D-Link®

NetDefendOS Version: 12.00.16

Published Date: 2019-04-23

Copyright © 2019

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:

dlink green

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
12.00.13	Apr. 23, 2019	DFL-1660/2560/2560G DFL-870	DFL-2560G A2 DFL-870/1660/2560 A1
12.00.13	Nov. 16, 2018	DFL-1660/2560/2560G DFL-260E/860E DFL-870	DFL-260E A2 A1 (for all models)
11.20.05	Apr. 10, 2018	DFL-1660/2560/2560G DFL-260E/860E DFL-870	DFL-260E A2 A1 (for all models)
11.10.01	Feb 20, 2017	DFL-1660/2560/2560G DFL-260E/860E DFL-870	DFL-260E A2 A1 (for all models)
11.04.01	Oct 13, 2016	DFL-1660/2560/2560G DFL-260E/860E DFL-870	DFL-260E A2 A1 (for all models)
10.22.01	Aug 03, 2015	DFL-1660/2560/2560G DFL-260E/860E	DFL-260E A2 A1 (for all models)
10.21.02	Dec 23, 2014	DFL-1660/2560/2560G DFL-260E/860E	DFL-260E A2 A1 (for all models)
2.60.02	Jul 07, 2014	DFL-1660/2560/2560G DFL-260E/860E	DFL-260E A2 A1 (for all models)
2.40.04	Jul 17, 2013	DFL-1660/2560/2560G DFL-260E/860E	DFL-260E A2 A1 (for all models)
2.40.03	Apr 05, 2013	DFL-1660/2560/2560G DFL-260E/860E	DFL-260E A2 A1 (for all models)
2.40.02	Dec 15, 2012	DFL-1660/2560/2560G DFL-260E/860E	DFL-260E A2 A1 (for all models)
2.40.01	Apr 15, 2012	DFL-1660/2560/2560G DFL-260E/860E	A1 (for all models)
2.40.00	Oct 21, 2011	DFL-1660/2560/2560G DFL-260E/860E	A1 (for all models)
2.30.01	June 1 2011	DFL-1660/2560/2560G DFL-260E/860E	A1 (for all models)
2.27.03	Nov 24 2010	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	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)
2.27.01	July 5 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	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)
2.26.02	Mar 4 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)

2.26.01	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 2.1.7, "Secure Copy" of NetDefend Firewall v12.00.13 user Manual*.

Upgrading by using Web-UI

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the *NetDefend Firewall v12.00.13 User Manual.*

New Features:

Firmware Version	New Features
12.00.16	1. **Enhanced SSH server security** New and more secure SSH algorithms have been added. In addition, new sections have been added with a set of recommended algorithms (which are now set as default, also for upgraded configurations) and a section of legacy algorithms that are no longer considered secure but are still available for backwards compatibility. Note that old SSH clients may not be able to connect after the upgrade since they may not support modern algorithms. 2. **SSH host key generation** Support for generating new SSH host keys from the WebUI and the CLI has

been added.

3. Updated cipher recommendations

The 3DES crypto algorithm has been moved to the "Deprecated cipher suites" sections under SSL Settings. In new configurations the algorithm is not enabled by default. Consider disabling the use of 3DES to increase security.

4. Added possibility to sort the output from the "memory" CLI command

The "memory" CLI command now can sort the output by total size, description and number of allocations.

5. New Application Control Library

The Application Library has been updated to version 1.400.

6. The "Neighbor Devices" WebUI data grid has been updated

An updated data grid has been added to the "Neighbor Devices" page that allows filtering.

7. Updated GeoIP Database

The GeoIP database has been updated to the 2019-01-22 release

8. Updated threat prevention behavior

The IP Reputation score needed for an IP address to be blacklisted has been increased from 10 to 20. The time an IP is blacklisted has also been increased from 1 minute to 5 minutes

9. IDP enhancement

The memory usage for the IDP engine has been optimized.

10. Application end log event now contains additional information

The 'Application End' log event now contains the family and risk for the specified application.

11. Added possibility to retrieve neighbor device information using REST

The REST API has been updated with the ability to get the neighbor devices information.

12.00.13	**1. New Web User Interface Style** New Web User Interface style is implemented for new outlook and feeling. The system overview gives more informative statistics of the traffic processed and analyzed by the firewall. New real-time graphs of blocked threats and malware have been added in addition to information of HA status, authenticated users and neighbor devices. **2. Threat Prevention** New Threat Prevention section has been developed to group together threat

prevention mechanisms within the web user interface. The Threat Prevention section includes both existing features as well as new features like Botnet, Scanner and DOS Protection. Existing features that have been moved into the Threat Prevention concept are Access Rules, IDP Rules, Threshold Rules and ZoneDefense configuration. In addition, the global IP Whitelist has also been positioned within Threat Prevention to exclude traffic from the mentioned threat prevention mechanisms.

3. **IP Reputation (Subscription Feature)**

Disabling inbound communications from the IPs with high risk is highly effective way to keep networks secure. Cooperating with Botnet Protection, DoS Protection and Scanner Protection on DFL series, IP Reputation Service offers an up-to-date database to allow the administrators to block and blacklisted the IP address known to be malicious. (*Only supported on DFL-870/1660/2560(G)*)

4. **Denial of Service Protection**

The system now supports Denial of Service Protection utilizing IP Reputation technology provided by Webroot. DOS Protection will analyze the source IP address of a packet before allowing new connections to be opened. If the IP address is found to be a known DOS source, the IP address is automatically blacklisted for one minute. DOS Protection is a part of the new Threat Prevention concept.

5. **GeoIP DOS Protection**

It is now possible to configure and block traffic from unwanted regions using GeoIP DOS Protection. The GeoIP DOS protection feature blocks traffic in the firewall at an early stage of the packet flow utilizing less processing power than normal IP rules/policies. It is suitable in scenarios where traffic from certain regions is not expected and can be used to minimize the DOS and malware attack surface from foreign regions.

6. **Scanner Protection**

The system now supports Scanner Protection utilizing IP Reputation technology provided by Webroot. Scanner Protection will analyze the source IP address of a packet before allowing new connections to be opened. If the IP address is found to be a known source performing reconnaissance such as probes, host scan or password brute force, the IP address is automatically blacklisted for one minute. Scanner Protection is a part of the new Threat Prevention concept.

7. **Botnet Protection**

The system now supports Botnet Protection utilizing IP Reputation technology provided by Webroot. Botnet Protection will analyze the source

and destination IP addresses of a packet before allowing new connections to be opened. If any IP address is found to be part of a botnet, the botnet IP address will be blacklisted for one minute, preventing any traffic to and from the blacklisted address.

8.   HTTP/HTTPS & SSH Remote Management over IPv6

It is now possible to configure an HTTP/HTTPS Management access filter with IPv6 networks or addresses, allowing IPv6 management access to the web user interface and SSH interface.

9.   Re-designed and Improved IPsec Status Page

The IPsec status page has been redesigned to give a better overview of configured and established tunnels.

10. UDP and TCP Traceroute Support

The 'traceroute' CLI command has been extended with UDP and TCP protocol support for both IPv4 and IPv6.

11. Persistent WebUI HTTP Connections

The internal web server now supports persistent HTTP connections which reduces the number of connections required for HTTP/HTTPS management.

12. Download anonymized configuration file

A possibility to download an anonymized configuration file where sensitive data (such as PSK, user passwords, certificates) is replaced with standard template values has been added.

13. Improved DHCP Server Logging

Log messages produced by the firewall when a DHCP lease is given out now includes the host name of the receiving client, if available.

14. Clear screen CLI Command

A new 'clear' CLI command that clears the screen has been added.

15. Change Blacklist "Time In List" column to "Time to live"

The name of hte blacklist column "Time In List" has been updated to "Time to live" in both the CLI and WebUI

16. SNMPv3 Traps

The system now supports SNMPv3 Traps allowing authentication and encrypted communication for traps. Note that the SNMPv3 engine ID might change when upgrading to this version.

17. Redirect Support for Web Profiles

The existing whitelist and blacklist feature in web profiles has been extended with redirect support. It is now possible to configure a URL filter and redirect all matching traffic to another web page.

18. User defined Brute Force Protection settings

Users can now define how many failed login attempts will be allowed on an admin/auditors account, as well as the number of seconds that account will be locked out.

19. Web Content Filter Reclassify Support

The reclassify-setting used for Web Content Filtering has changed from providing a local submit form to provide a link to an external reclassification page. This change allows web profile configurations to use the faster LW-HTTP ALG even in scenarios where reclassification is allowed. The default 'ReclassifyURL' and 'RestristedSiteNotice' banner files have been updated and any custom banner files are compatible so that they now show the new reclassify link.

20. The option to disable AV/IDP signature update after reconfigure or HA activation

Previously a check for updated AV/IDP signature files (and possibly a download if they were outdated) were always performed after a reconfigure or an HA failover. This can now be configured not to take place and the check for updated signature files will only take place according to the configured schema.

21. Pre-allocation of HTTP sessions

To improve performance directly after booting up, up to 50,000 HTTP sessions can be pre-allocated by the system. The number of allocated sessions is dependent on the number of sessions configured on service objects with the protocol set to HTTP.

22. Enhanced support for character encoding in email attachments

The mail header parsing has been enhanced with support for the mime parameter "filename" encoded in UTF-8 according to RFC2184.

23. Improved HTTPS Performance

HTTPS support has been added to the LW-HTTP engine. The LW-HTTP engine provides an HTTPS throughput performance boost of roughly 400%. The LW-HTTP engine supports Web Content Filtering and URL Blacklisting for HTTPS connections and is automatically enabled when used in an IP Policy with connected Web Profile. Existing IP Policy HTTPS configurations are automatically upgraded and will be using the new LW-HTTP engine when used with a Web Profile.

24. Added MAC Vendor information to Neighbor Devices list

The Neighbor Devices information has been extended to show MAC Ethernet Vendor information in both the WebUI and the CLI.

25. Server Load Balancing functionality enhanced for unreachable servers

The Server Load Balancing service will now respond with a reset (TCP RST / ICMP Port Unreachable) if it receives data from a client and monitor instance has detected the destination server down.

26. Default setting for minimum TLS version updated to TLS v1.2

The new default setting for the minimum TLS version for SSL connections is now TLS v1.2, upgraded configurations will not be affected. It is highly

recommended to change minimum TLS version to v1.2 for existing configurations.

27. HTTP Protocol Upgrade Control

A new setting has been added to the Web Profile to control whether HTTP Protocol Upgrade shall be allowed or not. The default behavior is to allow Protocol Upgrade which is commonly used for e.g. Web Sockets.

28. New Neighbor Devices status page

A status page of neighbor devices has been added to the web user interface. The status page indicates the presence and status of neighboring devices that are communicating through the device.

29. DHCP status enhancement

The DHCP status page for leases/mappings now shows the hostname and/or configured name for the leased addresses when applicable.

30. IPv6 support for SSH Remote Management

It is now possible to configure an HTTP/HTTPS Management access filter with IPv6 networks or addresses, allowing IPv6 management access to the SSH interface.

31. Server Offline Notification for Server Load Balancing

The Server Load Balancing feature has been extended with capabilities to send TCP Reset packets on established connections to a server that goes offline. Two modes of operation are available. The system can either passively send a TCP Reset packet when the system receives a packet from a client on a connection where the server has been flagged as offline. The second alternative is to actively send a TCP Reset as soon as a server is detected to be offline, without waiting for the client to first send a packet. The second alternative requires additional state tracking within the system and thus more RAM resources.

32. Increased Browser Cache Time for WebUI Objects

The HTTP header that tells the web browser how long a static object (like javascript files and images) can be cached has been updated. The web user interface now allows static object to be cached for 30 days, instead of 4 hours. The implemented fix will improve loading times.

33. Packet capture support for multiple ports

The Packet Capture (pcapdump) function in the WebUI and CLI now supports using filters with multiple ports and ranges such as "67,68, 8080-8088".

34. IPv6 and FQDN netobject support for time server

The time servers can now be configured with FQDN objects and/or IPv6 addresses. Existing time server configurations are automatically upgraded to use FQDN objects.

35. General FQDN Policy Support

It is now possible to configure and use FQDN address objects in Intrusion

Detection, Threshold rules, IP policies, Traffic shaping and Policy Based Routing rules.

36. DNS Monitoring and Control

The system has been enhanced with DNS monitoring support. By configuring an IP policy with a DNS profile, it is now possible to both monitor and control what type of DNS traffic that is allowed in the network. The DNS profile also plays a central role for FQDN Address objects configured with wildcard FQDN names. The DNS inspector uses the client's DNS queries to populate the system's DNS cache which in turn is used by various FQDN supporting rule types.

37. Wildcard Support for FQDN Policies

The FQDN address support for several system features has been improved with wildcard support. It is now possible to configure Intrusion Detection, Threshold rules, IP policies, Traffic shaping and Policy Based Routing using FQDN address objects configured as domain filters. This will only work when combined with the new DNS-ALG to make the system learn the IP addresses for configured FQDN filters by monitoring clients' DNS traffic.

38. New setting for "Non-Managed" categories for Email Control

The Email Control Profile has been enhanced so the user can specify whether non-managed categories should be denied or allowed.

39. Enhanced WebUI ping tool

FQDN/DNS names can be used when using the WebUI Ping tool.

40. New IPsec profile for Microsoft Azure

A new predefined IPsec profile has been added to simplify connecting to a Microsoft Azure VPN.

41. Assign config mode clients static IPs

VPN users connecting with IKE and config mode can now be assigned static IPs when a local user database is used for authentication. The IPsec Tunnel property "ConfigMode" value "RADIUS" has been renamed to "UserAuth" in the CLI to better reflect that it's up to the user authentication rule how the IP will be assigned: Either from a RADIUS server or from a local user database.

42. Proxy ARP support for IPsec tunnels

It's now possible to configure an IPsec tunnel to proxy ARP IPs that have been added dynamically from connecting clients.

43. Advanced Schedule Improvements

Advanced Schedule Occurrences can now be configured to be active for up to 24 hours after their start time. This makes it possible to chain multiple days together without interruptions.

44. More secure self-signed certificates

The default SSL certificate on the firewall is now generated using SHA-256 as the signature hash algorithm. This is also the hash algorithm used when

generating new self-signed certificates through the web user interface. The system can no longer generate certificates with weak keys (512 and 1024 bits). The HTTPS admin certificate is not automatically replaced during an upgrade. It is highly recommended to generate a new certificate if the configuration uses a weak HTTPS certificate (signed with SHA-1 and/or fewer than 2048 bits).

45. Update to stat CLI command

The 'Last Shutdown' row of the stats CLI command was renamed to 'Last Event' to make it clearer since the log can contain entries not related to an actual system shutdown/restart (such as a reconfigure)

46. Shared address sender for High Availability timesync

Timesync messages (NTP requests) were always sent using the local address as sender. The active HA node will now use the shared address for NTP requests.

47. Antivirus Advisory Link for Virus Found HTTP Page

A clickable advisory link has been added to the 'virus found' web page displayed when a virus has been detected in an HTTP stream.

48. Updated Configuration and System Backup default Filenames

When creating a configuration or system backup, the configured device name will be part of the file name of the downloaded file.

49. Improved HTTP Antivirus Performance

The antivirus scanning performance has been significantly improved by adding virus scanning support to the light-weight HTTP scan engine. In addition, the memory usage for each ALG session has been decreased which allows more concurrent HTTP sessions while using less memory. The new scan engine will be automatically selected when using IP Policies configured with antivirus and a service configured with HTTP as protocol.

50. Simplified IPsec Configuration

Simplified IPsec profiles provide quick and easy configuration of new VPN Client and VPN LAN to LAN Tunnels. By using the VPN Client profile, a roaming tunnel for IKEv2 clients can easily be configured in just a few steps supporting iOS, Mac OS and Windows users. The LAN to LAN tunnel allows simplified setup of a tunnel between two firewalls with algorithms that are known to be secure.

51. IPv6 User Authentication for IPsec Tunnels

The user authentication subsystem has been upgraded with IPv6 support. This allows IPsec tunnels to authenticate users connecting with IPv6. In addition, authentication using RADIUS now supports RADIUS servers configured with an IPv6 address.

52. Local User Database Authentication of Roaming IKEv2 Clients

In addition to RADIUS authentication, IKEv2 roaming clients can now be authenticated using the local user database with a pre-shared key. Supported authentication mechanisms are EAP-MSCHAPv2 and EAP-MD5.

53. IPsec EAP-MD5 and EAP-MSCHAPv2 Client Authentication

The IPsec tunnel has been extended with EAP-MD5 and EAP-MSCHAPv2 support when authenticating itself towards a remote IKEv2 VPN gateway.

54. IPsec Config Mode Client

When the firewall is acting as an IPsec client, the IP address and network can now be assigned from its peer using Config Mode.

55. MOBIKE Support (IKEv2 Mobility and Multihoming Protocol: RFC 4555)

The IPsec suite has been extended with MOBIKE support. MOBIKE allows the VPN connection to remain open even if a client changes its local IP address or if a NAT device along the path changes the client's originating IP address.

56. New CLI Command for SLB (Server Load Balancing)

A new 'slb' CLI command has been added. The CLI command provides status of the configured SLB servers and can also be used for suspending and resuming distribution of new connections to a specific server.

57. Server Load Distribution Method added to Server Load Balancing (SLB)

A new distribution method has been added to SLB. The distribution method allows servers to post the current load of e.g. CPU, memory or disk usage, to the firewall using a REST API. This opens up for improved load balancing between servers of uneven hardware configurations.

58. Advisory Links for Antivirus

The system log in the web user interface has been extended to include a clickable advisory link in virus found log messages. When clicked, the link leads to a web page giving more information about the identified virus.

59. RADIUS Assigned IP Addresses for IPsec Roaming Clients

When configuring an IPsec tunnel for roaming clients using config mode, the connecting client's IP address may now be assigned by the same RADIUS server as used for authenticating the user. The RADIUS server provides the IP address using the Framed IP attribute. RADIUS assigned IP address is supported for both IKEv1 and IKEv2.

60. High Availability Status available using SNMP

The current High Availability status can now be queried using SNMP. The SNMP values added are HA Role (master or slave), HA State (active or inactive) and the number of seconds since last role change.

