despite being fully capable of receiving unicast replies.<br>27. The updatecenter CLI command would return an error if no argument was specified. It will now show the status of all databases as default action.<br>28. The L2TP/PPTP client used the wrong source IP when the interface used for L2TP/PPTP traffic was changed due to a DHCP update.<br>29. NATed traffic sometimes used an old source IP address for connections opened prior to a dynamic update of the IP address of the outgoing interface.<br>30. The switch driver used on DFL-260E (rev a2) appliances had a faulty default configuration, which lead to performance issues. |
| 2.27.07-RU | 1. In some rare occasions, the memory consumption of the firewall could increase unexpectedly when deploying cluster configurations.<br>2. The output list from the CLI command 'vlan' was not sorted in VLAN ID order. This has been corrected and the command was enhanced with the parameters to segment long output lists ‘num’ and ‘page’.<br>3. The 'blacklist' CLI command did not set the correct port number and destination URL in its output.<br>4. A configuration with the now obsolete selection of Log And Event Receiver category '36 (USAGE)' would send out empty log data. The configuration is now silently updated to exclude this category. |

5. The shared IP was not used in LDAP server queries for High Availability cluster nodes.
6. The realm string for HTTP basic authentication was incorrectly not optional in the configuration.
7. The unit for the OSPF memory max usage in the WebUI was 'kilobytes', but has now been corrected to 'bytes'.
8. The Local Gateway configured in an IPsec tunnel was not shown in the CLI command "ipsectunnels -iface" printout.
9. The link status of the DMZ, WAN1 and WAN2 interfaces on the DFL-860E model and DMZ and WAN on the DFL-260E would disappear shortly during the reconfigure process.
10. The filename for an attachment was incorrectly required for the SMTP ALG and POP3ALG. The ALGs have now been updated to handle attachments without filenames, according to the RFCs.
11. The SIP ALG did not use the "420 Bad Extension" response in certain circumstances.
12. The built in L2TP client did not work correctly when put behind a NAT device.
13. The configuration was not always updated correctly when upgrading to a newer version.
14. HTTPS webauth using Internet Explorer versions 8 and older did not show the logged in page after the user had logged in.
15. When using a large number of neighbors in nodes running OSPF, there was a rare possibility of memory corruption.
16. A prompt was not added after various SSH printouts in the CLI.
17. Routemon did not detect link state changes on some Realtek interfaces. Affected models: DFL-260E/DFL-860Es.
18. The link status info for the Realtek interfaces disappeared after a reconfigure. Affected models: DFL-260E/DFL-860E
19. In some scenarios with IDP configured, traffic of certain patterns could in rare circumstances be delayed
20. It was not possible to connect multiple L2TP/IPsec clients behind the same NAT gateway.
21. SNMP Interface Alias field was empty when selecting "Comment" in "Interface Alias".
22. If L2TP clients with the same local IP address established IPsec tunnels behind a NAT device there were sometimes problems with the connections.
23. The OSPF routes database was not updated during reconfigure in some High Availability scenarios.

| | |
|---|---|
| | 24. In some unusual circumstances the use of XAuth based authentication would lead to an unexpected reboot<br>25. The web user interface was not 100% compatible with Explorer 10. The basic structure has now been updated to render the page correctly in all major browsers.<br>26. The firewall Dynamic Routing Rules did not properly export / import OSPF routes when they were filtered by "OSPF Tag range" or "Router Type".<br>27. A few log message categories, such as SSL VPN and IPv6 Neighbor Discovery were missing from the log message exception list..<br>28. In some scenarios when using IPsec with XAuth, ESP delete notifications would not be sent. |
| 2.27.06-RU | 1. Corrected leap year problem where leap year day was added to January instead of February.<br>2. The log event no_arp (ID:04100007) firewall action text was previously route_enabled, the text is now corrected to route_disabled.<br>3. Time unit 'seconds' added to help texts in WebUI ALG SIP dialog and CLI command 'help ALG_SIP'.<br>4. The memory consumption of the firewall could in some rare occasions increase unexpectedly when deploying cluster configurations.<br>5. The output list from the CLI command 'vlan' was not sorted in VLAN ID order. This has been corrected and the command was enhanced with the parameters to segment long output lists using 'num' and 'page'.<br>6. The 'blacklist' CLI command did not set the correct port number and destination URL in its output.<br>7. The output text for the CLI command 'dns -list' was not formatted correctly when using SSH remote management.<br>8. In rare occasions, closing down a SIP session could lead to an unexpected restart.<br>9. Using the H323 ALG could in rare circumstances lead to malfunction.<br>10. The corruption of a linked list could lead to a crash. This is corrected now.<br>11. The output of the CLI command "ifstat" has been extended to list the shared MAC addresses on the interfaces of High Availability cluster nodes.<br>12. During tunnel set up, the L2TP client would abort and restart tunnel negotiation if the server response deviated from commonly agreed communication protocols.<br>13. In a rare High Availability situation where a large amount of IPsec traffic (with a very large number of tunnels) was making the firewall loaded, it was possible that both nodes were set as the active node. |

