
**NetDefendOS Version:** 11.04.01

**Published Date:** 2016-10-13



## Copyright Notice



## Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

## Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

## Content:

## Revision History and System Requirement:

| Firmware Version | Date | Model | Hardware Version |
|---|---|---|---|
| 11.04.01 | Oct 13, 2016 | DFL-1660/2560/2560G<br>DFL-260E/860E<br>DFL-870 | DFL-260E A2<br>A1 (for all models) |
| 10.22.01 | Aug 03, 2015 | DFL-1660/2560/2560G<br>DFL-260E/860E | DFL-260E A2<br>A1 (for all models) |
| 10.21.02 | Dec 23, 2014 | DFL-1660/2560/2560G<br>DFL-260E/860E | DFL-260E A2<br>A1 (for all models) |
| 2.60.02 | Jul 07, 2014 | DFL-1660/2560/2560G<br>DFL-260E/860E | DFL-260E A2<br>A1 (for all models) |
| 2.40.04 | Jul 17, 2013 | DFL-1660/2560/2560G<br>DFL-260E/860E | DFL-260E A2<br>A1 (for all models) |
| 2.40.03 | Apr 05, 2013 | DFL-1660/2560/2560G<br>DFL-260E/860E | DFL-260E A2<br>A1 (for all models) |
| 2.40.02 | Dec 15, 2012 | DFL-1660/2560/2560G<br>DFL-260E/860E | DFL-260E A2<br>A1 (for all models) |
| 2.40.01 | Apr 15, 2012 | DFL-1660/2560/2560G<br>DFL-260E/860E | A1 (for all models) |
| 2.40.00 | Oct 21, 2011 | DFL-1660/2560/2560G<br>DFL-260E/860E | A1 (for all models) |
| 2.30.01 | June 1 2011 | DFL-1660/2560/2560G<br>DFL-260E/860E | A1 (for all models) |
| 2.27.03 | Nov 24 2010 | DFL-210/800/1600/2500<br>DFL-260/860/1660/2560/2560G<br>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<br>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<br>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<br>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<br>DFL-210/800/1600/2500<br>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<br>DFL-210/800/1600/2500<br>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<br>DFL-260/860/1660/2560/2560G | A1 (for all models), A2/A3/A4/A5 (for DFL-210/800/1600/2500) |
| 2.25.01.28 | July 15, 2009 | DFL-210/260/800/860/1600/2500 | A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500) |
| 2.25.01.22 | Jun 11, 2009 | DFL-210/260/800/860/1600/2500 | A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500) |

| | | | |
|---|---|---|---|
| 2.20.03 | Oct 21, 2008 | DFL-210/260/800/860/1600/2500 | A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500) |
| 2.20.02 | Jul 10, 2008 | DFL-210/260/800/860/1600/2500 | A1 (for all models), A2/A3/A4 (for DFL-210/800/1600/2500) |

## Upgrading Instructions:

### Upgrading by using CLI via SCP protocol

*SCP (Secure Copy)* is a widely used communication protocol for file transfer. No specific SCP client is provided with NetDefendOS distributions but there exists a wide selection of SCP clients available for nearly all workstation platforms. SCP is a complement to CLI usage and provides a secure means of file transfer between the administrator's workstation and the NetDefend Firewall. Various files used by NetDefendOS can be both uploaded and downloaded with SCP. This feature is fully described in *Section 2.1.6, "Secure Copy" of NetDefend Firewall v11.04.01 user Manual*.

### Upgrading by using Web-UI

For detailed installation and upgrade instructions, please refer to the Firmware Upgrades chapter in the *NetDefend Firewall v11.04.01 User Manual.*

## New Features:

| Firmware Version | New Features |
|---|---|
| 11.04.01 | **1. Tunnel Monitoring of IPsec Interfaces**<br>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.<br>**2. SNMPv3 Support**<br>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.<br>**3. Protection Against Password Brute Force Attacks**<br>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.<br>**4. Transparent Mode Configuration in the Startup Wizard**<br>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.<br>**5. Automatic Daylight Saving Time**<br>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.<br>**6. IPv6 Router and Prefix Discovery**<br>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.<br>**7. Web Profile**<br>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.<br>**8. User Authentication REST API**<br>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.<br>**9. Broadcast Forwarding**<br>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.<br>**10. IPv6 Web Content Filtering and Anti-Virus on HTTP data**<br>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.<br>**11. IPv6 support in Loopback interfaces**<br>Loopback interfaces have been enhanced to enable IPv6 communication, allowing the administrator to apply more advanced IPv6 routing scenarios.<br>**12. WebUI Time Synchronization Improvements**<br>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.<br>**13. Custom Banner Support for LW-HTTP ALG**<br>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-2560 and DFL-2560G models.