61. Maintenance Mode for SLB Servers

Server Load Balancing Server can now be put into maintenance mode either using the newly introduced 'slb' CLI command or using the SLB Status page

	in the WebUI. A server in suspended mode, will have no new connections distributed to it. **62. Improved 'connection' CLI command** The 'connection' CLI command has been improved with an '-extended' flag to show the number of bytes transferred and the application name in for connections. When combined with the '-verbose' flag, the data transferred is shown for each direction instead of the total data which is shown without the flag. **63. Improved Protection Against ZIP Bombs** The Anti-Virus subsystem has been updated to offer better protection against ZIP bomb attacks. The "Scan" Compression Ratio Action has been removed. Existing configurations will automatically be converted to use "Drop" instead. Moreover, the Compression Ratio setting can no longer be configured with values greater than 500. **64. Removal of Global Enable IPv6 Setting** The advanced IP setting to globally enable IPv6 has been removed. From now on, IPv6 only needs to be enabled on the interface. **65. Clarified Log, Event and Mail Alerting Configuration** The Log, Event and Mail Alerting configuration has been split up into separate sections in order to be easier to find and configure. **66. Connection Replacement Statistics Counter** A statistics counter for the number of connections replaced per second has been added. Connections are replaced when the maximum number of allowed connections within the system has been reached and can be an indication of abnormal traffic load. The value can be polled by using SNMP. **67. New Application Control Library** The Application Library has been updated. **68. Updated GeoIP Database** The GeoIP database has been updated
11.10.01	**1. Improved fragmented packet handling** The possibility to drop fragmented SYN packets and/or SYN packets carrying payload data was added. The default settings for these options are: drop and log. **2. Improved Protection Against ZIP Bombs** The Anti-Virus subsystem has been updated to offer better protection against ZIP bomb attacks. The "Scan" Compression Ratio Action has been removed. Existing configurations will automatically be converted to use "Drop" instead. Moreover, the Compression Ratio setting can no longer be configured with values greater than 500. **3. Update New Application Control Library & GeoIP database** **4. More categories added to Web Content Filtering**

	More categories allowing more granular control of Content Filtering in Web and email Control Profiles. **5. IPv6 support for IPsec tunnels** Support for IPv6 in IPsec tunnels has been added. This makes it possible to tunnel IPv4 packets inside an IPv6 tunnel, IPv6 in IPv4 or tunnels using IPv6 addresses only. The tunnel peer can be specified using an FQDN that resolves to an IPv4 or IPv6 address. CRL lookups can be performed against an IPv6 address. **6. Grouped FQDN Address objects** It is now possible to create and use groups of FQDN/DNS Addresses. **7. Support for Strong Password Policy** It is now possible to enforce a policy to ensure that user passwords within the local user database comply with predefined complexity rules. **8. Support for Multiple IPsec Config Mode Pools** The system now supports multiple config mode pools. Each IPsec interface can be configured to use its own pool or share pools with other interfaces. The pools can be configured to either distribute IPv4 or IPv6 addresses. **9. FQDN Address Object Support for IPsec Remote Endpoints** Host names that could resolve to multiple IPv4 and IPv6 addresses can be used as remote endpoint for IPsec tunnels. The firewall will connect to one IP only when acting as initiator (the first IP received from the DNS server), however all other resolved IPs are allowed to negotiate using this tunnel for incoming tunnel negotiations. Existing configurations using the 'dns:' keyword for FQDN names will get converted to FQDN address objects. **10. Option added to User Authentication Configuration** A new option has been added to the User Authentication Rule configuration object that makes it possible to specify in Multiple Username Logins to only allow one login per username without any exception. **11. IPsec Configuration Improvements** Many configuration options in the IPsec configuration pages in the WebUI have been modified and moved around to give a better overview of the IPsec configuration properties.
11.04.01	**1. Tunnel Monitoring of IPsec Interfaces** This feature enables ICMP ping monitoring of a host and when the host stops answering, the tunnel's IKE and IPsec SAs are removed and a new negotiation will be triggered. ICMP ping messages will be sent every second and if a configurable amount of packets has been lost, the tunnel monitoring will trigger renegotiation. **2. SNMPv3 Support** The system has been extended with SNMPv3 support allowing authentication and encryption to the SNMP management interface. The default local user

database is used as the authentication source for SNMPv3 credentials and the supported encryption method is AES.

3.   Protection Against Password Brute Force Attacks

Password brute force attack protection is now always active for local user databases. Log events and a list of temporarily blocked users have been added to help the administrator monitoring the activity of the feature.

4.   Transparent Mode Configuration in the Startup Wizard

Configuring transparent mode can be a fairly complex task. To speed up the process, a configuration step to enable transparent mode has been added to the Startup Wizard. The wizard step allows the administrator to select which interfaces to use in the transparent mode setup and whether DHCP and Layer 2 pass-through should be enabled or not.

5.   Automatic Daylight Saving Time

The configuration of Daylight Saving Time (or "Summer-time" as it is called in some countries) has been enhanced by adding an automatic mode where the administrator specifies a location name. The system then applies the local DST rules.

6.   IPv6 Router and Prefix Discovery

The system can now as a host locate IPv6 routers and network prefixes on Ethernet, VLAN and Link Aggregation interfaces. This can be used with the system DHCPv6 client or by itself using address auto-configuration.

7.   Web Profile

URL Filter Profile and Web Content Filtering Profile have been combined into one Web Profile for a simpler way of configuring IP Policies. Existing URL Filter Profiles and Web Content Filtering Profiles will be converted into the new type upon upgrade.

8.   User Authentication REST API

A REST API for managing authenticated users has been added. The API supports logging in and out users as well as retrieving information about logged in users. Additional information can be found in the NetDefendOS REST API manual.

9.   Broadcast Forwarding

The administrator can now configure the system to apply IP Policies to and forward broadcast packets in both Transparent Mode (Layer 2) and static Routing Mode (Layer 3) scenarios.

10. IPv6 Web Content Filtering and Anti-Virus on HTTP data

The HTTP ALG and Light Weight HTTP ALG can now be used with IPv6 IP Policies and Rules. This opens up the possibility to enhance security of HTTP data transfers with features such as Active Content handling, File Integrity checks, Web Content Filtering, Anti-Virus Scanning and URL Filtering.

11. IPv6 support in Loopback interfaces

Loopback interfaces have been enhanced to enable IPv6 communication, allowing the administrator to apply more advanced IPv6 routing scenarios.

12. WebUI Time Synchronization Improvements

The WebUI Date & Time configuration page has been extended with a button for forcing an immediate time synchronization. The button will appear when time synchronization is enabled by using NTP. In addition, status fields have been added to inform the administrator of recent time synchronization activities and will also state the time of the next synchronization attempt.

13. Custom Banner Support for LW-HTTP ALG

The Light-Weight HTTP ALG now supports the possibility to customize the different banner pages that are displayed in place of blocked websites.

14. Improved logs for the HTTP Poster

The HTTP Poster has been extended with more logs giving an indication whether the post succeeded or not.

15. LW-HTTP ALG IPv6 Support

The Light Weight HTTP ALG can now be used on IPv6 traffic.

16. FQDN Support in IP Policies

Create easy-to-use and efficient IP Policies by using the new FQDN address objects as an alternative to policies based on IP addresses. FQDN based IP Policies can drastically reduce continuous administration as changes of IP-addresses are automatically detected and updated using DNS, without any need for manual maintenance tasks.

17. GEO IP Support in IP Policies

GEO IP support in IP Policies adds the possibility to create policies based on the geographical location of an IP address. This can be a powerful feature when trying to combat advanced threats or when mitigating the consequences of a Denial of Service attack that has its origin from countries that are not part of the normal traffic pattern.

18. Mail Alerting

The new Mail Alerting feature helps administrators detect abnormal behaviors and take rapid action when needed. Customizable thresholds, filters and interval timing enable the administrators to fine-tune the feature to fit specific needs and requirements in an optimal way.

19. TLS 1.2 Support for the Web User Interface

TLS 1.2 is a significantly more secure and robust version of TLS than its predecessors and allows administrators to use the Web interface with added security.

20. Voice over IP Profile

New and improved way of configuring Voice over IP using the intuitive Policies section instead of the IP Rules section.

21. SHA-256 Support for SSL/TLS

The SSL/TLS ALG has been improved with support for the SHA-256 hashing algorithm to enhance security.

22. Extended IP Policy Support

New IP Policies have been added to the system to allow configuration of Server Load Balancing, Multicast and Stateless connections using the newer and intuitive Policies section instead of the older IP Rules section.

23. Color Coded Memory Log Messages

Improved and more intuitive presentation of memory log records. Log records are color coded according to the severity group which makes it easy to directly spot critical and important events without having to read through hundreds of log records.

24. Configuration Scripts

Upload script files directly in the web user interface in a convenient and user-friendly way.

25. Support for SHA2 Hardware Acceleration

Hardware acceleration of the SHA-256 and SHA-512 hashing algorithms is now possible on the DFL-1660/2560/2560G/870.

26. IPsec IKEv2

The IPsec engine has been extended with support for IKEv2. Compared to IKEv1, IKEv2 provides faster tunnel setup negotiation with fewer messages exchanged and increased stability. IPsec tunnels can now be configured in IKEv1, IKEv2 or Auto mode where auto allows a fallback to IKEv1 for non IKEv2 capable peers. In IKEv2 mode, the Extended Authentication Protocol (EAP) authentication method is supported. IKEv2 has been tested for roaming clients using Windows 8.1, Windows 10 and Mac OS X 10.11.

27. Anti-Virus for IMAP

The system now supports Anti-Virus scanning of e-mail attachments transferred over the IMAP protocol. Anti-Virus scanning of IMAP transactions can be enabled on an IP Policy that uses a service with the protocol field set to IMAP.

28. Anti-SPAM for POP3 and IMAP

The system now supports Anti-SPAM for POP3 and IMAP, with fully configurable threshold levels and usage of mechanisms such as Reply Address Domain Verification, DNS Blacklisting and Distributed Checksum Clearinghouses (DCC). Malicious Link Protection detects malicious links in e-mails and protects users from clicking on them by breaking the malicious link. E-mails identified as SPAM can be tagged by the system in both subject and headers to notify the end-users mail clients that the e-mail is identified as SPAM. Configurable whitelists and blacklists allow the administrator to statically decide how to treat e-mails to and from specific IP address and e-

mail addresses, such as bypassing SPAM protection for certain IPs or e-mails. Please note that DCC is a subscription based feature.

29. Anti-Virus Support for Scanning of ZIP-in-ZIP Files

The system now supports antivirus scanning of nested ZIP files, i.e. ZIP within ZIP files, transported over HTTP or FTP, configurable to support up to 10 levels of ZIP-in-ZIP.

30. IMAP File Control with MIME Type Verification

The system can now block unwanted E-mail attachments transferred over the IMAP protocol. File Control comes with MIME type verification, which allows blocking of files that claim to be of a specific type according to its file extension while the file contents indicate another type.

31. IPv6 HA Support

The DFL-1660/2560/2560G/870 now support redundancy in a high availability setup while actively forwarding IPv6 traffic. Note: DFL-260E/860E don't support High Availability.

32. DHCPv6 Client

A DHCPv6 Client has been added, which can be used on Ethernet, VLAN and link aggregation interfaces.

33. IPv4 Path MTU Discovery

The system now supports IPv4 Path MTU Discovery which allows communicating endpoints to use optimal packet sizes that prevent fragmentation at intermediate routers.

34. SSL/TLS AES 128 and AES 256

The system now supports AES 128 and AES 128 SHA-1 cipher suites to be used by the TLS-ALG and Web UI HTTPS management. It is recommended to review currently used SSL settings and disable unsecure ciphers.

35. Use of HMAC-MD5 in IPsec and SSH

Due to known weaknesses with the MD5 crypto hash function, the use of HMAC-MD5 based integrity algorithms has been disabled in default configurations. For legacy compatibility reasons, HMAC-MD5 is still supported and can be enabled in the configuration.

36. Use of HMAC-SHA1 in IPsec

Due to known weaknesses with the SHA-1 crypto hash function, the use of HMAC-SHA1 based integrity algorithms has been disabled in default configurations. For legacy compatibility reasons, HMAC-SHA1 is still supported and can be enabled in the configuration.

37. Improved Anti-Virus Block Pages for HTTP

The system now supports an Anti-Virus cache that allows improved notification pages when viruses are found in large files.

38. IP Policies with Application Layer Functionality

The system has been improved with protocol specific settings applicable to IP

Policies. Previously, layer 7 features for FTP, TFTP, TLS and PPTP were only configurable using an Application Layer Gateway (ALG) and an IP Rule. With 11.02.01, these settings can now be configured directly on the IP Policy as long as the selected service is configured with a matching protocol in the protocol field. When using an HTTP/HTTPS service, it is possible to control HTTP protocol syntax validation. Some features e.g. Anti-Virus will enable protocol validation automatically in the background if needed.

39. HTTP Content Inspection Improvements

A new lightweight HTTP ALG is now supported that more efficiently can handle content inspection of HTTP, such as web content filtering and client user-agent filtering. The new HTTP ALG is more efficient and requires less resources which leads to higher HTTP content inspection throughput capabilities.

40. Updated Pre-Defined Services

To simplify the configuration of advanced features for IP policies e.g. Anti-Virus and email control, the list of pre-defined services has been updated with protocol settings for services that can be used with IP policies. Deprecated services that could only be used by Application Layer Gateways (ALGs) have been removed. These changes apply only to new configurations/installations and do not affect existing systems or configurations.

41. TLS improvement

The TLS library has been enhanced to provide better security.

42. Automatic Exception Reporting

Automatic exception reporting has been added. Crash reports are automatically sent to D-Link anonymously and encrypted once the system has booted up after an incident. Crash reports help D-Link to identify critical issues and to provide a correction quicker. The functionality may be disabled via the Diagnostics Settings.

43. RADIUS Relay Improvements

RADIUS Relay now supports manual configuration of the interface where the user traffic is expected for authenticated users via the "Override User Data Interface" setting. This is needed if the interface used for the user data traffic is different from the interface where the RADIUS messages are sent to the system.

44. Improved Support for Virtual Routing

The system now supports configuration of the source IP to use when communicating with RADIUS and LDAP for authentication, as well as configuration of the source IP to use when performing route monitoring. This is useful in virtual routing scenarios where the interface IP is not necessarily

the correct IP to use as source IP for this communication.

45. SHA-2 Signed Certificates for IKE Authentication

The system now supports using SHA-2 signed certificates for IKE

authentication, including SHA-256, SHA-384 and SHA-512 hashing

algorithms.

46. Configurable Behavior for CRL Failures

The system now supports configuration of how the system should behave

when a CRL for a certificate cannot be accessed on the CA server. A

"conditional" option has been added to allow use of the certificate even if the

CRL cannot be accessed.

47. Configurable CRL Distribution Points for Certificates

The system now supports configuration of the CRL distribution points (CDPs)

to use with a certificate.

48. Configurable Differentiated Services field for IKE packets

The system now supports configuration of the value of the Differentiated

Services (DSCP) field in the IP header of IKE packets sent by the system.

49. MIB File Download via Web UI or SCP

The system MIB files can now be downloaded directly from the device either

via the web user interface or via SCP.

50. Improved SNMP Support

The system can now keep interface SNMP indexes and interface OIDs

persistent during reconfigures and restarts.

51. Traceroute Support in CLI

A new "traceroute" CLI command has been added that can be used to

perform traceroute towards domain names, IPv4 and IPv6 addresses.

52. Improved Ping CLI Command

The "ping" CLI command has been improved to support ping towards IPv6

addresses and domain names.

53. L2TP CLI Command

A CLI command has been added to list active L2TP client sessions.

54. Improved ifstat CLI Command

The ifstat CLI command now prints the link status of any configured

interfaces when executed without any arguments.

55. Improved 'ike -show' CLI Command

The 'ike -show' CLI command now prints the local and remote IDs in addition

to the existing interface, remote and local endpoints.

56. PPTP CLI Command

A CLI command has been added to list active PPTP client sessions.

57. Improved Statistics for IKE/IPsec

The statistical counters available via SNMP for IKE/IPsec have been improved

to include a wide range of statistical values useful for troubleshooting or

monitoring.

10.22.01	**1. RADIUS Management Authentication:** Remote management with the WebUI and CLI now supports using RADIUS as the authentication source.
10.21.02	**1. True Application Control:** 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. **2. SSL Inspection for Application Control:** 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. **3. IKE/IPsec HA synchronization:** 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. **4. IKE/IPsec Virtual Routing support:** 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.

23. Web Content Filtering update:

Web Content Filtering category 31 has been changed from "Spam" to "Remote control/desktop".

24. Improved certificate information in the CLI:

The CLI has been improved to show more detailed information about the IPsec certificate cache.

25. Alias for routes

It is now possible to use "route" as an alias to the CLI command "routes".

26. High Availability Status in the Web User Interface

The current High Availability status is now visible in the "System Information" list on the main status page in the web user interface.

| 2.60.02 | 1. **New Web User Interface:** The Web User Interface has been reworked with a more user friendly touch. Administrative tasks can now be performed faster with less work and is more intuitive, even for the less experienced user.

2. **Application Control:** Support has been added to control what applications users behind the firewall are using. It is now possible to select what applications should be allowed and the administrator can monitor data transfer and other statistics for the applications accessing the Internet.

3. **IPv6:** Numerous changes have been implemented in order to improve interoperability and protocol compliance.

4. **User Identity Awareness:** The administrator of a firewall now has the possibility to control the access of users authenticated to a Windows Active Directory Domain.

5. **Routing support in SSL VPN Client:** It is now possible to configure routing information for SSL VPN clients. In addition to the default use of all-nets, explicit routing information can be supplied to the client.

6. **Web Content Filtering for HTTPS:** Web Content Filtering support has been added for HTTPS traffic.

7. **L2TPv3 server support:** Support had been added to create L2TPv3 server interfaces. With these, Ethernet and VLAN interfaces can be interconnected through the networks using the L2TPv3 protocol.

8. **URL filter for HTTPS:** URL filter support has been added to the HTTP ALG when using the HTTPS protocol.

9. **Route Fail Over Enhancement:** A Route Fail Over setting has been |

added - 'Gratuitous Proxy ARP On Fail' that enables the transmission of gratuitous ARP packets on fail over to alert hosts about changed interface Ethernet address of Proxy ARPed hosts.

10. **Search filter enhancement:** The search filter on the memory log pages was using a lot of space at the top of the page. The filter is now by default hidden, only showing the free text search form. The entire filter can be shown by clicking its header.

11. **WebUI speed improvement:** The speed of browsing through the WebUI, in particular pages where there is a large number of objects, has been improved.

12. **Logout message for DHCP server:** A new feature has been added to 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.