| | |
|---|---|
| | 14. A prompt was not printed in the CLI after activating a new configuration.<br>15. In scenarios where all routes announced in an OSPF area are added to a routing table, pre-existing static routes could be overwritten. Now static routes received from the OSPF process will not replace pre-existing static routes in a routing table.<br>16. The filename for an attachment was incorrectly required for the SMTP ALG and POP3 ALG. The ALGs have now been updated to handle attachments without filenames, according to the RFCs.<br>17. Static destination address translation would fail for transport mode IPsec traffic.<br>18. When using a large number of neighbors in nodes running OSPF, there was a rare possibility of memory corruption. |
| 2.27.05-RU | 19. An expired AV or IDP license in an HA environment could trigger unexpected behavior in the inactive cluster node.<br>20. Some web authentication scenarios could lead to unexpected behavior by the firewall.<br>21. Some VPN configurations using Radius Accounting did not report in/out octet statistics to the Radius Accounting server.<br>22. The H.323 ALG did not allow FACILITY messages to be sent during the ALERTING state.<br>23. In some cases, the ping -verbose CLI command did not print the correct translated port if the packet was affected by a SAT rule. The correct translated port will now be printed.<br>24. In certain scenarios, traffic originating from LDAP could lead to unexpected behavior by the firewall.<br>25. CorePlus did not handle lower and upper case correctly in some configuration scenarios where objects were named almost identically.<br>26. In some High Availability scenarios, the HA setting ReconfFailoverTime was not obeyed, resulting in a failover when deploying a configuration on the active peer before the ReconfFailoverTime was reached.<br>27. Setting up a High Availability cluster using the "backup and restore" method would result in problems synchronizing the configuration because of an invalid interface configuration. The units now correctly handle that interface configuration by using information from the old configuration.<br>28. A recent change in scp (secure copy) use an end of option parameter that was handled erroneously by the firewall. Now this option is handled correctly and scp connections will no longer be closed unexpectedly.<br>29. The Web Content Filtering (WCF) server connection could stall after a |

| | |
|---|---|
| | reconfigure and fail to resolve new URLs. The issue has been corrected together with additional server connection statistics for the 'httpalg -wcfcache' CLI command.<br>30. Some network scenarios caused the SIP ALG to close SIP calls two minutes after the call was established.<br>31. Using a PPTP server together with pipes could occasionally prevent the PPTP server from accepting new connections.<br>32. Passive OSPF-interfaces were allowed to send out "OSPF-hello" messages. Passive OSPF-interfaces are now prohibited from taking part in the OSPF discovery process.<br>33. OSPF did not detect the link status of physical interfaces. Link status is now periodically monitored within OSPF.<br>34. The HWM functionality was malfunctioning for the DFL-1600 and has been corrected in this release.<br>35. The "Route Type" in "OSPF Actions" was incorrectly interpreted by the firewall when the configuration was activated.<br>36. The source port 20 is now used when combining the SAT Action in an IPRule with the FTP ALG.<br>37. An unexpected restart could occur during a configuration deployment when new IPsec tunnels were added to the configuration. Changes have been made to prevent a resource conflict, causing the unexpected restart.<br>38. It was not possible to use all address object combinations in places like routes or in the Address Book. The WebUI validation code has been extended to handle arrays of IP4 Addresses in order to correct the problem.<br>39. TLS ALG rejected SSL HELLOs with zero or more than 1 compression method.<br>40. Invalid values entered in properties in the WebUI would silently be rejected. An error is now properly reported when a property has an error.<br>41. Some cipher suite combinations prevented the AES256 algorithm to be used when establishing SSH administration sessions to the firewall.<br>42. Some specially crafted SDP payloads could cause unexpected reboots of the firewall.<br>43. The WebUI page for interface status showed the Send Rate and Receive Rate as average for the last 24h. The values have been updated to use the average for the last 2 minutes. |
| 2.27.04-RU | 1. The usage column in the DHCP Server status page has been updated to show active clients.<br>2. References to UserAuth privileges for authenticated users could change when |