**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.<br>**31. IPv6 HA Support**<br>The system now supports redundancy in a high availability setup while actively forwarding IPv6 traffic.<br>**32. DHCPv6 Client**<br>A DHCPv6 Client has been added, which can be used on Ethernet, VLAN and link aggregation interfaces.<br>**33. IPv4 Path MTU Discovery**<br>The system now supports IPv4 Path MTU Discovery which allows communicating endpoints to use optimal packet sizes that prevent fragmentation at intermediate routers.<br>**34. SSL/TLS AES 128 and AES 256**<br>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.<br>**35. Use of HMAC-MD5 in IPsec and SSH**<br>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.<br>**36. Use of HMAC-SHA1 in IPsec**<br>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.<br>**37. Improved Anti-Virus Block Pages for HTTP**<br>The system now supports an Anti-Virus cache that allows improved notification pages when viruses are found in large files.<br>**38. IP Policies with Application Layer Functionality**<br>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.<br>**39. HTTP Content Inspection Improvements**<br>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.<br>**49. MIB File Download via Web UI or SCP**<br>The system MIB files can now be downloaded directly from the device either via the web user interface or via SCP.<br>**50. Improved SNMP Support**<br>The system can now keep interface SNMP indexes and interface OIDs persistent during reconfigures and restarts.<br>**51. Traceroute Support in CLI**<br>A new "traceroute" CLI command has been added that can be used to perform traceroute towards domain names, IPv4 and IPv6 addresses.<br>**52. Improved Ping CLI Command**<br>The "ping" CLI command has been improved to support ping towards IPv6 addresses and domain names.<br>**53. L2TP CLI Command**<br>A CLI command has been added to list active L2TP client sessions.<br>**54. Improved ifstat CLI Command**<br>The ifstat CLI command now prints the link status of any configured interfaces when executed without any arguments.<br>**55. Improved 'ike -show' CLI Command**<br>The 'ike -show' CLI command now prints the local and remote IDs in addition to the existing interface, remote and local endpoints.<br>**56. PPTP CLI Command**<br>A CLI command has been added to list active PPTP client sessions.<br>**57. Improved Statistics for IKE/IPsec**<br>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:**<br>Remote management with the WebUI and CLI now supports using RADIUS as the authentication source. |
| 10.21.02 | **1. True Application Control:**<br>The addition of Application Content Control allows for granular policies using application attributes to control the contents of data streams for applications. This will not only allow for granular policies on an application level, but also on an application content level, such as restricting access to certain usage of application functions such as web browser version control, blocking of DNS queries for certain domains and blocking of mail transfers containing certain keywords in the subject field. This will also allow for granular logging of the contents of data streams generated by the applications and protocols, providing an unprecedented audit view of data that applications in the network transmit.<br>**2. SSL Inspection for Application Control:** |

| | |
|---|---|
| | This new feature provides D-Link NetDefendOS the capability to identify applications that use the HTTPS protocol. Based on the result, the applications can be bandwidth managed, blocked and/or logged.<br>**3. IKE/IPsec HA synchronization:**<br>Full HA synchronization of established IKE negotiated IPsec tunnels are now supported, providing full redundancy for service critical installations where IPsec tunnels are used. Fully established IKE and IPsec SAs are now synchronized to the inactive HA cluster node, making it possible to keep tunnels up and running throughout a node failure, restart or upgrade, eliminating the need to renegotiate the tunnel after HA system fail-over. Fail-over times should be less than a second and the impact on routed packets over the tunnel is minimal. Note, only available on DFL-1660, DFL-2560 and DFL-2560G.<br>**4. IKE/IPsec Virtual Routing support:**<br>Virtual Routing for IKE/IPsec tunnels is now supported, which allows for flexible usage of IKE/IPsec tunnels in more complex networks with overlapping IP ranges, or where multiple routing tables are used. In practice this means that you can now terminate or initiate IKE and IPsec traffic in any routing table and not only in the main routing table. It also allows for a more flexible configuration of an IKE/IPsec tunnel, where it is possible to configure any ARP or core routed IP to listen on for incoming IKE/IPsec traffic, and not only the interface IP address.<br>**5. Link Aggregation support:**<br>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.<br>**6. Improved anti-virus scanning:**<br>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.<br>**7. 6-in-4 Tunneling:**<br>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.<br>**8. Support for IEEE 802.1ad (QinQ) Service VLAN:**<br>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.<br>**9. PCAP support in the Web User Interface:**<br>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.<br>**10. Added Diagnostic Console Page in the Web User Interface:**<br>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.<br>**11. DHCP Client Enhancements:**<br>The DHCP Client is now supported on VLAN interfaces.<br>**12. PPPoE Client Enhancements:**<br>It is now possible to use the PPPoE client over VLAN as well as Ethernet Interfaces.<br>**13. RADIUS Enhancements:**<br>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.<br>**14. Command-Line Interface (CLI) Enhancements:**<br>The Command-Line Interface (CLI) now supports viewing and filtering the Memory Log using CLI commands.<br>**15. User Identity Awareness Enhancement:**<br>The User Identity Awareness Agent has been updated with a protocol that supports a larger number of group memberships for a user.<br>Note: NetDefendOS 10.21.02 and up is required for use with this new 1.01.00 Agent version.<br>**16. ZoneDefense with Universal MIB:**<br>ZoneDefense now supports switches that use the Universal MIB.<br>**17. Diagnostics & Quality Improvements:**<br>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.<br>**18. Source IP selection for RADIUS requests:**<br>The RADIUS server configuration has been enhanced with the possibility to manually specify the source IP for RADIUS requests.<br>**19. DHCPv6 Server support:**<br>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.<br>**20. RADIUS Relayer:**<br>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.<br>**21. ARP Authentication:**<br>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.<br>**22. RADIUS server retry:**<br>Configuration options have been added to make the firewall able to retry contacting the primary RADIUS server if failing to contact the backup servers configured.<br>**23. Web Content Filtering update:**<br>Web Content Filtering category 31 has been changed from "Spam" to "Remote control/desktop".<br>**24. Improved certificate information in the CLI:**<br>The CLI has been improved to show more detailed information about the IPsec certificate cache.<br>**25. Alias for routes**<br>It is now possible to use "route" as an alias to the CLI command "routes".<br>**26. High Availability Status in the Web User Interface**<br>The current High Availability status is now visible in the "System Information" list on the main status page in the web user interface. |
| 2.60.02 | 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.<br>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.<br>3. **IPv6:** Numerous changes have been implemented in order to improve interoperability and protocol compliance.<br>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.<br>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.<br>6. **Web Content Filtering for HTTPS:** Web Content Filtering support has been added for HTTPS traffic.<br>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.<br>8. **URL filter for HTTPS:** URL filter support has been added to the HTTP ALG when using the HTTPS protocol.<br>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.<br>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.<br>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.<br>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.<br>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.<br>14. **Added "IPA" as recognized MIME type** An .ipa file is an iPhone |