13. **High Availability role switch improvement:** The role change between High Availability nodes has been enhanced with a seamless transition to ensure uninterrupted traffic in the network.

14. **Added "IPA" as recognized MIME type** An .ipa file is an iPhone application archive file which stores an iPhone app.

15. **Support for hardware acceleration of IKE negotiations:** Hardware acceleration of IKE negotiations is now possible on the DFL-2560 and DFL-2560G models to offload the CPU and make IPsec tunnel setup faster.

16. **Chain of certificates** The use of certificates has been enhanced to support configuring a chain of X509 root certificates to use with the HTTPS Web Administrator page, SSL VPN Portal, TLS ALG and Use Authentication Rules.

17. **Enhanced ICMPv6 configuration:** A setting was added to control the maximum number of ICMPv6 Neighbor Discovery Options allowed and hence improve network security.

18. **New PPP configuration settings:** A new 'Advanced Settings/PPP settings' row is created in WebUI. A new 'Initial Resend Time' value is added and the existing 'Max PPP Resends' value has been moved to this new dialog page

19. **Ping CLI parameter renaming**
The ping CLI command has been updated with a more logical parameter naming. The '-recvif parameter is now renamed to '-srcif'.

	20. **HTTP ALG: Added "Force SafeSearch" option:** A new option "Force SafeSearch" has been added to the HTTP ALG. This option can be enabled so search queries to Google, Bing and Yahoo through this HTTP ALG will be modified to enforce the SafeSearch functionality these search engines provide. 21. **L2TPv3 server enhancement:** The L2TPv3 server has been improved to better handle scenarios with a high amount of L2TPv3 clients connected to the same L2TPv3 server interface. 22. **L2TPv3 client** Support for L2TPv3 client has been added. The client can be configured to run over an Ethernet or a VLAN interface. Protocols supported are UDP and IP. In addition to this, extended security can be added by routing the L2TPv3 client through an IPsec interface. 23 **New 'ipver' argument to the 'connections' CLI command:** The 'connections' CLI command has been enhanced with an additional argument '-ipver=' that makes it possible to list only IPv4 or IPv6 connections. 23. **SHA256 and SHA512 IPsec algorithms:** The IPsec engine now supports the SHA256 and SHA512 algorithms to be configured on IPsec tunnels.
2.40.03	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. 2. Added "IPA" as recognized MIME type. 3. Support for hardware acceleration of IKE negotiations for DFL-2560/2560G to offload the CPU and make IPsec setup faster.
2.40.02	No new features are introduced in the 2.40.02 release.
2.40.01	1. Support the Cisco IPSec client on iPhone. 2. Double Web Content Filtering local cache size on all models to accommodate more categorized sites. 3. Support CHAP, MS-CHAP, MS-CHAPv2 and No authentication mechanisms for SSL VPN. 4. Web Content Filtering Configuration Improvement. When filtering override is enabled, it is now possible to enter a custom timeout of the override period.
2.40.00	1. Support for IPv6 in routing, IPRules and Policy Based Routing in Ethernet as well as VLAN interfaces.

	2. Remove restrictions on the number of HTTP posters. All other network clients listed in "Misc Clients" also benefit from this restriction removal. 3. Support authenticating users using the Ethernet MAC address over HTTP(S). 4. Update password field: when focus is moved to a text input field which contains a password, the field will now be cleared so the user can type in a new password directly. 5. 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.
2.30.01	1. Support SSL VPN feature. 2. Support TLS renegotiation (RFC 5746) in the TLS ALG. 3. Increase the number of IDP signatures to up to 30,000. Configuration of up to 30,000 IDP signatures is now possible. (Affected models:DFL-1660/2560/2560G) 4. Add clone functionality to Web GUI. It's now possible to create a copy of an object in the Web GUI by selecting Clone in the context menu in the data grids, the edit page will pop-up with information copied from the original object. 5. Enhancement of services drop down menu. The drop down menu for services has been enhanced to show port numbers. 6. Enhanced IDP signature configuration. It's now possible to select IDP signature groups from a visual tree interface. 7. Add lifetime for connection in the log messages. 8. Warning for incompletely cloned objects. When cloning objects that contain properties which cannot be cloned, an alert will be displayed. 9. Support for dynamic server addresses in SSL VPN. The SSL VPN server has been updated to support the sending of an optional domain name (FQDN) to the client that will be used to connect to the server.
2.27.02	1. The D-Link DES-3528 switch can now be used by ZoneDefense. 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+.
2.27.01	1. A confirmation question will be prompted if the user attempts to execute a CLI command that may cause system delays.
2.27.00	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.
	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.
	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.
	4. The script command has been updated to handle adding objects with dependencies between each other.
	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.
	6. All rule page layouts have been updated for how to enter the interface and network combination to be more intuitive.
	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).
2.26.02	*[DFL-210/260/800/860/1600/1660/2500/2560/2560G]* 1. Added the possibility to disable and enable Ethernet interfaces using WebUser Interface. 2. Separate icon for User Authentication enabled objects. 3. Improved file names for backup packages, including the configuration version number. 4. Connection Rate Statistic Values can be viewed using SNMP.
2.26.01	*[DFL-210/260/800/860/1600/1660/2500/2560/2560G]* 1. The name of the authenticated user is logged together with the requested URL in HTTP ALG log messages *[DFL-160]* 1. DHCP relaying through the firewall in transparent mode is supported 2. 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:

Firmware Version	Modified Features
10.21.02	1. Disable SSLv3 support due to the vulnerability CVE-2014-3566
2.30.01	1. The firmware 2.30.01 and latter would ONLY be applied on the current platform: DFL-260E/860E/1660/2560/2560G
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
12.00.16	1. IDP content scanning could in some rare occasions report false positives. 2. Content scanning using IDP sometimes failed to find and report the pattern specified in certain IDP signatures. 3. The Web Profile Fail Mode setting was not always obeyed. 4. Incoming packets were not captured when using packet capture on a Link Aggregation interface. 5. IDP content scanning sometimes worked incorrectly when the triggering content was divided in multiple packets. 6. On rare occasions, the firewall could make an unexpected restart when having PPTP interfaces configured.

7. A High Availability system with IPsec configured sometimes restarted unexpectedly during reconfiguration.

8. DNS responses were dropped by the DNS ALG if the length of the response packet exceeded 512 bytes or the EDNS0 "UDP payload size" was included in the response packet.

9. The Setup wizard contained a reference to an obsolete way of configuring and when using it, there was an error displayed.

10. The setup wizard did not have a button for going back to the previous page.

11. Validation of upgrade packages using old upgrade package format failed with an error. The upgrade notification page now correctly handles old upgrade packages

12. During a reconfiguration, the system could stop responding and eventually restart unexpectedly if no route existed to the Remote Endpoint of an IPsec tunnel using AutoEstablish.

13. The system could in some rare occasions, due to an error in the IPsec subsystem, restart unexpectedly after a reconfiguration.

14. It was possible to set link speed to 10 Gbps when manually changing link speed.

15. Memory consumption increased over time when the system performed IP Reputation updates.

16. The timer at save and activate was set too high. It has now been decreased to 25 seconds.

17. An incorrect URL was used for web content filtering reclassification.

18. The "groups" property in the REST API user authentication list was limited to 255 characters before being truncated. The limit has been increased to 2048 characters.

19. IPsec user logged in via XAuth or EAP was sometimes logged out after the "Idle Timeout" on systems using IPsec hardware acceleration even if the user was active.

20. Android phones could encounter an issue where they would be required to authenticate again after becoming disconnected from WiFi when using DHCP server with HTTP authentication.

21. The configuration page for IDP did not follow the same design as similar pages with address filters.

22. If DHCP client was enabled on a VLAN interface, the assigned IP details were not shown for the respective objects in the status page of the web user interface.

	23. IPsec tunnels could in some situations stop working after High Availability Failover. 24. The firewall could on rare occasions restart unexpectedly when using L2TP servers. 25. On rare occasions, the system could make an unexpected restart when handling traffic on interfaces in Transparent Mode. 26. The system sometimes restarted unexpectedly when processing IPsec traffic. 27. The DNS resolver could not parse some messages utilizing message compression which could lead to e.g. reduced anti-spam performance. 28. The on/off sliders in the web user interface were sometimes too narrow to fit all text.
12.00.13	1. Unknown algorithms in received IPsec proposal lists for IKEv1 could fail the whole negotiation. [**DRU20180910000002, DRU20171121000004**] 2. L2TPv3 interface responds with the incorrect mac address. 3. The way interface packet queues were flushed during reconfigure could cause unnecessary packets loss. It could result in packet loss when NetDefendOS performs a reconfigure even when the system load was low. Affected model DFL-870. [**DRU20180314000003**] 4. Poll Offloading feature could lead the firewall crashed. Poll Offloading is a functionality/feature that increases Firewall's performance on certain hardware appliances by utilizing a secondary CPU core which ultimate and only job is handling Firewall's Ethernet interfaces polling function. Please refer to the page 989 on the user manual 12.00.13. [**DRU20171108000005**] 5. Gratuitous ARP was not sent at startup on some devices and interface types. 6. The system could on rare occasions restart unexpectedly during IDP or antivirus updates. 7. On rare occasions the firewall could make an unexpected restart when having interfaces in Transparent Mode. 8. The ARP table was not correctly updated in a rare scenario when using a DHCP server. 9. The system sometimes restarted unexpectedly when handling fragmented traffic. 10. MIME extended filenames without character set or language were not parsed correctly. 11. The system sometimes restarted unexpectedly when receiving traffic

handled by the HTTP ALG. [**DRU20171128000002**]

12. The system could restart unexpectedly when receiving TFTP traffic through the TFTP ALG

13. On rare occasions, the firewall could make an unexpected restart when using the HTTP ALG and users accessed certain web server.

14. The config converter for the Strong Password setting didn't correctly handle the upgrade of factory version configurations.

15. In certain configuration scenarios the system could make an unexpected restart during an IPsec negotiation.

16. Infected files were only partially blocked in some SMTP anti-virus scenarios.

17. The AutoEstablish feature on IPsec Tunnels only retried to connect the tunnel once if the remote endpoint didn't respond.

18. Configuring time sync servers where some of the IPs weren't reachable in the routing table made the time sync to fail even though other IPs could have been reached.

19. Some hardware accelerators caused the port update of the IKEv1 SA to fail when the port needed to be changed because of an incoming ESP packet.

20. When acting as an IKE responder, NetDefendOS did not validate that the config mode IP handed out to the client matched the client's first traffic selectors. This could cause unnecessary IPsec SAs on the responder side.

21. The system could restart unexpectedly during reconfigure if the system contained active SSL VPN users.

22. An IPsec EAP tunnel could stop working after a number of tunnel connection setups.

23. The VLAN command showing detailed information about a VLAN interface did not contain any information about IPv6 addresses.

24. Users were unable to see what errors occured on the configuration of the device after uploading a script.

25. Packets did in some configured scenarios not always retain the original source MAC address in transparent mode.

26. If Route Monitoring failed on a route used for RADIUS authentication for an L2TP/PPTP Interface, unexpected system restarts could in some rare occasions occur.

27. The SNMP value HOST-RESOURCES-MIB::hrSystemDate would be generated incorrectly when one of the time fields was zero resulting in partly invalid timestamp. The SNMP timestamp is now correctly formatted.

28. The WebUI configuration page showed an incorrect unit for the router

priority of an OSPF interface.

29. IPsec tunnels used the IP address with the oldest lifetime when it tried to connect to an endpoint specified as an FQDN. It should now start with the latest IP address added instead.

30. An SNMPv3 event receiver did not use the specified routing tables when attempting connections to their specified IP addresses if the configured routing table was different from the main routing table.

31. After a reconfiguration when changing the IPsec ConfigModePool object, the system could restart unexpectedly.

32. Upgrading a firewall could cause reboot loops if OSPF interfaces referred to an IPsec Tunnel as interface and the network wasn't set.

33. SNMP statistics was not available for some IP Policies.

34. IPsec rekey were not triggered correctly by an HA cluster node that imported its SAs from its cluster peer.

35. The DHCP relay autosave timer was not used.

36. The distinction of IPv4 and IPv6 on the DNS client configuration page was missing.

37. DHCP Relay PPM limiting incorrectly applied to both requests and responses. Now it applies only to requests.

38. Using Auto Establish on an IPsec tunnel could lead to duplicate IPsec SAs and/or negotiation failures.

39. The system sometimes restarted unexpectedly due to an error in the IPsec engine.

40. Removing an HA synced User could trigger unexpected behavior on the inactive node.

41. The system sometimes restarted unexpectedly when mail was handled by the SMTP or IMAP ALG.

42. The IPsec subsystem could in some rare occasions cause the system to restart unexpectedly.

43. Upgrading a firewall firmware when running with configuration version 1 would bypass the strong password check resulting in that the admin user would be disabled and unable to login. The strong password feature is now disabled if initiating a firmware upgrade when the firewall is running a configuration with version 1 to prevent lockout.

44. Email with very long padding just before end-of-email marker could cause a stall in SMTP and POP3 ALGs.

45. Antivirus did not work as intended for singlepart messages when using POP3 or SMTP.

46. Multiple IKE SAs against the same peer with the same authentication method could cause issues with dropped traffic at rekey or HA failover. The peers of the tunnel could end up with different numbers of IKE/IPsec SAs if both peers initiated a negotiation at the same time. This could lead to packet loss for an extended time at rekey or failover until the peers detected and resolved the different states. The firewall is now more restrictive with multiple negotiations against the same peer to avoid any differences in state between the peers.

47. The Web Content Filtering Log page would display a "No Logs" message even though the page contained WCF logs.

48. The HTTP ALG handled HTTP responses for certain web pages incorrectly and made them unreachable. A system log about an 'invalid server http header received' was seen when trying to reach those pages.

49. Memory corruption could in some rare occasions occur during an IPsec Informational message exchange.

50. IKEv1 could be vulnerable to a Bleichenbacher attack when used in IPsec tunnels configured with certificate authentication. Reference ID CVE-2018-8753.

51. The IPsec interface name was not shown in the interface column in the web user interface memlog. The interface name was instead shown in the general text line.

52. Some IPsec log messages used source_ip and dest_ip as parameter names, while most other subsystems use srcip and destip as parameter names. The parameter names have been updated to be more aligned with the rest of the system. IPsec log message ID 103, 110, 111, 112, 113, 114, 115, 116, 117, 118 and 119 have been updated. This change also makes the source and destination IPs be parsed in the correct columns in the web user interface system log page, instead of being shown in the general text part of the message.

53. The firewall could on rare occasions make an unexpected restart after logging into the WebUI when receiving a large number of user authentication requests against the REST API.

54. ARP Cache authenticated users were not listed in the mouse-over popup on the dashboard. The users were counted in the total value, which made the sum of all authentication methods not match with the total value.

55. Multiple IPsec rekeys were sometimes initiated when IPsec Lifetime KiloBytes was exceeded.

56. After HA failover Application Control connections could stop working

because of faulty classifications. The Application Control binding is removed from connections on HA failover to prevent connections from being miss classified.

57. OSPF did not send any updates for a period of time after a reconfigure, which could cause problems for other OSPF nodes.

58. Some checkboxes in the Web User Interface did not enable additional configuration options (where applicable) when checked.

59. The High Availability Wizard had graphical errors which made it hard to select interfaces in the combobox controls.

60. Entries in the neighbor cache could sometimes linger forever.

61. There was no configuration warning when services dependent of IP Reputation were configured and no valid IP Reputation license was installed.

62. Application rule dialog had no scrollbar when the window had been resized to be very small.

63. Gratuitous ARP queries was not correctly forwarded in transparent mode.

64. The system could sometimes restart unexpectedly when processing specially crafted HTTP headers.

65. DIGEST-MD5 authentication for SMTP was not fully supported.

66. Threshold rules could trigger on connections opened by an ALG even when it shouldn't.

67. Changing cluster ID on an HA cluster could cause the state synchronization to fail between the cluster members until a restart of the member.

68. The web user interface DHCP Server status page could render incorrectly if special characters were used in the DHCP hostname.

69. Log messages containing special characters could prevent the WebUI System log page to render correctly. System log page has been updated to better handle special characters.

70. It was not possible to disconnect an IPv6 session using the session manager CLI command.

71. When issuing the 'rules' CLI command when having more than 1000 rules or policies defined, the index column would display '...' for indexes larger than 999.

72. The SSH server only supported AES ciphers in CBC mode, not in CTR mode.

73. It was not possible to retrieve statistics via encrypted SNMP (SNMPv3 in AuthPriv mode) on models DFL-260E/860E.

74. Emails could not be sent through the IMAP ALG for some email clients that

were set to save a copy of the mail in the sent folder.

75. Sending fragmented IP packets into an IPsec transport mode tunnel, where the resulting ESP packets were fragmented again when going out on the Ethernet interface, would cause the packets to be dropped by the receiver. The packets couldn't be reassembled correctly by the receiver due to lost fragmentation information. All fragmented IP packetsgoing into a transport mode IPsec tunnel are now reassembled before encryption.

76. When acting as an L2TP/Client, the IPsecTunnel was incorrectly required to be configured with "SetupSAPer" to "Host" to be able to negotiate the tunnel successfully.

77. ID passed from the IKE negotiation to the RADIUS server was incorrectly formatted when an IP address was used as ID.

78. DHCP server sent duplicate NAKs for some requests, occasionally with invalid options.

79. A modification to a netobject configured on a user in a user local database didn't take effect until after a restart.

80. DHCPv6 server and client did not treat the DUID as an opaque value and therefore did not work correctly with other devices using the newer UUID type.

81. Some items in the MIB had incorrect variants of unsigned integer types.

82. The system could in some rare occasions restart during an IPsec EAP negotiation.

83. It was possible to authenticate multiple users on the same IP / Interface combination using different username. The IP / Interface is now enforced as unique identifier.

84. The calculation of the shared MAC address on Link Aggregation interfaces, when UseUniqueSharedMac is enabled, was using the same MAC address for all Link Aggregation interfaces.

85. The Address column inside Address Folder objects only showed a single address for High Availability objects.

86. Packet loss at rekey triggered an unnecessary tunnel deletion for IKEv2 tunnels.

87. The firewall responded to a peer with no PFS, even though the peer was only suggesting one PFS group, if "None" was part of the configured PFS groups. Scenarios where NetDefendOS is used on both endpoints may fail after upgrade if only one is upgraded to this release. Upgrade both endpoints or make sure the PFS groups are configured with the samevalues on both peers to ensure a working tunnel after upgrade.