| | |
|---|---|
| | modifying the number of configured privileges.<br>3. The web server could under certain conditions deadlock and print a "500 - Internal Server Error" message when trying to access the web user interface. The web server has been extended with better error handling to prevent this kind of deadlock.<br>4. The interface traffic counters were only of size 32-bit and often wrapped around when the throughput was high. Corresponding 64-bit counters have been added to ensure that wrapping will not occur as often as the corresponding 32-bit values.<br>5. The block list file verification failed for files with a size smaller than one packet. The blocklist now validates the extension for the first packet when the content type could not be determined in the first packet.<br>6. In certain scenarios, the voice transmitted through the SIP ALG terminated suddenly two minutes after the call was established.<br>7. Office "xlsm" files were blocked by the SMTP ALG. Encrypted "xlsm" files are embedded in an "Office 97/2000 Compatible" container which results in an incorrect file typ according to file integrity control. The file integrity control has been updated to handle encrypted "xlsm" files.<br>8. A faulty model check made the Switch Management not display all the switch ports in the WebUI for the DFL-860E model.<br>9. The Realtek 8169 interface reported link down incorrectly. This caused route monitor to not work properly. Affects: DFL-260E and DFL-860E.<br>10. The HTTP ALG failed to load web pages from certain web servers correctly. The HTTP ALG will now respond with a TCP RESET should the server continue to send packets after the client has closed the connection.<br>11. Anti-virus scanning of zip files containing files with a large compressed size could sometimes lead to unexpected behavior.<br>12. Using HTTP web authentication with a RADIUS server as authentication source, could in very rare scenarios cause the firewall to malfunction during save & activate (reconfigure).<br>13. Two HTTP ALGs with the same name, but with different case (e.g. "MYHTTPALG" and "myhttpalg"), could sometimes cause the firewall to freeze during save & activate (reconfigure). |
| 2.27.02-RU | 1. It was not possible to use User Authentication on IP4Group objects.<br>2. Certain SIP server scenarios in REGISTER transactions made the firewall reject incoming SIP calls.<br>3. In some situations when using SMTP ALG with Anti-Virus e-mails with attachments would not be completely transferred, resulting in a timeout. The |

| | |
|---|---|
| | ALG Anti-Virus feature now specifically logs failure to decompress encrypted zip files. A setting to allow or deny encrypted zip files have also been added.<br>4. The usage bars on the DHCP Server status page were not displayed correctly when leases reached 100% usage.<br>5. ACK messages for non 2xx PBXs responses were not forwarded by the SIP ALG.<br>6. The DHCP Server did not send DHCP NAK messages in all scenarios. This change speeds up the process of receiving a new IP address lease in these scenarios.<br>7. The SMTP ALG always allowed emails where the SMTP "from" address and email header "from" address did not match. A new setting has been added which allows the administrator to deny or tag these mails as spam.<br>8. CLI command "ipsecdefines" has been removed from "techsupport" command.<br>9. During configuration certain values were not reset after parsing an IGMP Report rule, which made the next IGMP Query misbehave. The configuration values are now properly reset after parsing IGMP Report rules.<br>10. Incoming SIP traffic routed through an IPsec tunnel was discarded by the SIP ALG.<br>11. Some empty configuration values were not written to the configuration. After a restart of the firewall the default values were used instead.<br>12. Some buttons in the web user interface had truncated text.<br>13. The reception of 255.255.255.254 as Framed-IP-Address in a RADIUS negotiation wasn't handled correctly in all installations. Now this will always lead to an IP being assigned, to the PPTP-/L2TP-client, from the configured IP pool.<br>14. It was not possible to click on the IDP signature group links in the web user interface page "IDP Factory Signatures". Clicking on the link now lists the signatures in the group.<br>15. The DNS client always dropped DNS replies that had the truncated bit set. The truncated bit indicates that the reply does not contain the complete response and that a new DNS request should be sent using TCP (if the client supports TCP DNS). The DNS client now uses the addresses in the partial response instead of ending up with no address at all.<br>16. Certain SIP PBX configurations blocked media transmission on calls established between devices located on the same interface of the firewall.<br>17. The POP3 ALG did not reset its state after a failed authentication. This could cause the next login attempt to fail.<br>18. Specific Intrusion Detection Protection (IDP) scenarios using hardware |