| | |
|---|---|
| | application archive file which stores an iPhone app.<br>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.<br>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.<br>17. **Enhanced ICMPv6 configuration:** A setting was added to control the maximum number of ICMPv6 Neighbor Discovery Options allowed and hence improve network security.<br>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<br>19. **Ping CLI parameter renaming**<br>The ping CLI command has been updated with a more logical parameter naming. The '-recvif parameter is now renamed to '-srcif'.<br>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.<br>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.<br>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.<br>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.<br>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.<br>2. Added "IPA" as recognized MIME type.<br>3. Support for hardware acceleration of IKE negotiations for DFL-2560/2560G |

| | |
|---|---|
| | to offload the CPU and make IPsec setup faster. |
| 2.40.02 | No new features are introduced in the 2.40.02 release. |
| 2.40.01 | 1. Support the Cisco IPSec client on iPhone.<br>2. Double Web Content Filtering local cache size on all models to accommodate more categorized sites.<br>3. Support CHAP, MS-CHAP, MS-CHAPv2 and No authentication mechanisms for SSL VPN.<br>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.<br>2. Remove restrictions on the number of HTTP posters. All other network clients listed in "Misc Clients" also benefit from this restriction removal.<br>3. Support authenticating users using the Ethernet MAC address over HTTP(S).<br>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.<br>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.<br>2. Support TLS renegotiation (RFC 5746) in the TLS ALG.<br>3. Increase the number of IDP signatures to up to 30,000. Configuration of up to 30,000 IDP signatures is now possible.<br>(Affected models:DFL-1660/2560/2560G)<br>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.<br>5. Enhancement of services drop down menu. The drop down menu for services has been enhanced to show port numbers.<br>6. Enhanced IDP signature configuration. It's now possible to select IDP signature groups from a visual tree interface.<br>7. Add lifetime for connection in the log messages.<br>8. Warning for incompletely cloned objects. When cloning objects that contain properties which cannot be cloned, an alert will be displayed.<br>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.<br>2. A new log message has been added indicating that an ARP resolve query failed.<br>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.<br>2. Logging enabled by default on rules for the following objects: Access, DHCP Server, DHCP Relay, Routing Rule, Dynamic Routing Policy Rule, IDP Rule Action, IP Rule, OSPF Router Process, Threshold Action and User Authentication Rule.<br>3. Static configuration objects default to their default values if the objects contain configuration errors. This will prevent the firewall to misbehave due to configuration errors on static objects.<br>4. The script command has been updated to handle adding objects with dependencies between each other.<br>5. User authentication has been updated with a new authentication source that will grant access to the user without checking any credentials. This functionality can be used to authenticate users from within login scripts etc, to make auditing easier.<br>6. All rule page layouts have been updated for how to enter the interface and network combination to be more intuitive.<br>7. The data grid in the Web User Interface now displays information for simple objects as tooltip (an example is a reference to an IP4Address which would show the address value as a tooltip). |
| 2.26.02 | *[DFL-210/260/800/860/1600/1660/2500/2560/2560G]*<br>1. Added the possibility to disable and enable Ethernet interfaces using WebUser Interface.<br>2. Separate icon for User Authentication enabled objects.<br>3. Improved file names for backup packages, including the configuration |

| | |
|---|---|
| | version number.<br>4. Connection Rate Statistic Values can be viewed using SNMP. |
| 2.26.01 | *[DFL-210/260/800/860/1600/1660/2500/2560/2560G]*<br>1. The name of the authenticated user is logged together with the requested URL in HTTP ALG log messages<br><br>*[DFL-160]*<br>1. DHCP relaying through the firewall in transparent mode is supported<br>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<br>2. DFL-210 and DFL-800 support anti-virus and dynamic web content filtering |
| 2.25.01.28 | No new features in this version.<br>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<br>2. Improved logging for Anti-SPAM<br>3. New log message at failover triggered by linkmon<br>4. A new advanced setting has been added to control the number of RADIUScommunication contexts that can be used simultaneously<br>5. DNS name resolving uses the shared IP in High Availability setups<br>6. Added support for Host Monitor for Routing<br>7. Added command to handle language files on disk<br>8. Improved LDAP functionality<br>9. Redesign of the tuple value controller in the webUI<br>10. Display of network objects<br>11. Extended route monitoring capabilities<br>12. The IPsec status page has been improved<br>13. PCAP Recording<br>14. New advisory link in virus found log messages<br>15. The webUI has been extended to handle child objects in a tab<br>16. Support of custom monitor interval in Linkmonitor<br>17. ZoneDefense now supports DGS-3200 series switches<br>18. Anti-Virus triggered ZoneDefense<br>19. LDAP Authentication<br>20. Route Load Balancing<br>21. Extended SIP Application Layer Gateway supporting new scenarios<br>22. TCP transport added to the SIP Application Layer Gateway |