88. The extended connection information e.g. data usage and identified application was not visible when printing IPv6 connections using the "connections" CLI command.

89. An IPsec EAP negotiation using a UserAuthRule with RADIUS as agent, could in some rare occasions lead to memory corruption if the negotiation happened at reconfiguration.

90. CLI command to force blacklist unblocking would sometimes remove wrong entries or all entries.

91. A large number of authenticated users would in certain scenarios lead to high CPU load on the firewall when used in High Availability cluster.

92. RADIUS protocol packet field for NAS-Identifier incorrectly sent a null termination character in the value string.

93. IKEv2 tunnels with failed negotiations could in some situations cause leakage of IKE SAs and eventually cause a max_ike_sa_reached log event. When this happens, no more IKE tunnels could be established.

94. If SSH remote management was configured for a specific interface, the SSH server could only be accessed using the core IP address for that specific interface. The behavior of SSH remote management is now changed to allow access from an interface usingany core IP address, consistent with how HTTP remote management works.

95. Log messages containing special characters could prevent the WebUI System log page to render correctly.

96. IPsec could leak memory on hardware models using specified CPU accelerators. Affected models: DFL-1660/2560/2560G.

97. Threshold rules could trigger on connections opened by an ALG even when it shouldn't.

98. The DHCP Client did not handle link down event correctly. The client could enter the discovery state without completely resetting previous values.

99. The file extension lists in the File Control profile could not handle long lists of file extensions.

100. HTTP protocol upgrade to e.g. websockets was not allowed when using an IP Policy with a Web Profile. Protocol upgrade is now allowed as per default.

101. The system incorrectly allowed configurations of RemoteManagementSSH objects where neither RSA or DSA were configured as host key. It was also possible to store configurations with neither password or public key as authentication method.

102. Several CLI commands that could modify the state of the system did

not require administrator privileges. The following CLI commands can no longer be executed as auditor: arp - flush, nd -flush, time - set, route - flushl3cache, zonedefense -blockip/blockenet, ike -delete, dhcp -lease renew/release, dhcp6 -lease renew/release, ha -activate/deactivate andldap -reset.

103. When an FQDN was resolved to both IPv4 and IPV6, the IPv4 addresses were overwritten by IPv6 addresses in the IPsec peers table, which led to some invalid entries in said table.

104. Users were unable to choose whether to send upper or lower cased Ethernet addresses for MAC/ARP authentication in user auth rules.

105. The reported SNMP value type for "HAStatusRole", "HAStatusState" and "HAStatusTimeWithinState" used the wrong datatype. The reported SNMP values have been updated to the correct datatype Integer.

106. Users were unable to test a ZoneDefense switch with an address inside of an address folder.

107. Disabled objects were shown in the available list in the WebUI group controller.

108. The ICMP service for IPv6 service was named IPv6-ICMP. It has now been renamed to ICMPv6 which is the name used in eg the RFC.

109. When issuing the 'rules' CLI command when having more than 1000 rules or policies defined, the index column would display '...' for indexes larger than 999.

110. An error message related to antivirus was displayed even though antivirus was not in use.

111. The date-time picker in the WebUI could malfunction when using non-English languages.

112. Configuring an SMTP ALG could lead to an unexpected restart.

113. The HTTP ALG could block certain file types that use ZIP format.

114. Excluding ipa files from antivirus scanning resulted in all ZIP files being excluded from scanning.

115. The check for max password length when configuring users in the Local User Database displayed an incorrect message if the entered password exceeded the max supported length.

116. Certain SIP traffic could result in memory leaks when using the SIP ALG. [DRU20160729000001]

117. The CLI command to list current DNS queries printed incorrect addresses.

118. The 'blacklist' CLI command did not have a default action. Now, the

"show"argument is the default action.

119. An administrator using the default password could be locked out when changing the first configuration through the command line.

120. Some configurations made it impossible to set Local and Remote Networks on an IPsec tunnel with IKEv2.

121. IPsec tunnel setup failed with reason "out of memory".

122. SNMP trap sometimes reported an incorrect value for "ifOperStatus".

123. Sending IKE/ESP packets into another IPsec tunnel caused the packets to be dropped.

124. ZoneDefense switch verification did not work in NetDefendOS 11.04.01.

125. Assigning a static client IP to a user from the Local User Database did not work as intended.

126. IP Pool could not be used with IPsec interfaces and config mode.

127. Traceroute for IPv6 did not work as intended.

128. The DHCP Relay function could in some situations fail to relay DHCP messages.

129. Reconfiguring an IPsec interface that had an ongoing IKE SA negotiation could lead to unexpected behavior.

130. There was a memory leak when using HTTP ALG and NAT.

131. It was not possible to use more than 512 FQDN addresses.

132. LACP was not compatible with implementations that produce Protocol Data Units that are longer than the standard specification dictates they should be.

133. There was no warning printed when using an Email profile with Domain Verification and no DNS server was configured.

134. Adding a new authenticated user through the REST API with space or new line characters at the end of the group list would make the authentication fail.

135. There could be erroneous logs for 'out of memory' in rare occasions when antivirus was used.

136. There was a memory leak in the Whitelist/Blacklist feature of an Email Profile.

137. There was a memory leak in the SMTP, POP3 and IMAP ALGs.

138. Established connections were not closed when blacklisted by an IDP Rule Action or Threshold Action if the setting to only block connections with the same service was enabled.

139. Uploaded DER certificate could cause failure to activate IPsec

configuration.

140. The pre-configured time synchronization interval was too high. The interval has been changed from every week to every day.

141. The userauth REST API limits the num variable to max 9999. The max limit has been increased to 1000000000.

142. The firewall could make an unexpected restart under heavy traffic load. Affected models DFL-260E/860E.

143. The system could unexpectedly reboot during IPsec tunnel setup if a previously non-responding CA server used for CRL lookup started responding again.

144. Re-authenticating user using the REST API didn't update the "idle_timeout" property.

145. The SSH server only supported AES ciphers in CBC mode, not in CTR mode.

146. The "userauth -list" CLI command could cause traffic interruption when large amount of users were authenticated even though only a few were shown. The CLI command has been optimized to only process the users shown by the command.

147. Reconfiguring with an IPsec tunnel with tunnel monitoring enabled could lead to unexpected behavior.

148. CLI command "hostmon" with the flag "num" printed one session short of the number specified by the user.

149. If both peers of an IPsec tunnel initiated IKE SA setup at the same time, one endpoint could end up with duplicate IPsec and IKE SAs causing issues with traffic through the tunnel.

150. IPsec rekey could fail if the tunnel was configured as a config mode client and remote network was set to something other than all nets.

151. It was not possible to specify more than one interface when issuing the CLI's command "pcapdump".

152. Adding an Interface with a configured DHCP client to a Link Aggregation group could failed. Now the DHCP client is not initiated, instead the DHCP client must be configured on the Link Aggregation interface if DHCP should still be used.

153. The "Download Logs" button was shown for the logging pages in the WebUI for Microsoft Edge even though the browser does not support this feature.

154. Certain conditions where the DNS lookup had failed could cause an FQDN Address to stop being updated by the DNS cache.

155.   ZoneDefense log events were incorrectly generated at the start of the firewall.

156.   It was possible to use the same name for an IP Policy in multiple rule sets.

157.   Rekey could fail in scenarios with multiple networks set as LocalNetwork or Remote Network on an IPsec Tunnel. This caused packets to be dropped during the recreation of IPsec SAs.

158.   In certain cases email headers were not interpreted correctly and blacklisted IP addresses could be missed.

159.   Upgrading from releases before 11.04.00 could cause a reboot loop if the certificate did not contain a properly formatted private key. The system now disables an invalid certificate and its dependent objects instead of rejecting the configuration. The administrator then needs to upload the certificate again, in a proper format, to enable the object again.

160.   A system running OSPF sometimes restarted unexpectedly when doing a reconfiguration on an OSPF Neighbor.

161.   The diagnostic console page could return an error and was not able to show the logs.

162.   Traffic could halt if an IP Policy using an ALG positioned before the active IP Policy in the rule list was added, enabled, deleted or disabled.

163.   OSPF Interfaces over IPsec were tagged as down even if they were up.

164.   MAC address formatting was previously inconsistent across several features, some used uppercase while others used lowercase. Now all of them use uppercase.

165.   When downloading an empty log file the received file contained the source code of the web page and was simply named "Logs.txt". Now the file contains the text "Empty log" and is named with date and time in the same way as log files that contain log data.

166.   There was high CPU load when scanning some emails for viruses.

167.   The firewall could become unresponsive if an entry in the dynamic blacklist timed out after a reconfiguration.

168.   Log entries were generated on each load/save of the blacklist file during reconfigure.

169.   When performing antivirus inspection of emails transported with IMAP, some emails could make the mail connection stall.

170.   Using an IPsec tunnel to assign clients IP addresses taken from a RADIUS server could cause unexpected behavior if a RADIUS accounting server was used as well.

171. Traffic through NATed IPsec client could stop when the NAT changed port of the UDP encapsulated ESP packets. Affected models: DFL-2560, DFL-2560G.

172. There was a memory leak in the LW-HTTP ALG.

173. Packets going into PPPoE interfaces were not captured by the packet capture functionality.

174. The possibility to drop fragmented SYN packets and/or SYN packets carrying payload data was added. The default settings for these options are: drop and log.

175. Using the HTTP ALG for an HTTP persistent connection including 7-bit Transfer Encoding would process all the following messages using the same 7-bit Transfer Encoding.

176. The Application Control subsystem sometimes did not log application identification.

177. Some connections using routes as part of a Route Load Balancing setup were sometimes incorrectly closed at reconfigure.

178. In some cases infected URLs were blocked and HTTP connection was terminated before showing any information to the user.

179. When the firewall initiated an IPsec tunnel with XAuth, an incorrect authentication method was sent to the peer.

180. The Fail-Mode setting in File Control did not have anything to do with File Control and has been moved to the antivirus profile. Existing configurations are converted and will use the previously configured value.

181. An HA member could make an unexpected restart at reconfigure due to synchronization of ZoneDefense settings.

182. TCP traffic in certain scenarios together with Traffic Shaping could in rare occasions cause an unexpected system restart.

183. Some music streams using HTTP were dropped when used in combination with Web Content Filter or File Control.

184. IPv4 DHCP server replies were not sent if the interface the DHCP server was listening on was not in the <main> routing table.

185. The Out-of-buffers counter in a High Availability cluster was sometimes incorrectly incremented.

186. IPsec status button icons were missing in the WebUI.

187. When adding an intrusion detection rule in the WebUI and leaving out certain settings, the user was incorrectly transferred to the main status home page of the firewall.

188. The TLS ALG had an idle timeout of 30 seconds which caused timeout

problems for some applications. This has been increased to five minutes.

189. Some emails with invalid MIME formatting failed to pass through the IMAP content scanner.

190. In scenarios where the route to the DNS server was not available, the DNS subsystem would back off and not resolve FQDN Addresses after the first failed attempt.

191. Scheduled updates of antivirus sometimes failed or stopped progressing. The scheduling engine has been updated to better handle if updates take a long time.

192. Some Email Control features for IMAP did not work when used within a private network.

193. Some email messages with long, encoded subject headers could be corrupted when using IMAP content scanning.

194. The same Updatecenter WCF server was retried again after receiving a connection close instead of trying the next server in the list.

195. Pre-authentication for IMAP did not work as intended.

196. The HTTP header field 'Content-type' only supported 64 characters which made certain URLs inaccessible when using the HTTP ALG. It has been increased to support 256 characters.

197. Host Monitoring using HTTP did not correctly match the received data with the supplied Expected Response parameter.

198. In some rare scenarios the SSH server could cause an increase of memory usage and lead to unexpected system restart.

199. It was not possible to select a Link Aggregation interface as source interface for a PPPoE interface.

200. The light-weight HTTP ALG could in rare scenarios fail to send a proper block page when the accessed web page was blocked by policies.

201. The application count on the main page did not display the correct number.

202. The stateful NAT Pool might not use the least used IP for a new state in some scenarios.

203. The firewall did not correctly handle cases where an IMAP connection was closed unexpectedly by either side while in the middle of transferring data.

204. Emails with large attachments could in some rare cases not pass through the antivirus scanner.

205. Anti-spam tagging for POP3 did not work as intended in some rare cases.

206.   Some compressed emails attachments could lead to unexpected behavior.

207.   In some rare situations, the antivirus scanner failed to scan ZIP files.

208.   The tooltip for the Gateway and Local IP columns on the routing table data grid in the Web UI didn't work correctly.

209.   It was possible to enter RADIUS shared secrets longer than the supported 99 characters but only the first 99 characters were used. Now the length is checked on input and restricted to 128 characters.

210.   The firewall incorrectly altered the data of some UDP fragments when using multicast address translation.

211.   In some cases when Mail Alerting was configured, configuration warnings would not be displayed when activating a new configuration.

212.   The Local Console Idle Timeout setting was incorrectly named SSH Idle Timeout. The setting does only affect the serial console and not SSH Idle timeout.

213.   Some compressed files were not correctly scanned for viruses.

214.   When a URL "virus" was detected the advisory link in the memlog entry pointed to the wrong URL.

215.   It was previously possible to trigger the firewall to send atomic IPv6 fragments.

216.   When doing antivirus URL scans and hitting a cached URL, the HTTP_ALG logged the hit as a file instead of as a URL. This generated a faulty advisory link.

217.   Removing all IPsec tunnel interfaces in the configuration could cause the configuration deployment change to take about a minute to complete.

218.   If DHCPv6 Client was configured on more than one interface and any of the interfaces never got a lease the system would wait almost indefinitely before starting to use leases on the interfaces that were successful.

219.   The email control Malicious Link Protection feature was only able to handle HTTP links and not HTTPS links.

220.   The Web Content Filter Memlog printed that no Web Content Filter ALGs were logging even though log entries were printed.

221.   When using a config mode pool on an IPsec tunnel, an already allocated IP could be handed out to another client after a reconfigure.

222.   Some non-multipart messages were not correctly scanned by the IMAP content scanner.

223.   On High Availability clusters the CPU load increased when the sync

	cable was unplugged.
	224. The firewall could sometimes resend IKEv2 delete messages after a reconfiguration even though the peer responded to the message.
	225. A Certificate Revocation List (CRL) lookup failed if the gateway certificate didn't contain a CRL Distribution Point (CDP) but the Certification Authority (CA) certificate did.
	226. It was not possible to remove an IKE SA from the Web UI.
	227. The CLI command "script -create" would create a faulty script if the current configuration contained an unnamed Route object with a child Monitored Host object.
	228. Some spam emails were not correctly tagged when using IMAP.
	229. When having an IDP rule with a drop rule on the "Invalid hex encoding" setting, certain emails would not be let through depending on the segmentation of the TCP traffic.
	230. The IMAP content scanner incorrectly blocked some rare messages when a specific combination of File Control settings was configured.
	231. The spam counter for the IMAP ALG could count wrong if spam was detected using different methods for the same mail. The spam counter is only increased once for each detected spam mail.
	232. FQDN Groups were selectable on IP-, Goto-, Return- and Routing-Rules even though they were not supported.
	233. Detailed information on a ZoneDefense block entry did not sync correctly to the inactive node in an HA configuration.
	234. Application Control was only enforced on IPv6 TCP packages. Now it is possible to use Application Control for all types of IPv6 packages.
	235. IPsec tunnels using FQDN endpoints could be taken down unexpectedly if the DNS Cache got a response from the DNS server indicating an error even though there were valid IP addresses in the cache.
	236. Sending IPv6 packets through an IPsec tunnel with IPv4 endpoints or the other way around could cause the hardware accelerator on the DFL-2560 and DFL-2560G to drop packets.
	237. Using FQDN Address as SMTP Server on Mail Alerting did not work.
	238. Some rare emails with infected attachments could not pass through the firewall.
11.10.01	1. Packets going into PPPoE interfaces were not captured by the packet capture functionality.
	2. Using the HTTP ALG for an HTTP persistent connection including 7-bit Transfer Encoding would process all the following messages using the same

7-bit Transfer Encoding.

3. On rare occasions, an HA member could make an unexpected restart at reconfigure due to synchronization of ZoneDefense settings.

4. TCP traffic in certain scenarios together with Traffic Shaping could in rare occasions cause an unexpected system restart.

5. Some music streams using HTTP were dropped when used in combination with Web Content Filter or File Control.

6. IPv4 DHCP server replies were not sent if the interface was not in the main routing table.

7. The Out-of-buffers counter in a High Availability cluster was sometimes incorrectly incremented.

8. The TLS ALG had an idle timeout of 30 seconds which caused timeout problems for some applications. This has been increased to five minutes.

9. Hostmonitor could fail if the configuration contained a large number of Hostmonitor addresses routed through an IPsec interface on a firewall using IPsec hardware acceleration.
   Affected model: DFL-870.

10. Some emails with invalid MIME formatting failed to pass through the IMAP content scanner.

11. In scenarios where the route to the DNS server was not available, the DNS Cache would back off and not resolve FQDN Addresses after the first failed attempt.

12. Resent TCP SYN packets would in some scenarios be replied to with an ACK to signal a drop. This behavior was not correct and the erroneous ACK reply has been removed.

13. Some Email Control features for IMAP did not work when used within a private network.

14. The same Updatecenter WCF server was retried again after receiving a connection close instead of trying the next server in the list.

15. Pre-authentication for IMAP did not work as intended.

16. An IPsec SA without an IKE SA was not removed when receiving Initial_Contact notification.

17. The HTTP header field 'Content-type' only supported 64 characters which made certain URLs inaccessible when using the HTTP ALG. It has been increased to support 256 characters.

18. HostMonitoring using HTTP did not correctly match the received data with the supplied ExpectedResponse parameter.

19. In some rare scenarios the SSH server could cause an increase of memory

usage and lead to unexpected system restart.

20. It was not possible to select a Link Aggregation interface as source interface for a PPPoE interface.

21. The light-weight HTTP ALG could in rare scenarios fail to send a proper block page when the accessed web page was blocked by policies.

22. The application count on the main page did not display the correct number.

23. The stateful NAT Pool might not use the least used IP for a new state in some scenarios.

24. The firewall did not correctly handle cases where an IMAP connection was closed unexpectedly by either side while in the middle of transferring data.