| | |
|---|---|
| | acceleration could cause scans to fail.<br>19. Restarting a GRE interface did sometimes trigger an unexpected restart of the firewall.<br>20. The POP3 ALG did not allow Digest-MD5 authentication.<br>21. The SIP ALG could forward malformed SIP messages if a range 0-65535 was used as destination port in the SIP service configuration.<br>22. Specific scenarios using the PPTP ALG could sometimes cause an unexpected restart of the firewall.<br>23. The log message sent when reclassifying a URL using Web Content Filtering showed the wrong category. The log message has been updated to display the correct category.<br>24. Web User Interface: Activating a configuration that had deleted an item that was represented in the navigation tree would not automatically update the navigation tree. This resulted in a navigation tree that did not correspond to the running configuration.<br>25. Checked checkbox properties that were disabled were unchecked when submitting data in the Web User Interface (since information sent by a web browser is identical for an unchecked checkbox and a disabled checkbox). The configuration engine now correctly remembers the state of disabled checkboxes when submitting data.<br>26. The HTTP ALG MIME type check did not have support for OpenDocument Text<br>Documents (odt).<br>27. Script execute did not allow the 'cc' command to run without parameters. The command has been updated. |
| 2.27.00-RU | 1. The IP4 Group object didn't handle excluded addresses correctly. It's now possible to use excluded and included objects in the correct way.<br>2. Certain SIP option messages with high values for the "expires" header field failed to be properly parsed. When that occurred incoming calls to phones placed behind the firewall failed.<br>3. Some HTTP headers could cause HTTP connections through the HTTP ALG to be closed down prematurely.<br>4. On DFL-260/ DFL-860, some specific high stressed Intrusion Detection and Protection scenarios using a hardware accelerator could drain the memory of the firewall.<br>5. The SMTP ALG did not accept response codes that only contained numeric data.<br>6. Browsing the Web User Interface over HTTPS would sometimes result in |

| | |
|---|---|
| | "Error 500 - Internal server error".<br>7. On DFL-1600/DFL-1660/DFL-2500/DFL-2560(G), after a reconfiguration using a HA configuration the interface synchronization list for the Inactive node contained invalid interface references which could cause problems when connections were synchronized before the list was rebuilt. The references are now properly cleared during a reconfiguration.<br>8. In the Web User Interface, when defining an IDP Rule, the check box to enable or disable the option "Protect against insertion/evasion attacks" was not visible.<br>9. The CLI techsupport command always sent a "sesmgr_file_error" log message, even when it worked correctly. The techsupport command now only sends log message when it fails.<br>10. A limitation on the number of simultaneous WebAuth transaction could prevent the authentication of authorized users.<br>11. The IP Rule view in the Web User Interface was slow when viewing large collection of rules. The rendering speed has been improved.<br>12. Dropdown menus in the Web User Interface used a fixed width, which caused objects with long names to push information outsize the window. The dropdowns are now scaled to be able to show all the information. The dropdown also automatically scrolls to the selected item when opened.<br>13. The Mappings and Leases links on the DHCP Server status page in the Web User Interface didn't work.<br>14. Disabling objects with references in the Web User Interface would delete the objects and references instead. The objects are now only disabled when selecting to disable them. |

## Known Issues:

| Firmware Version | Known Issues |
|---|---|
| 2.27.05-RU | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>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.<br>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.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>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.<br>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.<br>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. |
| 2.27.04-RU | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>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.<br>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.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>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.<br>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.<br>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.<br>10. The function "StateKeepAlive" of NAT Pool is not working.<br>11. SIP ALG: Limited functionality on SIP ALG. It supports three scenarios: (a) Protecting local clients - Proxy located on the Internet; (b) Protecting proxy and local clients - Proxy on the same network as clients; (c) Protecting proxy and local clients - Proxy on a DMZ interface. A more detailed description and network topologies can be found in the Admin Guide. Any scenario different from these three might be difficult to deploy.<br>12. SIP ALG: Limited functionality on IP telephony. It is not support all functionality in RFC-3261 or other RFC's that is referred to from RC-3261. There may be third party SIP-aware units that cannot be configured to be compatible with the SIP-ALG. |
| 2.27.02-RU | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>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.<br>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.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>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.<br>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.<br>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.<br>10. The function "StateKeepAlive" of NAT Pool is not working. |
| 2.27.00-RU | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>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.<br>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.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>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.<br>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.<br>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.<br>10. The function "StateKeepAlive" of NAT Pool is not working. |

## Related Documentation:

- NetDefend Firewall User Manual v2.27.05
- NetDefend Firewall CLI Reference Guide v2.27.05
- NetDefend Firewall Logging Reference Guide v2.27.05