| | |
|---|---|
| | 23. Multiple media connections for SIP Application Layer Gateway<br>24. PPTP server support for multiple PPTP clients behind the same NAT gateway<br>25. PPTP server and client have been extended to support stateful MPPE<br>26. Improved verification of IP4 values<br>27. IDP Triggered Traffic Shaping<br>28. AVSE_MaxMemory setting has been removed<br>29. Relayer IP address filter at DHCP Server<br>30. Support for VLAN priority derived from IP DSCP precedence<br>31. Gigabit Traffic Shaping Support<br>32. The PPPoE client has been changed to support unnumbered PPPoE<br>33. Improved server monitoring for Server Load Balancing<br>34. The ping CLI command has been improved<br>35. The schedule page has been improved<br>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<br>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 |
|---|---|
| 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.<br>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.<br>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.<br>4. IPsec performance sometimes degraded over time. Affected models: DFL-260E and DFL-860E.<br>5. Some configurations involving the PPTP ALG could cause the firewall to make an unexpected restart.<br>6. The application control engine could not completely block Google Drive, when an application rule set was configured to do so.<br>7. On rare occasions there was an unexpected restart with certain IPsec traffic.<br>8. Connection timeouts created from service objects with custom timeout values were not properly synchronized between High Availability cluster peers.<br>9. The packet buffers managing IPsec traffic were not optimized.<br>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.<br>11. Download of certain files failed when using the HTTP ALG configured to do Anti-Virus scanning.<br>12. Email Control blacklist and whitelist filters did in some cases not match correctly.<br>13. The OSPF subsystem in a High Availability setup sometimes caused the system to restart unexpectedly.<br>14. The firewall sent UDP encapsulation mode in the IPsec proposal even when NAT-Traversal on the IPsec tunnel was set to OFF.<br>15. When receiving traffic through the IMAP ALG, the system sometimes rebooted unexpectedly.<br>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.<br>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.<br>31. Some packets generated by the firewall could get an erroneous hardware address when routed through a switch route.<br>32. An Anti-Virus signature update interrupted by a reconfiguration needed a manual update to resume the download after the unit finished configuring.<br>33. Upgrading from versions prior to 11.00 to 11.00 and later versions, could in rare occasions fail with a configuration error.<br>34. On rare occasions the firewall could restart unexpectedly when errors occurred in the connection with the SSL VPN client.<br>35. When using Anti-Virus scanning on IMAP traffic, emails with deeply nested and/or encrypted zip attachments were not forwarded correctly.<br>36. Some VoIP scenarios did not work as intended when using IP Policies and VoIP Profiles.<br>37. Connection failures when updating the Anti-Virus databases implied a restart of the whole updating process.<br>38. Cloning a read-only object in the WebUI did not copy any values from the original object.<br>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.<br>40. The system did not respond to Dead Peer Detection messages in some cases when the IKE Security Association was about to expire.<br>41. It was not possible to upload a configuration backup using Safari as web browser.<br>42. Running the ping CLI command with certain parameters could make the firewall perform an unexpected restart.<br>43. The "%URL%" variable was not correctly substituted in some built in HTTP banner files.<br>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.<br>45. POP3 connections could become unresponsive in rare cases.<br>46. The NATPool subsystem did not use the full configured IP-range.<br>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.<br>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.<br>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.<br>51. Dead Peer Detection for IPsec tunnels using XAuth was in rare occasions not initiated.<br>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.<br>53. Under special circumstances the firewall reported the wrong number of Anti-Virus signatures loaded in memory.<br>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.<br>55. Some non-standard IMAP extensions were not supported.<br>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.<br>57. POP3 message transactions did not complete successfully in some cases.<br>58. Plain text email attachments were not scanned for viruses when using IMAP.<br>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.<br>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.<br>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.<br>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.<br>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).<br>64. ESP traffic was sometimes incorrectly routed into the IPsec tunnel.<br>65. Some methods of downloading E-Mail data using IMAP did not work as intended.<br>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.<br>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.<br>69. Brute force history was lost after reconfiguration.<br>70. Certificates could not be successfully downloaded using scp.<br>71. Some E-Mails with incorrect MIME formatting were not forwarded correctly.<br>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.<br>73. Some log events were missing for the Authentication Agent and the REST API users.<br>74. The WebUI was missing some Anti-Virus settings for an IP Policy.<br>75. TCP packets inside of certain ICMP and ICMPv6 errors could in some scenarios contain faulty SEQ and ACK numbers.<br>76. E-Mails containing empty MIME body parts could in some cases not pass through the POP3 content scanner.<br>77. In some scenarios when the HTTP ALG was used on IPv6 traffic, path MTU discovery did not work.<br>78. There was a column miss alignment in the output of the CLI command "routemon".<br>79. In rare occasions, the POP3 ALG made mail fetching time out.<br>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.<br>81. On rare occasions, the firewall could make an unexpected reboot when using the HTTP ALG.<br>82. Some E-Mails with message attachments were not forwarded correctly by the IMAP content scanner.<br>83. The firewall could make an unexpected restart with certain configurations containing a Policy Based Routing rule.<br>84. Some rare E-Mail messages were not forwarded correctly by the POP3 content scanner.<br>85. The individual NAT Pool CLI overview could show the wrong number of flows associated with it.<br>86. The stateful NAT Pool didn't correctly restrict the number of states according to the configured maximum limit.<br>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.<br>88. The schedule feature was never applied in NetDefendOS 11.04.00 even though it was configured.<br>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.<br>90. The remote management SSH session could get interrupted during reconfigure when the primary authentication source was RADIUS.<br>91. Certain types of faulty ESP packets could cause undefined behavior on platforms using a hardware accelerator for IPsec encryption/decryption.<br>92. IMAP scanning could lead to unintended behavior if not all data was available.<br>93. Some E-Mail headers could not be downloaded using the IMAP ALG.<br>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.<br>95. E-Mails containing empty MIME body parts could in some cases not pass through the POP3 content scanner.<br>96. It was not possible to configure a SAT policy to single IP policy because of a missing UI element.<br>97. Update center did not remove a corrupted IDP signature database.<br>98. Log messages for ESP packets that failed to decrypt could generate logs with the wrong reason for the failure.<br>99. In rare occasions there could be an unexpected restart for traffic going through the SIP ALG.<br>100. Certain rare E-Mails were not interpreted correctly by the POP3 content scanner, which could cause detection errors.<br>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.<br>102. The firewall generated invalid DNS queries in some rare cases.<br>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.<br>104. The HTTP Poster did not auto update the IP address properly.<br>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.<br>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.<br>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.<br>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.<br>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.<br>111. IPsec performance sometimes degraded over time. Affected models: DFL-260E and DFL-860E.<br>112. Some configurations involving the PPTP ALG could cause the firewall to make an unexpected restart.<br>113. The application control engine could not completely block Google Drive, when an application rule set was configured to do so.<br>114. On rare occasions there was an unexpected restart with certain IPsec traffic.<br>115. Connection timeouts created from service objects with custom timeout values were not properly synchronized between High Availability cluster peers.<br>116. The packet buffers managing IPsec traffic were not optimized.<br>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.<br>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.<br>119. Download of certain files failed when using the HTTP ALG configured to do Anti-Virus scanning.<br>120. Email Control blacklist and whitelist filters did in some cases not match correctly.<br>121. Under certain conditions the IMAP ALG could cause an unexpected restart of the firewall.<br>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.<br>132. Some email messages with nested multiparts were corrupted when using POP3 or SMTP content inspection.<br>133. Tab completion for the Ping CLI command did not work correctly.<br>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.<br>135. The system could restart unexpectedly when removing all IPsec connections with the "killsa" CLI command.<br>136. Under certain rare circumstances it was not possible to download a backup of the working configuration from the firewall.<br>137. The HA log messages with ID 616, 617 and 618 used the wrong syntax for describing the event.<br>138. The SMTP ALG sometimes incorrectly marked mail sent with the Outlook Mail client as spam.<br>139. The system did not terminate the previous PPPoE session when PPPoE settings were changed.<br>140. Disabling the usage of legacy IPRules would also disable Threshold, Pipe, IDP and Routing rules.<br>141. Disabling usage of legacy IPRules would not disable IPRules in IPRuleSets.<br>142. IPsec tunnel setup rate was slow and caused high CPU load in certain large setups that contained a large number of IPsec tunnels.<br>143. Some packets generated by the firewall could get an erroneous hardware address when routed through a switch route.<br>144. An Anti-Virus signature update interrupted by a reconfiguration needed a manual update to resume the download after the unit finished configuring.<br>145. Upgrading from versions prior to 11.00 to 11.00 and later versions, could in rare occasions fail with a configuration error.<br>146. On rare occasions the firewall could restart unexpectedly when errors occurred in the connection with the SSL VPN client.<br>147. When using Anti-Virus scanning on IMAP traffic, emails with deeply nested and/or encrypted zip attachments were not forwarded correctly.<br>148. Some VoIP scenarios did not work as intended when using IP Policies and VoIP Profiles.<br>149. Connection failures when updating the Anti-Virus databases implied a restart of the whole updating process.<br>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.<br>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".<br>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.<br>3. In rare occasions when using the PPTP ALG an incorrect ALG associated connection could be closed, resulting in unexpected behavior.<br>4. OSPF "point-to-multipoint" interfaces didn't allow for more than one neighbor to be configured.<br>5. OSPF "point-to-multipoint" interfaces discovered neighbors using multicast instead of unicast.<br>6. OSPF "point-to-multipoint" interfaces created an invalid "dummy" route for the interface IP.<br>7. An Ethernet interface with a manually assigned MAC address would revert to its original MAC address after issuing the console command "ifstat -restart".<br>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.<br>9. The NetDefendOS web authentication feature could fail in some rare situations when the system was under heavy stress.<br>10. The firewall's SNMP statistics could report active IPsec tunnels as "down" under certain circumstances.<br>11. It was not possible to use Interface Groups as the OuterInterface when configuring an SSL VPN interface.<br>12. The H.323 ALG sometimes caused unexpected reboots.<br>13. It was not possible to use the CLI command "ippool -renew" to renew leases.<br>14. An error message is now displayed when trying to save a certificate with the same name as an existing object.<br>15. The E-flag in OSPF could in certain scenarios be set incorrectly which resulted in connectivity problems.<br>16. A large number of applications that were previously unsupported have been added to Application Control feature.<br>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.<br>19. The message shown when trying to log in with a user with insufficient privileges was not descriptive enough.<br>20. The Advanced TCP Setting for CC (Connection Count) option was incorrectly named<br>"TCP Option Connection Timeout" in the WebUI.<br>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.<br>22. The configuration warning message "Shared IP address cannot be equal to iface IP address" was missing the name of the offending interface.<br>23. Non pertinent information was displayed in the console command "appcontrol -show_lists".<br>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.<br>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.<br>26. Comments were not visible on folders in the WebUI address book.<br>27. DHCP Relay did not forward DHCPACK messages if they were received on port 68.<br>28. Some scenarios with static route insertion/removal through OSPF did not work in a High Availability setup.<br>29. Values for advanced IPsec settings "DPDExpireTime" and "DPDKeepTime" were missing from the WebUI and could only be changed using the CLI.<br>30. Some HTTP operations could under certain situations result in second long lockups.<br>31. NAT-T Vendor ID was sent even when NAT-T setting on IPsec tunnel was set to OFF.<br>32. The firewall could in rare occasions reboot unexpectedly when checking IPsec connections during a reconfiguration.<br>33. DHCP Server configured with "Relayer Filter" erroneously dropped the unicast DHCP request/renewal messages from DHCP clients.<br>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.<br>35. TCP segments with RST flag did not have 0x00000000 as acknowledge number.<br>36. Interoperability issues regarding NAT-T sometimes caused IPsec traffic to be incorrectly dropped.<br>37. After receiving large LSA, the OSPF module reported memory error despite having enough available memory to use.<br>38. Some log messages did not correctly display the access_level for some users.<br>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.<br>40. Some rare URLs were incorrectly forbidden by the Web Content Filtering (WCF) functionality.<br>41. The H323 ALG could in rare occasions cause a system reboot.<br>42. ICMPv6 error message "Packet too big" was not passed through NetDefendOS causing traffic to be blocked in certain scenarios.<br>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.<br>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.<br>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.<br>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.<br>47. There were no warnings about changed IPRules or IPPolicies due to configuration changes.<br>48. ZoneDefense did not log the unblocking events.<br>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.<br>50. The span for the Update Center's Hourly setting was not correct and has been |