25. Emails with large attachments could in some rare cases not pass through the anti-virus scanner.

26. Anti-spam tagging for POP3 did not work as intended in some rare cases.

27. Some compressed emails attachments could lead to unexpected behavior.

28. In some rare situations, the Anti-Virus scanner failed to scan ZIP files.

29. The firewall incorrectly altered the data of some UDP fragments when using multicast address translation. [DRU20160923000001]

30. Some compressed files were not correctly scanned for viruses.

31. It was previously possible to trigger the firewall to send atomic IPv6 fragments.

32. Removing all IPsec tunnel interfaces in the configuration could cause the reconfiguration to take about a minute to complete.

33. Some non-multipart messages were not correctly scanned by the IMAP content scanner.

34. Some spam emails were not correctly tagged when using IMAP.

35. The spam counter for the IMAP ALG could count wrong if spam was detected using different methods for the same mail. The spam counter is only increased once for each detected spam mail.

36. The DHCPRelaySettings MaxAutoRoutes has been renamed to MaxConcurrentRelays to make the function of the setting clearer.

37. When receiving an LDAP reply, only the 256 first characters of the user groups in the memberOf attribute were used.

38. When hovering over an address group in the WebUI, like the system whitelist, the addresses of the individual address objects were not presented in a tool-tip.

39. A transport mode IPsec tunnel, configured with a remote endpoint of type IP range or network, failed to negotiate against peers behind a NAT.

40. If ARP Monitoring was used on Route Failover and then later disabled, the

system continued sending ARP monitoring queries until the system was restarted.

41. Configuring host monitoring could under rare conditions cause configuration errors. Also, in certain rare conditions where HTTP was used for host monitoring and the HTTP response was fragmented, the system might fail in matching a correct response.

42. If traffic stopped going through an IPsec tunnel, for whatever reason, the tunnel monitoring feature and the "ike -delete" CLI command failed to delete some IPsec SAs that didn't belong to an IKE SA. (IKEv1 only).

43. Some methods of downloading email data using IMAP did not work as intended.

44. It was not possible to detect invalid FQDN addresses before attempting to save & activate the new configuration.

45. The SYN Relay feature did not correctly restore TCP headers inside of ICMPv6 Error Packet Too Big messages when the packet was forwarded.

46. Using the blacklist command to block an IP for zero seconds would result in a negative value in the blacklist listing, also the host would be blocked until the next reconfiguration event. It's no longer possible to block an IP for zero seconds when configuring blacklist.

47. Brute force history was lost after reconfiguration.

48. Certificates could not be successfully downloaded using scp.

49. POP3 message transactions did not complete successfully in some cases.

50. The user privileges were truncated if more than 255 characters long when output in the CLI.

51. Some emails with incorrect MIME formatting were not forwarded correctly.

52. On rare occasions there was an unexpected reboot with certain IPsec traffic.

53. The firewall did not allow multiple logins originating from the same interface and IP into the SSL VPN Portal when using RADIUS as Authentication Source and the User Authentication Rule was using the option "Allow multiple logins per username".

54. In rare cases, email attachments containing viruses were not detected by the POP3 ALG.

55. Some log events were missing for the Authentication Agent and the REST API users.

56. The WebUI was missing some Anti-Virus settings when using IP Policies.

57. TCP packets inside ICMP and ICMPv6 errors could in some scenarios contain faulty SEQ and ACK numbers.

58. Emails containing empty MIME body parts could in some cases not pass through the POP3 content scanner.

59. In some scenarios when the HTTP ALG was used on IPv6 traffic, path MTU discovery did not work.

60. In rare cases, email attachments containing viruses were not detected by the SMTP ALG.

61. The output of the "routemon" CLI command was misaligned.

62. In rare occasions, the POP3 ALG made mail fetching time out.

63. On rare occasions, the firewall could make an unexpected reboot when using the HTTP ALG.

64. Emails with abnormally large epilogues, usually corrupted, failed to pass through the IMAP content scanner.

65. Some emails with message attachments were not forwarded correctly by the IMAP content scanner.

66. The individual NATPool CLI overview could show the wrong number of flows associated with it.

67. The stateful NATPool didn't correctly restrict the number of states according to the configured maximum limit.

68. The POP3 content scanner could not handle messages that violate the requirement that lines beginning with a terminating octet be "byte-stuffed", as specified in RFC 1939.

69. The schedule feature did not trigger even though it was configured.

70. When using the Basic authentication option for authenticating users via the web portal, the correct post-login page was not displayed after logging in.

71. Certain types of faulty ESP packets could cause undefined behavior on platforms using a hardware accelerator for IPsec encryption/decryption. Affected models: DFL-260E and DFL-860E.

72. IMAP scanning could lead to unintended behavior if not all data was available.

73. Some email headers could not be downloaded using the IMAP ALG.

74. After a reconfiguration, some of the states in a stateful NAT Pool would be stuck and could not be removed when the connections timed out.

75. Emails containing empty MIME body parts could in some cases not pass through the POP3 content scanner.

76. It was not possible to configure a SAT policy to single IP policy because of a missing UI element.

77. It was not possible for Update center to remove an invalid IDP signature database.

	78. Log messages for ESP packets that failed to decrypt could generate logs with the wrong reason for the failure. 79. In rare occasions there could be an unexpected restart for traffic going through the SIP ALG. 80. Certain rare emails were not interpreted correctly by the POP3 content scanner, which could cause detection errors. 81. The POP3 content scanner failed to detect threats in the last body part of a message if an explicit Content-Type header field was missing. 82. The firewall generated invalid DNS queries in some rare cases. 83. A warning about an unknown setting was erroneously shown when configuring ZoneDefense. 84. The HTTP Poster did not auto update the IP address properly. 85. Scheduled updates of Anti-Virus sometimes failed or stopped progressing. The scheduling engine has been re-written to better handle if updates takes a long time. 86. In some scenarios involving 6in4 tunnels, PacketTooBig was not sent when the system received packets with a size over the configured MTU. 87. Some email messages with long, encoded subject headers could be corrupted when using IMAP content scanning. 88. In some cases when Mail Alerting was configured, configuration warnings would not be displayed when activating a new configuration. 89. Routes, added when a user in a local user database logs in, could become corrupted or not added at all after a reconfigure of the system. [DRU20170120000002]
11.04.01	1. There was no clear error message displayed when the user tried to configure PPPoE on an HA cluster. Since this is not supported the user now gets this information when trying to save this invalid configuration. 2. The index column for DataGrids in the Web UI could display max 999 items and has now been changed to allow five digit numbers. 3. The firewall did not verify Identification field uniqueness when stripping the Don't Fragment flag from IPv4 headers. This could cause reassembly problems for other nodes. Any zero-value Identification field is now replaced with a suitable value, when the Don't Fragment flag is stripped. 4. IPsec performance sometimes degraded over time. Affected models: DFL-260E and DFL-860E. 5. Some configurations involving the PPTP ALG could cause the firewall to make an unexpected restart. 6. The application control engine could not completely block Google Drive,

when an application rule set was configured to do so.

7. On rare occasions there was an unexpected restart with certain IPsec traffic.

8. Connection timeouts created from service objects with custom timeout values were not properly synchronized between High Availability cluster peers.

9. The packet buffers managing IPsec traffic were not optimized.

10. The HTTP ALG used underscores to replace unsupported keywords in the "Accept-Encoding" header which could make strict web servers fail the request. Now the whole keyword is replaced with spaces to ensure the header is correct.

11. Download of certain files failed when using the HTTP ALG configured to do Anti-Virus scanning.

12. Email Control blacklist and whitelist filters did in some cases not match correctly.

13. The OSPF subsystem in a High Availability setup sometimes caused the system to restart unexpectedly.

14. The firewall sent UDP encapsulation mode in the IPsec proposal even when NAT-Traversal on the IPsec tunnel was set to OFF.

15. When receiving traffic through the IMAP ALG, the system sometimes rebooted unexpectedly.

16. It was possible to use snoop commands when logged in with a user with auditor access. Now they are only available when logged with a user that has as administrator access permissions.

17. "Malformed Request" error page generated by the HTTP ALG would also contain the error page for "Reclassification Request Failed".

18. Some email content was incorrectly blocked when using the POP3 ALG.

19. Inspecting non-standard e-mail sometimes caused the firewall to make an unexpected restart.

20. Protocols using UDP may be vulnerable to being used in a DDoS attack to amplify the effect of the attack. Implementations of IKE, both IKEv1 and IKEv2, have been shown to be vulnerable (see http://www.kb.cert.org/vuls/id/419128 for more info). An implementation following the IKEv2 specification (RFC 7296) isn't subject for the vulnerability and NetDefendOS is following the RFC making it impossible to be used in an amplification attack when using IKEv2 tunnels. NetDefendOS also follows the specification for IKEv1 (RFC 2408) which makes it vulnerable to the attack. Changes have been made to NetDefendOS that

will break RFC compliance to mitigate the risk of being used in an amplification attack. NetDefendOS will no longer resend responses to the first IKE message of a Main mode exchange. This is similar to how the IKEv2 implementation works and will not cause issues with retransmissions. Aggressive mode tunnels will still be vulnerable though, since changes to this exchange can't be made to both protect against the attack and still have a functional retransmission process. The recommendation is therefore to not use aggressive mode tunnels in a roaming scenario. I.e. where LocalEndpoint attribute on the tunnel hasn't been set. Using aggressive mode in this configuration would still make the firewall subject for the attack.

21. Some email messages with nested multiparts were corrupted when using POP3 or SMTP content inspection.

22. Tab completion for the Ping CLI command did not work correctly.

23. The system could restart unexpectedly when removing all IPsec connections with the "killsa" CLI command.

24. Under certain rare circumstances it was not possible to download a backup of the working configuration from the firewall.

25. The HA log messages with ID 616, 617 and 618 used the wrong syntax for describing the event.

26. The SMTP ALG sometimes incorrectly marked mail sent with the Outlook Mail client as spam.

27. The system did not terminate the previous PPPoE session when PPPoE settings were changed.

28. Disabling the usage of legacy IPRules would also disable Threshold, Pipe, IDP and Routing rules.

29. Disabling usage of legacy IPRules would not disable IPRules in IPRuleSets.

30. IPsec tunnel setup rate was slow and caused high CPU load in certain large setups that contained a large number of IPsec tunnels.

31. Some packets generated by the firewall could get an erroneous hardware address when routed through a switch route.

32. An Anti-Virus signature update interrupted by a reconfiguration needed a manual update to resume the download after the unit finished configuring.

33. Upgrading from versions prior to 11.00 to 11.00 and later versions, could in rare occasions fail with a configuration error.

34. On rare occasions the firewall could restart unexpectedly when errors occurred in the connection with the SSL VPN client.

35. When using Anti-Virus scanning on IMAP traffic, emails with deeply nested

and/or encrypted zip attachments were not forwarded correctly.

36. Some VoIP scenarios did not work as intended when using IP Policies and VoIP Profiles.

37. Connection failures when updating the Anti-Virus databases implied a restart of the whole updating process.

38. Cloning a read-only object in the WebUI did not copy any values from the original object.

39. The clone function did not support cloning certain objects and has been updated to support a wider range of objects to clone in the WebUI.

40. The system did not respond to Dead Peer Detection messages in some cases when the IKE Security Association was about to expire.

41. It was not possible to upload a configuration backup using Safari as web browser.

42. Running the ping CLI command with certain parameters could make the firewall perform an unexpected restart.

43. The "%URL%" variable was not correctly substituted in some built in HTTP banner files.

44. The checksum for TCP packets in IPsec transport mode were incorrect when using SAT rules and caused traffic to be dropped in certain scenarios. Affected models: DFL-2560 and DFL-2560G.

45. POP3 connections could become unresponsive in rare cases.

46. The NATPool subsystem did not use the full configured IP-range.

47. DHCP Server didn't use the configured Relayer Filter to filter the received DHCPREQUEST messages when a client tried to obtain a previously allocated IP address.

48. In certain scenarios IP addresses could remain in the DNS Cache after the Life Time had been passed.

49. When authenticating users, the group membership list was limited to 255 characters which could lead to missing user privileges.

50. The HTTP ALG did not accept a missing version number in the SSL server certificate. A missing version number is now interpreted as version 1.

51. Dead Peer Detection for IPsec tunnels using XAuth was in rare occasions not initiated.

52. Using FQDN objects in rule sets other than the Main rule set could lead to duplicate log events with corrupted information when IP addresses were removed and added to the FQDN object.

53. Under special circumstances the firewall reported the wrong number of Anti-Virus signatures loaded in memory.

54. The command "ike -show -tunnel=<tunnel_name>" didn't filter the output correctly if an IKE SA had made an IKE rekey during its lifetime.

55. Some non-standard IMAP extensions were not supported.

56. The default allowed server port range for IP policies using FTP was incorrectly set to 0-65535. The default value is now set to 1024-65535.

57. POP3 message transactions did not complete successfully in some cases.

58. Plain text email attachments were not scanned for viruses when using IMAP.

59. When hovering over an address group in the WebUI, like the system whitelist, the addresses of the individual address objects were not presented in a tool-tip.

60. A transport mode IPsec tunnel, configured with a remote endpoint of type IP range or network, failed to negotiate against peers behind a NAT.

61. The system did not disable route failover ARP monitoring when manual ARP lookup interval was specified even though ARP monitoring was disabled in the configuration.

62. Configuring host monitoring could under rare conditions cause configuration errors. Also, in certain rare conditions where HTTP was used for host monitoring and the HTTP response was fragmented, the system might fail in matching a correct response.

63. If traffic stopped going through an IPsec tunnel, for whatever reason, the tunnel monitoring feature and the "ike -delete" CLI command failed to delete some IPsec SAs that didn't belong to an IKE SA. (IKEv1 only).

64. ESP traffic was sometimes incorrectly routed into the IPsec tunnel.

65. Some methods of downloading E-Mail data using IMAP did not work as intended.

66. Anti-Virus scanning for the SMTP and HTTP ALGs sometimes caused the system to lose memory over time.

67. It was not possible to detect invalid FQDN addresses before activation.

68. Using the blacklist command to block an IP for zero seconds would result in a negative value in the blacklist listing, also the host would be blocked until the next reconfiguration event. It's no longer possible to block an IP for zero seconds when configuring blacklist.

69. Brute force history was lost after reconfiguration.

70. Certificates could not be successfully downloaded using scp.

71. Some E-Mails with incorrect MIME formatting were not forwarded correctly.

72. The firewall did not allow multiple logins originating from the same interface and IP into the SSL VPN Portal when using RADIUS as

Authentication Source and the User Authentication SSL VPN Rule allowing multiple log in.

73. Some log events were missing for the Authentication Agent and the REST API users.

74. The WebUI was missing some Anti-Virus settings for an IP Policy.

75. TCP packets inside of certain ICMP and ICMPv6 errors could in some scenarios contain faulty SEQ and ACK numbers.

76. E-Mails containing empty MIME body parts could in some cases not pass through the POP3 content scanner.

77. In some scenarios when the HTTP ALG was used on IPv6 traffic, path MTU discovery did not work.

78. There was a column miss alignment in the output of the CLI command "routemon".

79. In rare occasions, the POP3 ALG made mail fetching time out.

80. E-Mails could not be sent through the IMAP ALG for some E-Mail clients that were set to save a copy of the mail in the sent folder.

81. On rare occasions, the firewall could make an unexpected reboot when using the HTTP ALG.

82. Some E-Mails with message attachments were not forwarded correctly by the IMAP content scanner.

83. The firewall could make an unexpected restart with certain configurations containing a Policy Based Routing rule.

84. Some rare E-Mail messages were not forwarded correctly by the POP3 content scanner.

85. The individual NAT Pool CLI overview could show the wrong number of flows associated with it.

86. The stateful NAT Pool didn't correctly restrict the number of states according to the configured maximum limit.

87. The POP3 content scanner could not handle messages that violate the requirement that lines beginning with a terminating octet be "byte-stuffed", as specified in RFC 1939.

88. The schedule feature was never applied in NetDefendOS 11.04.00 even though it was configured.

89. When using the Basic authentication option for authenticating users via the web portal, the correct post-login page was not displayed after logging in.

90. The remote management SSH session could get interrupted during reconfigure when the primary authentication source was RADIUS.

91. Certain types of faulty ESP packets could cause undefined behavior on

platforms using a hardware accelerator for IPsec encryption/decryption.

92. IMAP scanning could lead to unintended behavior if not all data was available.

93. Some E-Mail headers could not be downloaded using the IMAP ALG.

94. After a reconfiguration, some of the states in a stateful NAT Pool will be stuck and cannot be removed when the connections time out.

95. E-Mails containing empty MIME body parts could in some cases not pass through the POP3 content scanner.

96. It was not possible to configure a SAT policy to single IP policy because of a missing UI element.

97. Update center did not remove a corrupted IDP signature database.

98. Log messages for ESP packets that failed to decrypt could generate logs with the wrong reason for the failure.

99. In rare occasions there could be an unexpected restart for traffic going through the SIP ALG.

100. Certain rare E-Mails were not interpreted correctly by the POP3 content scanner, which could cause detection errors.

101. The POP3 content scanner failed to detect threats in the last body part of a message if an explicit Content-Type header field was missing.

102. The firewall generated invalid DNS queries in some rare cases.

103. The system could in case of high buffer usage, reboot unexpectedly when using features dependent on the pseudo-reassembler e.g. IDP, Anti-Virus, Web Content Filtering.

104. The HTTP Poster did not auto update the IP address properly.

105. The HTTP ALG configured with Anti-Virus scanning failed to properly scan for viruses if the connected web server used content compression. The Anti-Virus engine could either incorrectly indicate that files were infected or that they were clean even though they in fact were infected.

106. The update center subsystem could fail to retrieve a fresh list of CSPN servers if a reconfigure was made within 24h from system boot.

107. In some scenarios involving 6in4 tunnels PacketTooBig was not sent when the system received packets with a size over the configured MTU.

108. There was no clear error message displayed when the user tried to configure PPPoE on an HA cluster. Since this is not supported the user now gets this information when trying to save this invalid configuration.

109. There was no clear error message displayed when the user tried to configure PPPoE on an HA cluster. Since this is not supported the user now gets this information when trying to save this invalid configuration.

110. The firewall did not verify Identification field uniqueness when stripping the Don't Fragment flag from IPv4 headers. This could cause reassembly problems for other nodes. Any zero-value Identification field is now replaced with a suitable value, when the Don't Fragment flag is stripped.

111. IPsec performance sometimes degraded over time. Affected models: DFL-260E and DFL-860E.

112. Some configurations involving the PPTP ALG could cause the firewall to make an unexpected restart.

113. The application control engine could not completely block Google Drive, when an application rule set was configured to do so.