| | |
|---|---|
| | changed from 11 to 12 hours.<br>51. When using the "Hourly" interval for Update Center the updates ran every hour despite the setting's value.<br>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.<br>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.<br>54. Spaces in passwords were incorrectly interpreted as '+'-signs when using Web Authentication.<br>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.<br>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.<br>57. Using certain addresses as IPv6AddressPool in the DHCPv6 Server caused the system to not give out any IP addresses.<br>58. IPsec tunnel setup could fail with certain configurations despite matching IPsec proposals.<br>59. The system sometimes experienced high memory consumption and sometimes rebooted due to low available memory when using IDP.<br>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.<br>61. There was no log or notification shown when IDP scanning was disabled because of the license expiration.<br>62. Received ICMPv6/Neighbor Advertisements containing multiple options were incorrectly interpreted by the firewall.<br>63. L2TP/IPsec traffic to multiple clients behind the same NAT device could in rare scenarios be mixed up.<br>64. Full system backup files did not include files related to SSL VPN and Application Control.<br>65. Connecting a second L2TP Client located behind a NAT gateway could in rare occasions disconnect the first client.<br>66. In rare occasions, the SMTP and POP3 ALG configured with Anti-Virus did not detect malicious email attachments.<br>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.<br>69. Blacklist logs sometimes showed incorrect protocol or port.<br>70. Memory usage for SIP was displayed incorrectly.<br>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.<br>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.<br>2. Fragmented traffic sent through an IPsec tunnel was sometimes dropped.<br>3. No error was generated when configuring HTTPS management without selecting an HTTPS certificate.<br>4. The Router Advertisement related settings had inconsistent naming. The names have been updated and a configuration converter has been added so that existing behavior is kept after upgrade.<br>5. IPsec interfaces could not be used by OSPF to communicate with a neighbor.<br>6. Connections using the secondary route in a route monitor setup where the primary route had failed were incorrectly closed during reconfiguration.<br>7. A firewall with User Identity Awareness configured could in rare scenarios reboot unexpectedly.<br>8. Memory consumption could in rare circumstances increase when an authenticated user timed out from a RADIUS server.<br>9. Configuring OSPF to run on top of VLAN interfaces did not set the VLAN's Ethernet base interface's receive mode parameter to accept OSPF multicast packets, causing OSPF communication fail in some scenarios.<br>10. The Web User Interface selection box was not wide enough, which made long object names not being displayed in full.<br>11. Error messages output by the "time -sync" command were in some failure cases not informative enough to describe the problem.<br>12. On rare occasions, the firewall could perform an unexpected restart after reconfiguring a PPTP server that used LDAP authentication.<br>13. Configuring an IPv6 core route would always cause a configuration warning.<br>14. Traffic passing through an IPsec tunnel was sometimes incorrectly dropped if there was fragmentation of the packets.<br>15. Valid UTF-8 characters were in some logs not shown properly.<br>16. UDP packets sent from the firewall when using the ping CLI command always had the same Fragmentation ID or Identification field set.<br>17. The output from the "time -sync" command was shown in all active CLI |