114. On rare occasions there was an unexpected restart with certain IPsec traffic.

115. Connection timeouts created from service objects with custom timeout values were not properly synchronized between High Availability cluster peers.

116. The packet buffers managing IPsec traffic were not optimized.

117. The "dhcprelay" CLI command listed an infinite number of entries. The command has been updated to list 20 entries by default with the option -num to show more if needed.

118. The HTTP ALG used underscores to replace unsupported keywords in the "Accept-Encoding" header which could make strict web servers fail the request. Now the whole keyword is replaced with spaces to ensure the header is correct.

119. Download of certain files failed when using the HTTP ALG configured to do Anti-Virus scanning.

120. Email Control blacklist and whitelist filters did in some cases not match correctly.

121. Under certain conditions the IMAP ALG could cause an unexpected restart of the firewall.

122. The OSPF subsystem in a High Availability setup sometimes caused the system to restart unexpectedly.

123. The firewall sent UDP encapsulation mode in the IPsec proposal even when NAT-Traversal on the IPsec tunnel was set to OFF.

124. When receiving traffic through the IMAP ALG, the system sometimes rebooted unexpectedly.

125. It was possible to use snoop commands when logged in with a user with auditor access. Now they are only available when logged with a user that has as administrator access permissions.

126. Import/export and validation of certificates has been improved to work in a more consistent way. Certificates and private keys are now exported as a PEM encoded file with the crt/key-file extension. Certificates can be imported if they are PEM or DER encoded.

127. "Malformed Request" error page generated by the HTTP ALG would also contain the error page for "Reclassification Request Failed".

128. Some email content was incorrectly blocked when using the POP3 ALG.

129. The setup wizard had an invalid redirection URL under time settings to set date time page. It is removed and now it is possible to set date and time within the same setup wizard page.

130. Inspecting non-standard e-mail sometimes caused the firewall to make an unexpected restart.

131. Protocols using UDP may be vulnerable to being used in a DDoS attack to amplify the effect of the attack. Implementations of IKE, both IKEv1 and IKEv2, have been shown to be vulnerable (see http://www.kb.cert.org/vuls/id/419128 for more info). An implementation following the IKEv2 specification (RFC 7296) isn't subject for the vulnerability and NetDefendOS is following the RFC making it impossible to be used in an amplification attack when using IKEv2 tunnels. NetDefendOS also follows the specification for IKEv1 (RFC 2408) which makes it vulnerable to the attack. Changes have been made to NetDefendOS that will break RFC compliance to mitigate the risk of being used in an amplification attack. NetDefendOS will no longer resend responses to the first IKE message of a Main mode exchange. This is similar to how the IKEv2 implementation works and will not cause issues with retransmissions. Aggressive mode tunnels will still be vulnerable though, since changes to this exchange can't be made to both protect against the attack and still have a functional retransmission process. The recommendation is therefore to not use aggressive mode tunnels in a roaming scenario. I.e. where LocalEndpoint attribute on the tunnel hasn't been set. Using aggressive mode in this configuration would still make the firewall subject for the attack.

132. Some email messages with nested multiparts were corrupted when using POP3 or SMTP content inspection.

133. Tab completion for the Ping CLI command did not work correctly.

134. In some scenarios with an external route configured through a PPPoE tunnel Anti-Virus databases would never get automatically updated after the tunnel acquired its IP.

135. The system could restart unexpectedly when removing all IPsec connections with the "killsa" CLI command.

136. Under certain rare circumstances it was not possible to download a backup of the working configuration from the firewall.

137. The HA log messages with ID 616, 617 and 618 used the wrong syntax for describing the event.

138. The SMTP ALG sometimes incorrectly marked mail sent with the Outlook Mail client as spam.

139. The system did not terminate the previous PPPoE session when PPPoE settings were changed.

140. Disabling the usage of legacy IPRules would also disable Threshold, Pipe, IDP and Routing rules.

141. Disabling usage of legacy IPRules would not disable IPRules in IPRuleSets.

142. IPsec tunnel setup rate was slow and caused high CPU load in certain large setups that contained a large number of IPsec tunnels.

143. Some packets generated by the firewall could get an erroneous hardware address when routed through a switch route.

144. An Anti-Virus signature update interrupted by a reconfiguration needed a manual update to resume the download after the unit finished configuring.

145. Upgrading from versions prior to 11.00 to 11.00 and later versions, could in rare occasions fail with a configuration error.

146. On rare occasions the firewall could restart unexpectedly when errors occurred in the connection with the SSL VPN client.

147. When using Anti-Virus scanning on IMAP traffic, emails with deeply nested and/or encrypted zip attachments were not forwarded correctly.

148. Some VoIP scenarios did not work as intended when using IP Policies and VoIP Profiles.

149. Connection failures when updating the Anti-Virus databases implied a restart of the whole updating process.

150. Cloning a read-only object in the WebUI did not copy any values from the original object.

151. The clone function did not support cloning certain objects and has been updated to support a wider range of objects to clone in the WebUI.

152. The system did not respond to Dead Peer Detection messages in some cases when the IKE Security Association was about to expire.

153. It was not possible to upload a configuration backup using Safari as web browser.

	154. Running the ping CLI command with certain parameters could make the firewall perform an unexpected restart.
	155. The "%URL%" variable was not correctly substituted in some built in HTTP banner files.
	156. The checksum for TCP packets in IPsec transport mode were incorrect when using SAT rules and caused traffic to be dropped in certain scenarios. Affected models: DFL-2560 and DFL-2560G.
	157. POP3 connections could become unresponsive in rare cases.
	158. The NATPool subsystem did not use the full configured IP-range.
	159. DHCP Server didn't use the configured Relayer Filter to filter the received DHCPREQUEST messages when a client tried to obtain a previously allocated IP address.
	160. In certain scenarios IP addresses could remain in the DNS Cache after the Life Time had been passed.
	161. When authenticating users, the group membership list was limited to 255 characters which could lead to missing user privileges.
	162. The HTTP ALG did not accept a missing version number in the SSL server certificate. A missing version number is now interpreted as version 1.
	163. Dead Peer Detection for IPsec tunnels using XAuth was in rare occasions not initiated.
	164. Using FQDN objects in rule sets other than the Main rule set could lead to duplicate log events with corrupted information when IP addresses were removed and added to the FQDN object.
	165. The HTTP ALG didn't handle certain non-success HTTP codes correctly which would prevent traffic to pass through.
	166. Under special circumstances the firewall reported the wrong number of Anti-Virus signatures loaded in memory.
	167. The SYN Relay feature did not correctly restore TCP headers inside of ICMPv6 Error Packet Too Big messages when the packet was forwarded.
	168. The command "ike -show -tunnel=<tunnel_name>" didn't filter the output correctly if an IKE SA had made an IKE rekey during its lifetime.
	169. Some non-standard IMAP extensions were not supported.
	170. The default allowed server port range for IP policies using FTP was incorrectly set to 0-65535. The default value is now set to 1024-65535.
	171. POP3 message transactions did not complete successfully in some cases.
10.22.01	1. The options "ValidateLogBad", "ValidateReopen", "ValidReopenLog", "ReopenValidate" and "ReopenValidLog" for the setting TCPSequenceNumbers did not work and the system behaved as if configured with "ValidateLogBad".

2. The system would sometimes log that a packet had invalid TCP sequence number and would be dropped, despite the fact that packets were allowed to reopen the connection and should be forwarded.

3. In rare occasions when using the PPTP ALG an incorrect ALG associated connection could be closed, resulting in unexpected behavior.

4. OSPF "point-to-multipoint" interfaces didn't allow for more than one neighbor to be configured.

5. OSPF "point-to-multipoint" interfaces discovered neighbors using multicast instead of unicast.

6. OSPF "point-to-multipoint" interfaces created an invalid "dummy" route for the interface IP.

7. An Ethernet interface with a manually assigned MAC address would revert to its original MAC address after issuing the console command "ifstat -restart".

8. The firewall might show unexpected behavior when restarting after changes in configuration if an SSL VPN interface using a specific Routing Table was already configured.

9. The NetDefendOS web authentication feature could fail in some rare situations when the system was under heavy stress.

10. The firewall's SNMP statistics could report active IPsec tunnels as "down" under certain circumstances.

11. It was not possible to use Interface Groups as the OuterInterface when configuring an SSL VPN interface.

12. The H.323 ALG sometimes caused unexpected reboots.

13. It was not possible to use the CLI command "ippool -renew" to renew leases.

14. An error message is now displayed when trying to save a certificate with the same name as an existing object.

15. The E-flag in OSPF could in certain scenarios be set incorrectly which resulted in connectivity problems.

16. A large number of applications that were previously unsupported have been added to Application Control feature.

17. Dead Peer Detection for IPsec interfaces didn't work against some remote clients.

18. The firewall could in rare occasions reboot unexpectedly if Anti-Virus scanning was configured.

19. The message shown when trying to log in with a user with insufficient privileges was not descriptive enough.

20. The Advanced TCP Setting for CC (Connection Count) option was

incorrectly named

"TCP Option Connection Timeout" in the WebUI.

21. The firewall could generate TCP packets with incorrect checksum on connections using address translation and some content inspection feature, such as, Application Control or Anti-Virus. In rare cases this could lead to stalled TCP connections.

22. The configuration warning message "Shared IP address cannot be equal to iface IP address" was missing the name of the offending interface.

23. Non pertinent information was displayed in the console command "appcontrol -show_lists".

24. Using some layer 7 features, such as, Application Control or Anti Virus, would prevent ICMP errors from being forwarded even when the service was configured to allow ICMP errors.

25. When using the "IPsecBeforeRules" or "L2TPBeforeRules" settings, i.e. bypassing rules, this registered as a default-rule in syslogs for IPsec and L2TP. Now it the correct specific rule is logged, for both categories respectively.

26. Comments were not visible on folders in the WebUI address book.

27. DHCP Relay did not forward DHCPACK messages if they were received on port 68.

28. Some scenarios with static route insertion/removal through OSPF did not work in a High Availability setup.

29. Values for advanced IPsec settings "DPDExpireTime" and "DPDKeepTime" were missing from the WebUI and could only be changed using the CLI.

30. Some HTTP operations could under certain situations result in second long lockups.

31. NAT-T Vendor ID was sent even when NAT-T setting on IPsec tunnel was set to OFF.

32. The firewall could in rare occasions reboot unexpectedly when checking IPsec connections during a reconfiguration.

33. DHCP Server configured with "Relayer Filter" erroneously dropped the unicast DHCP request/renewal messages from DHCP clients.

34. The firewall failed to match an HTTP Monitoring response when it was used in SLB and the "expected response" value given by the user contained special characters like spaces, tabs,line feeds, carriage returns.

35. TCP segments with RST flag did not have 0x00000000 as acknowledge number.

36. Interoperability issues regarding NAT-T sometimes caused IPsec traffic to be incorrectly dropped.

37. After receiving large LSA, the OSPF module reported memory error despite having enough available memory to use.

38. Some log messages did not correctly display the access_level for some users.

39. Unsupported ISAKMP and IPsec Security Association Attributes received during IPsec tunnel setup resulted in a failed setup even if configured attributes also were sent.

40. Some rare URLs were incorrectly forbidden by the Web Content Filtering (WCF) functionality.

41. The H323 ALG could in rare occasions cause a system reboot.

42. ICMPv6 error message "Packet too big" was not passed through NetDefendOS causing traffic to be blocked in certain scenarios.

43. In rare occasions, the firewall's 'sysmsgs' console command could report "FAT chain inconsistence" for its internal media, for instance when using Anti-Virus.

44. Modern browsers were not correctly identified in the Web User Interface causing a message to be displayed that an unsupported browser version was being used.

45. The wrong IPsec Authentication Algorithm (SHA) was sometimes added to an IPsec tunnel configuration if it was set in the same tunnel's IKE Algorithms, i.e if for instance SHA1 was configured in the IKE Algorithm it would also be automatically added to the IPsec Algorithm.

46. In certain scenarios, the number of "Active flows" reported by the 'ipsecglobalstats' CLI command always reached the maximum value even for connections with short lifetime.

47. There were no warnings about changed IPRules or IPPolicies due to configuration changes.

48. ZoneDefense did not log the unblocking events.

49. The firewall sent IPsec "initial contact" notification when rekeying an IPsec SA without an existing IKE SA. This could case the responder to first delete the IPsec SA before the rekey request was processed and lead to interruptions in traffic going through the tunnel since whole new IKE and IPsec SA could be established as a result instead of a rekey.

50. The span for the Update Center's Hourly setting was not correct and has been changed from 11 to 12 hours.

51. When using the "Hourly" interval for Update Center the updates ran every hour despite the setting's value.

52. The blacklist -show command displayed all blacklisted and whitelisted

hosts. It has been updated to display a default of 20 blacklisted and whitelisted hosts, or the specified number of hosts using the -num argument.

53. The NAT-pool IP range setting used to accept very wide ranges (> 65535) of IPv4 addresses if such an address started at 0.0.0.0.

54. Spaces in passwords were incorrectly interpreted as '+'-signs when using Web Authentication.

55. An incorrect date was displayed in the Update Center section of the management WebUI when an Anti-Virus or IDP database was deleted manually.

56. The pcapdump -show command displayed all the captured packets. Now the pcapdump -show command displays a default of 20 packets, or the specified number of packets using the -num argument.

57. Using certain addresses as IPv6AddressPool in the DHCPv6 Server caused the system to not give out any IP addresses.

58. IPsec tunnel setup could fail with certain configurations despite matching IPsec proposals.

59. The system sometimes experienced high memory consumption and sometimes rebooted due to low available memory when using IDP.

60. The Anti-Virus log message ID 115 and Application Control log message ID 4 had swapped the event and the action. The log revisions have been updated for both messages.

61. There was no log or notification shown when IDP scanning was disabled because of the license expiration.

62. Received ICMPv6/Neighbor Advertisements containing multiple options were incorrectly interpreted by the firewall.

63. L2TP/IPsec traffic to multiple clients behind the same NAT device could in rare scenarios be mixed up.

64. Full system backup files did not include files related to SSL VPN and Application Control.

65. Connecting a second L2TP Client located behind a NAT gateway could in rare occasions disconnect the first client.

66. In rare occasions, the SMTP and POP3 ALG configured with Anti-Virus did not detect malicious email attachments.

67. In rare High Availability scenarios a restart of the nodes would be necessary in order to finish configuration synchronization.

68. Configured IDP pipes were not always displayed in the CLI.

69. Blacklist logs sometimes showed incorrect protocol or port.

70. Memory usage for SIP was displayed incorrectly.

	71. A DHCP server lease was not removed from the inactive HA node when the CLI command "dhcpserver -releaseip" was issued on the active node.
	72. The system could unexpectedly restart if a service's ALG type changed from e.g. FTP to HTTP while having active connections.
10.21.02	1. Source Address Translation 'Auto' would not result in correct behavior when configuring IPPolicies.
	2. Fragmented traffic sent through an IPsec tunnel was sometimes dropped.
	3. No error was generated when configuring HTTPS management without selecting an HTTPS certificate.
	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.
	5. IPsec interfaces could not be used by OSPF to communicate with a neighbor.
	6. Connections using the secondary route in a route monitor setup where the primary route had failed were incorrectly closed during reconfiguration.
	7. A firewall with User Identity Awareness configured could in rare scenarios reboot unexpectedly.
	8. Memory consumption could in rare circumstances increase when an authenticated user timed out from a RADIUS server.
	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.
	10. The Web User Interface selection box was not wide enough, which made long object names not being displayed in full.
	11. Error messages output by the "time -sync" command were in some failure cases not informative enough to describe the problem.
	12. On rare occasions, the firewall could perform an unexpected restart after reconfiguring a PPTP server that used LDAP authentication.
	13. Configuring an IPv6 core route would always cause a configuration warning.
	14. Traffic passing through an IPsec tunnel was sometimes incorrectly dropped if there was fragmentation of the packets.
	15. Valid UTF-8 characters were in some logs not shown properly.
	16. UDP packets sent from the firewall when using the ping CLI command always had the same Fragmentation ID or Identification field set.
	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.
	18. The description of the Facility parameter in the Syslog Receiver configuration object was incorrect.
	19. The device could restart unexpectedly when Application Control was disabled on an IPRule matching active IPv6 traffic
	20. Certain rare certificates could not be added to the configuration.
	21. Web Content Filtering did not work for HTTPS when the traffic was directed to a proxy.
	22. Descriptions were missing for some advanced settings alternatives.
	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.
	24. Application Control frequently failed to recognize Skype. Changes have been made to improve the classification of Skype.
	25. Application Control sometimes identified the application as just TCP or just UDP.
	26. Using an IP4Address object with a DNS name as Remote Endpoint for an IPsec tunnel could lead to IPsec traffic problems.
	27. In rare occasions, some applications, such as Skype or RDP, could not be allowed by Application Control.
	28. The background colors of the row on the connection page in the Web UI were not alternating after a filter had been applied.
	29. Traffic using routing rules with routing tables where the "Ordering" setting was set to "Default" was sometimes routed incorrectly.
	30. Accessing certain HTTPS sites sometimes failed if the HTTP ALG was configured to do Web Content Filtering.
	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.
	32. Safe Search configured together with Web Content Filtering sometimes caused system reboot.
	33. Removing a large number of IPsec tunnels from the configuration could cause the system to restart.
	34. Application Control Rules would, with certain selected applications, take longer time than necessary to parse during reconfiguration.
2.60.02	1. No validation was done on hexadecimal pre-shared keys before pressing 'OK' on the configuration page. They are now validated to only accept

hexadecimal strings.

2. It was possible to create user authentication rules without giving them a name, but when saving the configuration an error was shown. The name is now required when adding the rule.

3. The CLI command "dns" showed servers with an index value of 0 to 2. The servers are now listed with an index value of 1 to 3.

4. The statistics value for connections in TCP_FIN state incorrectly also included TCP_OPEN.

5. Long pipe names would disrupt the format of the CLI command "pipes - show".

6. The VLAN interface statistics was reset on each reconfiguration.

7. DHCP relay packets received on interfaces without configured DHCP relay could in some configuration scenarios be dropped.

8. The "Add" button on the application control tab on an IP Policy was enabled even when application control was turned off. It is now enabled/disabled based on the application control slider.

9. Enabling IPv6 on a VLAN interface with IPv6 disabled in the global settings did not produce a configuration warning.

10. Route monitoring using link status did not recover a disabled route after a reconfigure had been issued.

11. Keep-alive set to "Auto" did not work on IPsec tunnels where the Remote Endpoint was a DNS name.

12. SSH CLI sessions could not handle large amount of data being pasted or piped into the session.

13. Connections scanned by IDP were sometimes broken at HA cluster configuration deployment.

14. In the WebUI's L2TP/PPTP client page there was no way of configuring the Originator IP Type or Originator IP.

15. It was not possible to change the index of an interface route that was created automatically by the system using the CLI.

16. In case of timeout, a SIP session was terminated without notifying the UAC and the UAS. This is now fixed by sending a timeout message to the UAC and a cancel message to the UAS in order to notify them before terminating the session.

17. The Application Control feature did not recognize the Sohu Video application correctly.

18. Anycast IPv6 source addresses were treated as invalid by the firewall. In accordance to RFC 4291 a new advanced setting has been added called

"IPv6 Anycast Source" where this behavior can be changed when needed.

19. The CLI commands "arpsnoop" and "ndsnoop" did not output status feedback when invoked. Now there is CLI output indicating what interfaces arpsnoop and ndsnoop are active on.

20. The "dhcpserver" CLI command did not obey the -num or -fromentry options in combination with the -mappings flag.

21. The firewall would in some cases fail to update its ND cache after receiving a valid Neighbor Solicitation.

22. IPv6 network address validation in the WebUI did not allow the usage of network size of 100 and larger.

23. It was not possible to use a DNS object from the address book on the L2TP/PPTP client's remote endpoint.

24. Some of the filter options in the *Status->Run-time information->Connections* page were not applied when selected.

25. The CLI command "sipalg -connection" did not show information under the appropriate columns.

26. No IPv6 interface routes were added in the routing table specified by the interface's routing table membership parameter if the selected routing table was different from the 'main' routing table.

27. Users authenticated by an Identity Awareness Agent were not synchronized to the inactive node in an HA cluster.

28. In certain SIP configuration scenarios the SIP ALG could cause an unexpected reboot of the firewall.

29. Users could be logged out if a large number of PPTP clients were trying to connect simultaneously.

30. The SIP vendor Aastra was not supported by the SIP ALG.

31. The SIP ALG's CLI command "sip -registration flush" did not work.

32. Unreachable RADIUS Accounting servers could in rare cases cause undefined behavior.

33. No log was generated when an L2TP session was closed.

34. The SIP ALG's CLI command "sip -statistics flush" did not work.

35. Valid Neighbor Discovery packets would always cause the interface drop statistics to increase.

36. After an HA failover the inactive node was getting stuck with old route states. This had the side effect that routes could be reported as down in the inactive node even if they were actually up. The issue is fixed by resetting the routes' states whenever a node becomes inactive, and for instance Route monitoring in High Availability will now work as it should.

37. The index value for SNMP stat values for HTTP ALG was reset at reconfiguration so when polling those, only one HTTP ALG was listed.

38. A help text in the HTTP ALG incorrectly mentioned that URL Filter was not supported for the HTTPS protocol.

39. Polling the SNMP property if Alias would, for certain interface types, not return the comment configured for the interface.

40. Configuration backup restore failed if the backup file contained an additional line break at the end of the configuration file.

41. When using DHCP client on an interface the broadcast address was not set. With the broadcast information missing, incoming traffic could not make ARP resolutions correctly.

42. In rare circumstances during HA hand-over, the inactive HA node could erroneously send neighbor solicitations for its own shared IP.

43. There was no error or warning generated when trying to configure switchroutes in an HA cluster.

44. If an authenticated user had a lot of privileges the CLI command "userauth" was printing unaligned output. Furthermore, the CLI command "userauth -user <user>" has been extended to show all the privileges the <user> has.

45. There were no logs about destination port, destination IP or name of SSL VPN interface for incoming SSL VPN connections.

46. It is now possible to use "route" as an alias to the CLI command "routes".

47. The Request URL property of an HTTP host to monitor required the "http://" prefix before the actual URL. This is now fixed by appending it automatically if not given.

48. The firewall failed to match an HTTP Monitoring response with the "expected response" value given by the user in case special characters existed (spaces, tabs, line feeds, carriage returns).

49. If DNS resolution of an HTTP monitored host failed, the respective route was always declared "up" and no other connection attempts were made. The fix allows proper action on the route and re-attempts for DNS resolution.

50. On systems with multiple active IPsec tunnels, configured to add dynamic routes, the memory usage increased for every reconfiguration.

51. Memory management in configurations with IPsec where Xauth and RADIUS was used was not always correctly done.

52. Using RADIUS for authentication and/or accounting under certain rare conditions, could sometimes lead to use of previously released memory

and system instability.

53. On systems with OSPF configured, an unexpected restart could in rare occasions happen after a large number of reconfigurations.

54. The system could in rare occasions restart unexpectedly when doing configuration changes related to IPsec tunnel(s) that uses XAuth for authentication.

55. Extensive memory usage occurred after a very large number of users having been logged in to system.

56. The system showed configuration warnings about overlapping services when a service group is configured as the member of another service group, even if the actual services don't overlap with each other.

57. It was possible to add an Authentication Agent object without specifying a name for it.

58. The "DirectedBroadcasts" drop log message was missing information about the source IP of the host sending the broadcast and the destination IP/network/broadcast it was attempting to use.

59. There was no check whether IPv6 was globally enabled when trying to send IPv6 ping messages, so the user could send pings without knowing this would not work.

60. The PPTP subsystem could in rare circumstances cause unexpected system reboots.

61. The CLI command "ifstat" omitted a line break at the end of the output for certain types of interfaces.

62. The firewall could run out of packet buffers when trying to send too many packets on an R8169 interface with no link. The R8169 driver will now drop packets if no link is detected. Affects DFL-260E/860E.

63. There was no warning issued if the user added an IPv6 route and IPv6 had not been enabled in the configuration.

64. ncorrect or outdated RADIUS Accounting responses could cause an increase in memory consumption.

65. The "pcapdump" functionality couldn't capture the outgoing packets flowing through a VLAN when the capturing target was its base interface.

66. On rare occasions, the firewall restarted unexpectedly when performing a reconfiguration following a previous IDP database update.

67. The last part of an ICMP packet sent through an IPsec tunnel was sometimes dropped.

68. IPv6 groups would in certain rare cases create wrong IPv6 address ranges.

69. The help section for SwitchManagement in the CLI was missing proper descriptions for some properties.

70. The configuration warning shown when a service group contains overlapping services was confusing and has been refined to more clearly show the problem and how it can be resolved.

71. Users being logged out after a timeout could in some rare cases appear to log out multiple times.

72. The pie chart describing category classification for the Web Content Filtering service calculated the percentage incorrectly when the number of hits was very large.

73. The Application Control subsystem allocated memory resources which remained allocated for a long time and could cause the system to run out of memory. A cleanup mechanism has been added that will optimize the Application Control memory usage when the system runs low on RAM.

74. It was not possible to configure two or more SSL VPN interfaces with the same server IP and port.

75. The firewall might experience unexpected behavior when reporting IDP events using SMTP LogReceiver under certain specific circumstances.

76. L2TP client behind NAT using L2TP/IPsec transport mode tunnel did not always succeed in reestablishing the L2TP tunnel.

77. Using RADIUS accounting could under certain rare conditions lead to system instability.

78. In rare occasions when an IPsec configuration was updated, the firewall could restart or stop responding unexpectedly.

79. The MTU for VLAN interfaces was calculated incorrectly, causing unnecessary ICMPv6 PacketTooBig error messages.

80. The invalid_ip_checksum log message did not correctly list the actual and expected checksums as intended.

81. CRL lookup over LDAP did not work if the URL for the CRL distribution point did not contain the port.

82. The ping command could in some rare cases report an incorrect round-trip time.

83. When using a routing table with the "Ordering" setting configured to "Default", the named table was sometimes incorrectly consulted first, instead of the default routing table, during route lookup.

84. Using SCP to download a file from the firewall whose filename included a hyphen (e.g my-cap.cap) would fail with a "Permission denied" error message.

85. The CLI prompt was not shown after the "pipes -show" CLI command.

86. In some situations the system would send an extra TCP ACK packet when it did not need to.

87. The pcapdump command did not print a warning message in the CLI when the buffer was full.

88. The descriptions of custom timeout settings in the WebUI were not consistent and have been changed from "timeout" to "idle lifetime".

89. When using a service group which contained overlapping services, there was no warning message that this may cause undefined behavior.

90. When "arp -notify" was used in an HA setup, the firewall incorrectly used its private MAC address instead of the shared MAC address.

91. The setting for SLB HTTP monitoring erroneously required a value and can now be left blank in the configuration without an error being generated.

92. Changes made to the HTTP normalization parameters on an IDP rule were ignored unless other settings were changed on the same IDP rule.

93. 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 cleared from the lease pool.

94. The WebUI status page for IDP Log always printed "No IDP or Threshold rules are currently logging." even though such rules were configured.

95. When the UTM service expired on one of the members in an HA cluster there was an infinite loop of sending databases from the active node to the inactive node.

96. The Log and Event receivers did not support using another routing table than "main".

97. Hardware statistics for Realtek interfaces of type "8169SC" and "8110SC" was incorrectly represented in the CLI and could not be reset.

98. The HostMonitor subsystem could cause an unexpected restart during reconfiguration when used together with Server Load Balancing.

99. One of the nodes in a High Availability cluster was entering a reconfiguration loop if the antivirus subscription had expired for at least one of the nodes, and there was an IDP database to be synchronized.

100. When using a NAT Pool with a large amount of addresses, the performance was affected in a negative way.

101. It was not possible to send IPv6 packets through an L2TPv3 Server interface.

102. The update center ping requests to update servers were incorrectly sent

when no ALG was in use.

103. The CLI tab completion when adding a Custom Option for a DHCP Server was confusing and has been improved.

104. The firewall's WebUI page showing authenticated users had the label "Logged in as" instead of the name or groups of the user(s).

105. The advanced IP setting to block multicast source addresses was covering a range that included too many addresses. The range has been decreased to the correct 224.0.0.0-239.255.255.255 span.

106. LDAP authentication was failing if the display Name of a user had a space and it was used as user name against an AD.

107. On rare occasions the system could make an unexpected restart when using the HTTP ALG together with Anti-Virus scanning.

108. In certain rare scenarios, the H323 ALG could make the firewall reboot unexpectedly.

109. The system would advertise the wrong IPv6 address when going active in a high availability scenario.

110. 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. Affected models were DFL-260E and DFL-860E.

111. When listing VLANs in the CLI and the same VLAN ID was available on more than one physical interface, the listing was incorrect.

112. Fragmented packets coming from a VLAN going into an L2TPv3 tunnel would be erroneously dropped in some situations.

113. The internal SSH Server could in rare circumstances use an increasing amount of memory.

114. Enabling Router Advertisement on an interface with an unnamed IPv6Network would produce a configuration error.

115. The properties for local_peer and remote_peer in the IPsec logs were sometimes truncated.

116. The system sometimes restarted unexpectedly during a reconfiguration.

117. 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.

118. The log events "too_many_flows_aged" and "failed_to_select_policy_rule" both used the same log ID 01803001. Now the former uses ID 01803005 and the latter ID 01803001.

119. Syslog messages sent from the firewall did not follow the standard

specified in RFC5424. A setting that enables sending Syslog messages according to RFC5424 has been added to the ' LogReceiverSyslog ' configuration object.

120. LDAP queries against OpenLDAP servers did not work as expected. It is now possible, via the new setting; 'Combined Username' and 'Optional Attribute', on the LDAP Server, to specify how LDAP queries towards an OpenLDAP server should be sent.

121. Certain web pages were not possible to reach or load when using the HTTPS ALG.

122. POP3 ALG log messages would sometimes contain incorrect e-mail addresses.

123. On rare occasions, the SMTP and POP3 ALGs could not read fields from the DataHeader correctly.

124. The firewall could perform an unexpected restart in case an up and running PPPoE tunnel was disabled by the user.

125. The DHCP Client did not renew its IP address lease after a link failure had been restored.

126. The firewall would incorrectly terminate some HTTPS sessions when using an HTTP ALG with HTTPS, resulting in a blank page in some browsers.

127. 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.

128. The community string in SNMP Remote Management was truncated if it was longer than 32 characters.

129. Unsolicited ARP reply was not handled correctly according to the Unsolicited ARPReplies setting.

130. 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.

131. When two SSL VPN Interfaces were configured on the same Interface with the same listening IP only one of them was triggering for all client connections, even though different ports were used.

132. The L2TPv3 Server leaked a small amount of memory when a new session was initiated within an established tunnel.

133. Certain SIP PBX configurations caused the firewall to drop INVITE requests.

134. In rare occasions when SIP was reconfigured, the firewall could make an unexpected restart.

135. Some characters were not supported in passwords for users being authenticated using LDAP as source.

136. It was possible to configure multiple static DHCP hosts with the same IP or MAC address without getting a configuration warning.

137. The cryptographic accelerator on DFL-260E/860E could in some high performance situations become unresponsive.

138. With Application Control enabled in some high bandwidth scenarios there was a possibility that connections might stall and make the traffic flow slow.

139. The CLI command "dhcpserver" was not able to show the client identifier string. Now it supports both MAC and identifier.

140. Unexpected exceptions sometimes occurred when the remote endpoint of an IPsec tunnel was set to a DNS object.

141. The system would set the BROADCAST flag in DHCP Discover and DHCP Request messages, despite being fully capable of receiving unicast replies.

142. The update center CLI command would return an error if no argument was specified. It will now show the status of all databases as default action.

143. The L2TP/PPTP client used the wrong source IP when the interface used for L2TP/PPTP traffic was changed due to a DHCP update.

144. The navigation menu disappeared when visiting the "List all active IKE SAs" from the IPsec status page. The navigation menu should now correctly still be there and highlight IPsec status.

145. 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.

146. The configurable minimum lease time of the DHCP server was incorrectly set to 0 seconds. This has now been changed to 30 seconds.

147. ndsnoop messages would sometimes show the firewall's MAC address as 00-00-00-00-00-00.

148. The system could in some situations misbehave when parsing malformed SNMP packets on the remote management interface.

149. Advisory links were missing on the IDP log event list in the web interface, and when listing a large amount of IDP log events the system could become unresponsive.

150. A space was placed before %REDIRHOST% in HTTP banner files leading to bad URLs.

151. The switch driver used on DFL-260E (rev a2) appliances had a faulty default configuration, which lead to performance issues.

152. Service custom timeouts did not trigger when used by an IP Policy.

153. Forcibly logging out authenticated users via the CLI command "userauth - remove" did not generate a log event.

154. The TFTP ALG would stop forwarding packets after 65535 blocks.

155. The CLI commands "ippool" and "idppipes" had no default usage and they were always in need of an argument. Now they can be used without any argument which implicitly means running them with the "-show" argument. Furthermore the "-max" option for "ippool" has been renamed to "-num" to be consistent with other CLI commands.

156. When using trace route through the firewall the responses were not forwarded correctly to the initiating client.

157. The icons for the collapsible search filters on log pages were not following user interface standards. The down arrow is now shown when the filter is expanded, instead of the opposite.

158. The ALG didn't handle SSLv2 compatibility mode with new TLS protocols. The ALG has been updated to handle compatibility mode correctly.

159. Some statistics for rejected DHCP Relay packets was increased even though nothing was rejected.

160. The "ipsecstats -ike" CLI command would output a lot of unnecessary "more entries not displayed" lines.

161. When using the HTTP ALG together with Anti-Virus scanning, the system would sometimes make an unexpected restart.

162. On rare occasions certain IP addresses in blacklist could lead to faulty behavior.

163. Port Based VLAN did not work on DFL-260E (rev a2) model.

164. An incorrect PPPoE interface name could be logged in closed / open events with certain configurations.

165. PPPoE interfaces could in rare circumstances make the firewall restart unexpectedly.

166. It was not possible to disable Port Based VLAN without rebooting the device.

167. Port Based VLAN didn't properly forward packets according to switch routes.

168. VLAN traffic sent over, and received from, L2TPv3 interfaces was incorrectly required to be received on, or forwarded on, a VLAN interface with identical ID. Now, L2TPv3 interfaces trust the routing configuration

and do not enforce any additional restrictions regarding how VLAN packets are handled by the rest of the system

169. Group names, returned from external databases e.g LDAP, that contained spaces were not supported.

170. 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'.

171. The 'blacklist' CLI command did not set the correct port number and destination URL in its output.

172. The default metric for a manually added route was 0 instead of 100.

173. Static destination address translation would fail for transport mode IPsec traffic.

174. Changing an IDP Rule Action setting from Action "Protect" and "Dynamic Black Listing" enabled to Action "Audit" left the "Dynamic Black Listing" enabled.

175. IPsec Transport mode clients using the same remote ID behind NAT devices failed to connect simultaneously.

176. A warning text has been added to inform the administrator when the maximum number of IPsec rules for an IPsec interface has been reached.

177. The SSL VPN Portal would sometimes not use the same authentication method as the SSL VPN Client when RADIUS authentication was enabled.

178. In rare circumstances when using High Availability and OSPF, there could be a flood of OSPF packets on the sync interface.

179. A RADIUS Accounting session was closed if the reply from the RADIUS server contained RADIUS Attributes.

180. The ifstat CLI command did not show the chip information for some E1000 based interfaces.

181. Phase one rekey negotiations in the cases where peer Xauth authentication is required were removed.

182. Under rare circumstances, an IPsec configuration could cause the firewall to run out of buffers.

183. The traffic shaping subsystem consumed a large amount of CPU resources when processing packets that could not fit within a configured pipe.

184. The system could in rare cases perform an unexpected restart when IPsec clients were connected behind a NAT gateway.