| | |
|---|---|
| | sessions. It will now only appear in the session where the command was executed.<br>18. The description of the Facility parameter in the Syslog Receiver configuration object was incorrect.<br>19. The device could restart unexpectedly when Application Control was disabled on an IPRule matching active IPv6 traffic<br>20. Certain rare certificates could not be added to the configuration.<br>21. Web Content Filtering did not work for HTTPS when the traffic was directed to a proxy.<br>22. Descriptions were missing for some advanced settings alternatives.<br>23. The DHCP Server Custom Option parameter value was possible to leave empty, but gave an error message during Save & Activate. An error message is now shown if the value is left empty when clicking Ok on the Custom Option page.<br>24. Application Control frequently failed to recognize Skype. Changes have been made to improve the classification of Skype.<br>25. Application Control sometimes identified the application as just TCP or just UDP.<br>26. Using an IP4Address object with a DNS name as Remote Endpoint for an IPsec tunnel could lead to IPsec traffic problems.<br>27. In rare occasions, some applications, such as Skype or RDP, could not be allowed by Application Control.<br>28. The background colors of the row on the connection page in the Web UI were not alternating after a filter had been applied.<br>29. Traffic using routing rules with routing tables where the "Ordering" setting was set to "Default" was sometimes routed incorrectly.<br>30. Accessing certain HTTPS sites sometimes failed if the HTTP ALG was configured to do Web Content Filtering.<br>31. The classified value in the Application Control statistics table suffered from duplicate and premature updates. This has been fixed, so, it is normal to expect a lower rate of updates after a firmware upgrade.<br>32. Safe Search configured together with Web Content Filtering sometimes caused system reboot.<br>33. Removing a large number of IPsec tunnels from the configuration could cause the system to restart.<br>34. Application Control Rules would, with certain selected applications, take longer time than necessary to parse during reconfiguration. |
| 2.60.02 | 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.<br>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.<br>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.<br>4. The statistics value for connections in TCP_FIN state incorrectly also included TCP_OPEN.<br>5. Long pipe names would disrupt the format of the CLI command "pipes -show".<br>6. The VLAN interface statistics was reset on each reconfiguration.<br>7. DHCP relay packets received on interfaces without configured DHCP relay could in some configuration scenarios be dropped.<br>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.<br>9. Enabling IPv6 on a VLAN interface with IPv6 disabled in the global settings did not produce a configuration warning.<br>10. Route monitoring using link status did not recover a disabled route after a reconfigure had been issued.<br>11. Keep-alive set to "Auto" did not work on IPsec tunnels where the Remote Endpoint was a DNS name.<br>12. SSH CLI sessions could not handle large amount of data being pasted or piped into the session.<br>13. Connections scanned by IDP were sometimes broken at HA cluster configuration deployment.<br>14. In the WebUI's L2TP/PPTP client page there was no way of configuring the Originator IP Type or Originator IP.<br>15. It was not possible to change the index of an interface route that was created automatically by the system using the CLI.<br>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.<br>17. The Application Control feature did not recognize the Sohu Video application correctly.<br>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.<br>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.<br>20. The "dhcpserver" CLI command did not obey the -num or -fromentry options in combination with the -mappings flag.<br>21. The firewall would in some cases fail to update its ND cache after receiving a valid Neighbor Solicitation.<br>22. IPv6 network address validation in the WebUI did not allow the usage of network size of 100 and larger.<br>23. It was not possible to use a DNS object from the address book on the L2TP/PPTP client's remote endpoint.<br>24. Some of the filter options in the *Status->Run-time information->Connections* page were not applied when selected.<br>25. The CLI command "sipalg -connection" did not show information under the appropriate columns.<br>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.<br>27. Users authenticated by an Identity Awareness Agent were not synchronized to the inactive node in an HA cluster.<br>28. In certain SIP configuration scenarios the SIP ALG could cause an unexpected reboot of the firewall.<br>29. Users could be logged out if a large number of PPTP clients were trying to connect simultaneously.<br>30. The SIP vendor Aastra was not supported by the SIP ALG.<br>31. The SIP ALG's CLI command "sip -registration flush" did not work.<br>32. Unreachable RADIUS Accounting servers could in rare cases cause undefined behavior.<br>33. No log was generated when an L2TP session was closed.<br>34. The SIP ALG's CLI command "sip -statistics flush" did not work.<br>35. Valid Neighbor Discovery packets would always cause the interface drop statistics to increase.<br>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.<br>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.<br>38. A help text in the HTTP ALG incorrectly mentioned that URL Filter was not supported for the HTTPS protocol.<br>39. Polling the SNMP property if Alias would, for certain interface types, not return the comment configured for the interface.<br>40. Configuration backup restore failed if the backup file contained an additional line break at the end of the configuration file.<br>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.<br>42. In rare circumstances during HA hand-over, the inactive HA node could erroneously send neighbor solicitations for its own shared IP.<br>43. There was no error or warning generated when trying to configure switchroutes in an HA cluster.<br>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.<br>45. There were no logs about destination port, destination IP or name of SSL VPN interface for incoming SSL VPN connections.<br>46. It is now possible to use "route" as an alias to the CLI command "routes".<br>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.<br>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).<br>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.<br>50. On systems with multiple active IPsec tunnels, configured to add dynamic routes, the memory usage increased for every reconfiguration.<br>51. Memory management in configurations with IPsec where Xauth and RADIUS was used was not always correctly done.<br>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.<br>54. The system could in rare occasions restart unexpectedly when doing configuration changes related to IPsec tunnel(s) that uses XAuth for authentication.<br>55. Extensive memory usage occurred after a very large number of users having been logged in to system.<br>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.<br>57. It was possible to add an Authentication Agent object without specifying a name for it.<br>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.<br>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.<br>60. The PPTP subsystem could in rare circumstances cause unexpected system reboots.<br>61. The CLI command "ifstat" omitted a line break at the end of the output for certain types of interfaces.<br>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.<br>63. There was no warning issued if the user added an IPv6 route and IPv6 had not been enabled in the configuration.<br>64. ncorrect or outdated RADIUS Accounting responses could cause an increase in memory consumption.<br>65. The "pcapdump" functionality couldn't capture the outgoing packets flowing through a VLAN when the capturing target was its base interface.<br>66. On rare occasions, the firewall restarted unexpectedly when performing a reconfiguration following a previous IDP database update.<br>67. The last part of an ICMP packet sent through an IPsec tunnel was sometimes dropped.<br>68. IPv6 groups would in certain rare cases create wrong IPv6 address ranges.<br>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.<br>71. Users being logged out after a timeout could in some rare cases appear to log out multiple times.<br>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.<br>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.<br>74. It was not possible to configure two or more SSL VPN interfaces with the same server IP and port.<br>75. The firewall might experience unexpected behavior when reporting IDP events using SMTP LogReceiver under certain specific circumstances.<br>76. L2TP client behind NAT using L2TP/IPsec transport mode tunnel did not always succeed in reestablishing the L2TP tunnel.<br>77. Using RADIUS accounting could under certain rare conditions lead to system instability.<br>78. In rare occasions when an IPsec configuration was updated, the firewall could restart or stop responding unexpectedly.<br>79. The MTU for VLAN interfaces was calculated incorrectly, causing unnecessary ICMPv6 PacketTooBig error messages.<br>80. The invalid_ip_checksum log message did not correctly list the actual and expected checksums as intended.<br>81. CRL lookup over LDAP did not work if the URL for the CRL distribution point did not contain the port.<br>82. The ping command could in some rare cases report an incorrect round-trip time.<br>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.<br>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.<br>85. The CLI prompt was not shown after the "pipes -show" CLI command.<br>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.<br>121. Certain web pages were not possible to reach or load when using the HTTPS ALG.<br>122. POP3 ALG log messages would sometimes contain incorrect e-mail addresses.<br>123. On rare occasions, the SMTP and POP3 ALGs could not read fields from the DataHeader correctly.<br>124. The firewall could perform an unexpected restart in case an up and running PPPoE tunnel was disabled by the user.<br>125. The DHCP Client did not renew its IP address lease after a link failure had been restored.<br>126. The firewall would incorrectly terminate some HTTPS sessions when using an HTTP ALG with HTTPS, resulting in a blank page in some browsers.<br>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.<br>128. The community string in SNMP Remote Management was truncated if it was longer than 32 characters.<br>129. Unsolicited ARP reply was not handled correctly according to the Unsolicited ARPReplies setting.<br>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.<br>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.<br>132. The L2TPv3 Server leaked a small amount of memory when a new session was initiated within an established tunnel.<br>133. Certain SIP PBX configurations caused the firewall to drop INVITE requests.<br>134. In rare occasions when SIP was reconfigured, the firewall could make an unexpected restart.<br>135. Some characters were not supported in passwords for users being authenticated using LDAP as source.<br>136. It was possible to configure multiple static DHCP hosts with the same IP or MAC address without getting a configuration warning.<br>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.<br>174. Changing an IDP Rule Action setting from Action "Protect" and "Dynamic Black Listing" enabled to Action "Audit" left the "Dynamic Black Listing" enabled.<br>175. IPsec Transport mode clients using the same remote ID behind NAT devices failed to connect simultaneously.<br>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.<br>177. The SSL VPN Portal would sometimes not use the same authentication method as the SSL VPN Client when RADIUS authentication was enabled.<br>178. In rare circumstances when using High Availability and OSPF, there could be a flood of OSPF packets on the sync interface.<br>179. A RADIUS Accounting session was closed if the reply from the RADIUS server contained RADIUS Attributes.<br>180. The ifstat CLI command did not show the chip information for some E1000 based interfaces.<br>181. Phase one rekey negotiations in the cases where peer Xauth authentication is required were removed.<br>182. Under rare circumstances, an IPsec configuration could cause the firewall to run out of buffers.<br>183. The traffic shaping subsystem consumed a large amount of CPU resources when processing packets that could not fit within a configured pipe.<br>184. The system could in rare cases perform an unexpected restart when IPsec clients were connected behind a NAT gateway.<br>185. The handling of large amounts of hosts in blacklist has been optimized.<br>186. The clone option was not always available on the WebUI objects.<br>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.<br>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.<br>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.<br>190. In an IPsec scenario where XAuth was used on the tunnel, the memory consumption could in rare circumstances increase unexpectedly after |

| | |
|---|---|
| | renegotiations.<br>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.<br>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<br>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.<br>2. The link status info for the Realtek interfaces disappeared after a reconfigure. Affected models: DFL-260E/DFL-860E<br>3. In some scenarios with IDP configured, traffic of certain patterns could in rare circumstances be delayed<br>4. It was not possible to connect multiple L2TP/IPsec clients behind the same NAT gateway.<br>5. SNMP Interface Alias field was empty when selecting "Comment" in "Interface Alias".<br>6. If L2TP clients with the same local IP address established IPsec tunnels behind a NAT device there were sometimes problems with the connections.<br>7. The OSPF routes database was not updated during reconfigure in some High Availability scenarios.<br>8. In some unusual circumstances the use of XAuth based authentication would lead to an unexpected reboot<br>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.<br>10. The firewall Dynamic Routing Rules did not properly export / import OSPF routes when they were filtered by "OSPF Tag range" or "Router Type".<br>11. A few log message categories, such as SSL VPN and IPv6 Neighbor Discovery were missing from the log message exception list..<br>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.<br>2. The output list from the CLI command 'vlan' was not sorted in VLAN ID order. This has been corrected and the command was enhanced with the parameters to segment long output lists ‘num’ and ‘page’.<br>3. The 'blacklist' CLI command did not set the correct port number and destination URL in its output.<br>4. A configuration with the now obsolete selection of Log And Event Receiver category '36 (USAGE)' would send out empty log data. The configuration is now silently updated to exclude this category.<br>5. The shared IP was not used in LDAP server queries for High Availability cluster nodes.<br>6. The realm string for HTTP basic authentication was incorrectly not optional in the configuration.<br>7. The unit for the OSPF memory max usage in the WebUI was 'kilobytes', but has now been corrected to 'bytes'.<br>8. The Local Gateway configured in an IPsec tunnel was not shown in the CLI command "ipsectunnels -iface" printout.<br>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.<br>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.<br>11. The SIP ALG did not use the "420 Bad Extension" response in certain circumstances.<br>12. The built in L2TP client did not work correctly when put behind a NAT device.<br>13. The configuration was not always updated correctly when upgrading to a newer version.<br>14. HTTPS webauth using Internet Explorer versions 8 and older did not show the logged in page after the user had logged in.<br>15. When using a large number of neighbors in nodes running OSPF, there was a rare possibility of memory corruption.<br>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.<br>2. The log event no_arp (ID:04100007) firewall action text was previously route_enabled, the text is now corrected to route_disabled.<br>3. Time unit 'seconds' added to help texts in WebUI ALG SIP dialog and CLI |