185. The handling of large amounts of hosts in blacklist has been optimized.

186. The clone option was not always available on the WebUI objects.

187. The IP protocols 33 and 48 were logged with incorrect names and IP

	protocols 131 to 142 were missing names. The IP protocol list has been updated according to the current IANA definition. 188. Receiving ESP packets for a new IPsec security association, before the last IKE message in the negotiation was received, could cause the firewall to drop the ESP packets for that security association during its entire lifetime. 189. ISAKMP cookies in IKEsnoop messages were sometimes displayed incorrectly and could lead to a mismatch in the print out of the 'Delete SPIs' and the cookies in an 'IKE delete' message. 190. In an IPsec scenario where XAuth was used on the tunnel, the memory consumption could in rare circumstances increase unexpectedly after renegotiations. 191. Certain configurations related to one sub system could cause a security vulnerability.
2.40.04	1. The IP protocols 33 and 48 were logged with incorrect names and IP protocols 131 to 142 were missing names. The IP protocol list has been updated according to the current IANA definition. 2. Syslog messages sent from the firewall did not follow the standard specified in RFC5424. A setting that enables sending Syslog messages according to RFC5424 has been added to the ' LogReceiverSyslog ' configuration object 3. Certain configurations related to one sub system could cause a security vulnerability.
2.40.03	1. Routemon did not detect link state changes on some Realtek interfaces. Affected models: DFL-260E/DFL-860Es. 2. The link status info for the Realtek interfaces disappeared after a reconfigure. Affected models: DFL-260E/DFL-860E 3. In some scenarios with IDP configured, traffic of certain patterns could in rare circumstances be delayed 4. It was not possible to connect multiple L2TP/IPsec clients behind the same NAT gateway. 5. SNMP Interface Alias field was empty when selecting "Comment" in "Interface Alias". 6. If L2TP clients with the same local IP address established IPsec tunnels behind a NAT device there were sometimes problems with the connections. 7. The OSPF routes database was not updated during reconfigure in some

High Availability scenarios.

8. In some unusual circumstances the use of XAuth based authentication would lead to an unexpected reboot

9. 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.

10. The firewall Dynamic Routing Rules did not properly export / import OSPF routes when they were filtered by "OSPF Tag range" or "Router Type".

11. A few log message categories, such as SSL VPN and IPv6 Neighbor Discovery were missing from the log message exception list..

12. In some scenarios when using IPsec with XAuth, ESP delete notifications would not be sent.

2.40.02	

1. In some rare occasions, the memory consumption of the firewall could increase unexpectedly when deploying cluster configurations.

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'.

3. The 'blacklist' CLI command did not set the correct port number and destination URL in its output.

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.
2.40.01	1. Corrected leap year problem where leap year day was added to January instead of February.
	2. The log event no_arp (ID:04100007) firewall action text was previously route_enabled, the text is now corrected to route_disabled.
	3. Time unit 'seconds' added to help texts in WebUI ALG SIP dialog and CLI command 'help ALG_SIP'.
	4. An expired AV or IDP license in an HA environment could trigger unexpected behavior in the inactive cluster node.
	5. Some web authentication scenarios could lead to unexpected behavior by the firewall.
	6. The output text for the CLI command 'dns -list' was not formatted correctly when using SSH remote management.
	7. The firewall did not handle lower and upper case correctly in some configuration scenarios where objects were named almost identically.
	8. 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.
	9. Cancelling the HA wizard would result in unexpected behavior of the firewall. Affected models: DFL-260E/860E.
	10. In rare occasions, closing down a SIP session could lead to an unexpected restart of the firewall.
	11. The general stability of SSL VPN tunnels has been improved.
	12. The deployment of new configuration could have a negative impact on the performance of Realtek 8169 interfaces. Affected models: DFL-260E/DFL-860E.
	13. Running SSL VPN on a shared IP in an HA cluster disconnected the client at reconfiguration due to the inactive node going active during reconfiguration.
	14. A recent change in scp (secure copy) uses an end of option parameter

that was handled erroneously by the firewall causing scp connections to be closed unexpectedly.

15. The "add" CLI command would in some cases add a new configuration object with errors, and the "set" CLI command allowed the user to modify configuration objects by entering invalid values. Now the behavior has been changed to not modify the configuration if the resulting change causes errors, unless the "-force" flag is specified.

16. The CLI "netobject" command incorrectly printed IPv6 addresses in IPv4 format.

17. It was not possible to disable sending out High Availablility cluster heartbeats on nodes. The setting was not obeyed.

18. The Web Content Filtering (WCF) server connection could stall after a reconfigure and fail to resolve new URLs. The issue has been corrected along with additional server connection statistics for the 'httpalg -wcfcache' CLI command.

19. Log messages containing routing information used invalid values.

20. Using the H323 ALG could in rare circumstances lead to unexpected behavior.

21. An error in the configuration module could in rare occasions lead to unexpected behavior during the deployment of a new configuration.

22. The output of the CLI command "ifstat" has been extended to list the shared MAC addresses on the interfaces of High Availability cluster nodes.

23. Passwords for newly added users were not encrypted in the configuration file.

24. OSPF MD5 authentication misbehaved when using ID other than 2.

25. The RADIUS accounting session ID string could under some circumstances be reused for a later session.

26. A prompt was not printed in the CLI after activating a new configuration.

27. A recent security patch for **CVE-2011-3389** in some popular web browsers made the firewall's SSL VPN client download page unreachable.

| 2.40.00 | 1. Some VPN configurations using Radius Accounting did not report in/out octet statistics to the Radius Accounting server.
2. The H.323 ALG did not allow FACILITY messages to be sent during the ALERTING state.
3. In certain scenarios, traffic originating from LDAP could lead to unexpected behavior by the firewall.
4. If SSL VPN was configured to listen on a proxy ARPed IP, it was not possible to log in to the SSL VPN portal. |

	5. Browsing to certain pages in the WebUI would lead to unexpected behavior for the firewall. Affected models: DFL-260E and DFL-860E.
	6. Some scenarios made the firewall send malformed packets in an SSL negotiation.
	7. In a High Availability scenario it was not possible to log in to the firewall in order to download the SSL VPN client.
	8. The value "Password Attribute" for LDAP Servers could not be empty. It is now possible to create an LDAP Server with an empty "Password Attribute" field.
	9. The possibility to configure interface groups inside interface groups has been added.
	10. Routes monitored only by ARP were not marked as down when the link on the Ethernet interface was down. Affected models: DFL-260E and DFL-860E.
	11. 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.
	12. Large VLAN tagged packets would be dropped by the RealTek R8169 driver. The driver has been updated to handle VLAN packets. Affected models: DFL-260E and DFL-860E.
	13. The RealTek R8169 interface reported wrong link speed for SNMP. The interface has been updated to report the correct speed. Affected models: DFL-260E and DFL-860E.
	14. The RealTek R8169 driver contained a watchdog that erroneously triggered too often and made the interface restart. The watchdog has been updated with a longer timer to prevent this from happening. Affected models: DFL-260E and DFL-860E.
2.30.01	1. The firewall did not forward SIP registrations REQUEST with null values in the "Authorization" field.
	2. The source port 20 is occupied when combining the SAT Action in an IP rule with the FTP ALG.
	3. The CLI commands "reset -configuration" and "reset –unit" show incorrect default management IP.
	4. SIP ALG would close SIP calls two minutes after the call session was established in some network scenario.
	5. The "Route Type" in "OSPF Actions" was incorrectly interpreted by the firewall when the configuration was activated.
	6. An unexpected restart could occur during a configuration deployment when

	new IPSec tunnels were added to the configuration.
	7. It was not possible to use all address object combinations in places like routes or in the Address Book.
	8. The severity for the log message sslvpn_max_sessions_reached was incorrectly set to DEBUG, but has been changed to NOTICE.
	9. IP4Groups containing Userauth configured objects were not available for selection in IPRules. The IPRules have been updated to allow IP4Groups containing objects with Userauth.
	10. The TLS ALG rejected SSL HELLOs with zero or more than one compression method.
	11. Some cipher suite combinations prevented the AES256 algorithm to be used when establishing SSH administration sessions to the firewall.
	12. Some specially crafted SDP payloads could cause unexpected reboots of the firewall.
	13. The edit alternative for Comment Groups was not shown.
	14. The Web GUI 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.
	15. The ping -verbose CLI command did not print the correct translated port if the packet was affected by a SAT rule in some cases.
	16. Some statistics on IXP interfaces were not correctly printed on the firewall console. Affected models: DFL-160/260E/860E.
2.27.03	1. The usage column in the DHCP Server status page has been updated to show active clients.
	2. References to UserAuth privileges for authenticated users could change when modifying the number of configured privileges.
	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.
	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.
	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.
	6. In certain scenarios, the voice transmitted through the SIP ALG terminated

suddenly two minutes after the call was established.

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.

8. A faulty model check made the Switch Management not display all the switch ports in the WebUI for the DFL-860E model.

9. The Realtek 8169 interface reported link down incorrectly. This caused route monitor to not work properly. Affects: DFL-260E and DFL-860E.

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.

11. Anti-virus scanning of zip files containing files with a large compressed size could sometimes lead to unexpected behavior.

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).

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 | 1. It was not possible to use User Authentication on IP4Group objects. |

1. It was not possible to use User Authentication on IP4Group objects.

2. Certain SIP server scenarios in REGISTER transactions made the firewall reject incoming SIP calls.

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.

4. The usage bars on the DHCP Server status page were not displayed correctly when leases reached 100% usage.

5. ACK messages for non 2xx PBXs responses were not forwarded by the SIP ALG.

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.

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.

8. CLI command "ipsecdefines" has been removed from "techsupport"

	command.
	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.
	10. Incoming SIP traffic routed through an IPsec tunnel was discarded by the SIP ALG.
	11. Some empty configuration values were not written to the configuration. After a restart of the firewall the default values were used instead.
	12. Some buttons in the web user interface had truncated text.
	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.
	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.
	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.
2.27.01	1. Certain SIP PBX configurations blocked media transmission on calls established between devices located on the same interface of the firewall.
	2. The POP3 ALG did not reset its state after a failed authentication. This could cause the next login attempt to fail.
	3. Specific Intrusion Detection Protection (IDP) scenarios using hardware acceleration could cause scans to fail.
	4. Restarting a GRE interface did sometimes trigger an unexpected restart of the firewall.
	5. The POP3 ALG did not allow Digest-MD5 authentication.
	6. The SIP ALG could forward malformed SIP messages if a range 0-65535 was used as destination port in the SIP service configuration.
	7. Specific scenarios using the PPTP ALG could sometimes cause an unexpected restart of the firewall.
	8. 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.
	9. 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. 10. 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. 11. The HTTP ALG MIME type check did not have support for OpenDocument Text Documents (odt). 12. Script execute did not allow the 'cc' command to run without parameters. The command has been updated.
2.27.00	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. 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. 3. Some HTTP headers could cause HTTP connections through the HTTP ALG to be closed down prematurely. 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. 5. The SMTP ALG did not accept response codes that only contained numeric data. 6. Browsing the Web User Interface over HTTPS would sometimes result in "Error 500 - Internal server error". 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. 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. 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.

	10. A limitation on the number of simultaneous WebAuth transaction could prevent the authentication of authorized users.
	11. The IP Rule view in the Web User Interface was slow when viewing large collection of rules. The rendering speed has been improved.
	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.
	13. The Mappings and Leases links on the DHCP Server status page in the Web User Interface didn't work.
	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.
2.26.02	*[DFL-210/260/800/860/1600/1660/2500/2560/2560G]* 1. The "range" parameter in the "rules" CLI command did not work. 2. The CLI command "dns -query" only returned one IP address even though the DNS Record contained multiple entries. 3. An error in the configuration engine caused problems when configuring the first OSPF Area for an OSPF Router Process. 4. When using services with the SYN flood protection (SYN Relay) functionality enabled, reconfigurations could result in unexpected behavior. 5. Certain conditions sometimes led to an unexpected behavior when a firewall had IPsec tunnels configured. 6. It was not possible to use User Authentication enabled objects in Routing Rules, Threshold Rules, IDP Rules or Pipe Rules. 7. The log pages for the Web User Interface were rendered incorrectly resulting in artifacts on some web browsers. 8. The SMTP ALG did not load all whitelist and blacklist entries if the number of entries were more than about 30. The entries that failed to load were silently ignored. All configured whitelisted and blacklisted addresses are now loaded and filtered correctly. 9. Users were not properly logged in when IPsec LAN to LAN tunnels were configured to require IKE XAuth. This could cause an unexpected reboot. Now the LAN to LAN case is properly handled by IKE XAuth. 10. The L2TP/PPTP Server overview grid did not have a column for "Server IP". 11. The dropdown to select the interface for OSPF Neighbor in the Web User Interface printed the name wrongly. The dropdown code has been enhanced to handle this value correctly and print the proper name.

	12. The validation of the latency setting in the Host Monitor configuration was not correct. The configured value was lowered to an incorrect value. 13. The setup wizard only created the second of the two possible Syslog servers. The first Syslog server is now correctly created by the wizard. 14. The "min" and "preferred" input fields had swapped position on the configuration page for IPsec Algorithms and IKE Algorithms in the Web User Interface. The position of the input fields has been corrected. 15. In the Web User Interface it was not possible to change order of objects that were both disabled and deleted. It's now possible to move objects that are both disabled and deleted. *[DFL-160]* 1. Enabling POP3 on the Inbound Traffic page did not have any effect.
2.26.01	*[DFL-210/260/800/860/1600/1660/2500/2560/2560G]* 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. 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. 8. 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 9. The license page showed an incorrect value for maximum number of PPP

	tunnels.
	10. 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.
	11. 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.
	12. 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.
	13. 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.
	14. 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.
	15. There was a critical defect in the Web Content Filter functionality that could cause the firewall to reboot unexpectedly.
	[DFL-160]
	1. 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.
	2. 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.

	rebooting.
	7. Web content filtering does not work for blocking HTTPS site and the ReclassifyURL is not working.
11.10.01	**1. HA: Transparent Mode won't work in HA mode:**
	There is no state synchronization for Transparent Mode and there is no loop avoidance.
	2. **HA: No state synchronization for Application Layer Gateways:**
	No aspect of Application Layer Gateways 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.
	3. HA: Tunnels unreachable from inactive node:
	The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.
	• Inactive HA member cannot send log events over tunnels.
	• Inactive HA member cannot be managed / monitored over tunnels.
	• OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.
	4. HA: No state synchronization for L2TP and PPTP tunnels:
	There is no state synchronization for L2TP and PPTP tunnels. On failover, incoming clients will e-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.
	5. 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.
	6. Not able to establish L2TP/L2TPv3 over IPSec tunnel between two DFL firewalls on transport mode.
	Workaround: Need to specify "local endpoint" to the WAN IP address on the client site.
11.04.01	**1. HA: Transparent Mode won't work in HA mode:**

	There is no state synchronization for Transparent Mode and there is no loop avoidance.
	2. **HA: No state synchronization for Application Layer Gateways:**
	No aspect of Application Layer Gateways 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.
	3. HA: Tunnels unreachable from inactive node:
	The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.
	• Inactive HA member cannot send log events over tunnels.
	• Inactive HA member cannot be managed / monitored over tunnels.
	• OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.
	4. HA: No state synchronization for L2TP and PPTP tunnels:
	There is no state synchronization for L2TP and PPTP tunnels. On failover, incoming clients will e-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.
	5. 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.
10.22.01	**1. L2TPv3 is not support:** DFL will not add a switch route for L2TPv3 remote client. **2. Radius server redundancy issue :** DFL will not rollback to primary Radius server till Secondary Radius server is down. **3. Unable to support Radius setting via CLI.**
10.21.02	**1. HA: Transparent Mode won't work in HA mode:** There is no state synchronization for Transparent Mode and there is no loop avoidance. **2**. **HA: No state synchronization for Application Layer Gateways:** No aspect of Application Layer Gateways 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. **3. HA: Tunnels unreachable from inactive node:** The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node. • Inactive HA member cannot send log events over tunnels. • Inactive HA member cannot be managed / monitored over tunnels. • OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings. **4. HA: No state synchronization for L2TP and PPTP tunnels:** There is no state synchronization for L2TP and PPTP tunnels. On failover, incoming clients will e-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range. **5. 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.

2.60.02	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 tundels are established to/from the active node.
	
	    A. Inactive HA member cannot send log events over tunnels.
	    B. Inactive HA member cannot be managed / monitored over tunnels.

	C. 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. 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.
2.40.04	1. SSL VPN: Outer interface 'any' limitation: If the SSL VPN interface is configured with the outer interface 'any' option, SSL VPN will be disabled. 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 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. 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. D. Inactive HA member cannot send log events over tunnels. E. Inactive HA member cannot be managed / monitored over tunnels. F. 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. 6. 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. 7. 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.
2.40.02	1. If the SSL VPN interface is configured with the outer interface 'any' option, SSL VPN will be disabled. 2. Don't support the latest protocol used by oray.net Peanut Hull clients. 3. Transparent Mode won't in HA mode. 4. ALGs won't synchronize states in HA mode. 5. L2TP, PPTP, IPSec won't synchronize states in HA mode. 6. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, L2TP and GRE tunnels. 7. If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over VPN 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. No aspects of the IDP signature states are synchronized in HA modes.
2.40.01	1. If the SSL VPN interface is configured with the outer interface 'any' option, SSL VPN will be disabled. 2. Don't support the latest protocol used by oray.net Peanut Hull clients. 3. Transparent Mode won't in HA mode. 4. ALGs won't synchronize states in HA mode. 5. L2TP, PPTP, IPSec won't synchronize states in HA mode. 6. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, L2TP and GRE tunnels. 7. If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over VPN 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. No aspects of the IDP signature states are synchronized in HA modes.
2.40.00	1. Don't support the latest protocol used by oray.net Peanut Hull clients. 2. Transparent Mode won't in HA mode. 3. ALGs won't synchronize states in HA mode.

	4. L2TP, PPTP, IPSec won't synchronize states in HA mode.
	5. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, L2TP and GRE tunnels.
	7. DFL cannot support redirecting L2TP/IPSec tunnels to another DFL working in LAN.
	8. No aspects of the IDP signature states are synchronized in HA modes.
2.30.01	1. Don't support the latest protocol used by oray.net Peanut Hull clients.
	2. Transparent Mode won't in HA mode.
	3. ALGs won't synchronize states in HA mode.
	4. L2TP, PPTP, IPSec won't synchronize states in HA mode.
	5. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, L2TP and GRE tunnels.
	7. DFL cannot support redirecting L2TP/IPSec tunnels to another DFL working in LAN.
	8. No aspects of the IDP signature states are synchronized in HA modes.
2.27.03	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.
	10. The function "StateKeepAlive" of NAT Pool is not working.
	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.
	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	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. 10. The function "StateKeepAlive" of NAT Pool is not working.
2.27.01	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. 10. The function "StateKeepAlive" of NAT Pool is not working.
2.27.00	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 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. 10. The function "StateKeepAlive" of NAT Pool is not working.
2.26.02	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.
	10. The function "StateKeepAlive" of NAT Pool is not working.
	11. The DUT would be crash and reboot after restart the GRE interface.
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 v12.00.13
- NetDefend Firewall CLI Reference Guide v12.00.13
- NetDefend Firewall Logging Reference Guide v12.00.13
- NetDefend Firewall Application Control Sigs v12.00.13