| | |
|---|---|
| | command 'help ALG_SIP'.<br>4. An expired AV or IDP license in an HA environment could trigger unexpected behavior in the inactive cluster node.<br>5. Some web authentication scenarios could lead to unexpected behavior by the firewall.<br>6. The output text for the CLI command 'dns -list' was not formatted correctly when using SSH remote management.<br>7. The firewall did not handle lower and upper case correctly in some configuration scenarios where objects were named almost identically.<br>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.<br>9. Cancelling the HA wizard would result in unexpected behavior of the firewall. Affected models: DFL-260E/860E.<br>10. In rare occasions, closing down a SIP session could lead to an unexpected restart of the firewall.<br>11. The general stability of SSL VPN tunnels has been improved.<br>12. The deployment of new configuration could have a negative impact on the performance of Realtek 8169 interfaces.<br>Affected models: DFL-260E/DFL-860E.<br>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.<br>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.<br>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.<br>16. The CLI "netobject" command incorrectly printed IPv6 addresses in IPv4 format.<br>17. It was not possible to disable sending out High Availablility cluster heartbeats on nodes. The setting was not obeyed.<br>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.<br>20. Using the H323 ALG could in rare circumstances lead to unexpected behavior.<br>21. An error in the configuration module could in rare occasions lead to unexpected behavior during the deployment of a new configuration.<br>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.<br>23. Passwords for newly added users were not encrypted in the configuration file.<br>24. OSPF MD5 authentication misbehaved when using ID other than 2.<br>25. The RADIUS accounting session ID string could under some circumstances be reused for a later session.<br>26. A prompt was not printed in the CLI after activating a new configuration.<br>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.<br>2. The H.323 ALG did not allow FACILITY messages to be sent during the ALERTING state.<br>3. In certain scenarios, traffic originating from LDAP could lead to unexpected behavior by the firewall.<br>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.<br>5. Browsing to certain pages in the WebUI would lead to unexpected behavior for the firewall. Affected models: DFL-260E and DFL-860E.<br>6. Some scenarios made the firewall send malformed packets in an SSL negotiation.<br>7. In a High Availability scenario it was not possible to log in to the firewall in order to download the SSL VPN client.<br>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.<br>9. The possibility to configure interface groups inside interface groups has been added.<br>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.<br>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.<br>12. Large VLAN tagged packets would be dropped by the RealTek R8169 driver. The driver has been updated to handle VLAN packets.<br>Affected models: DFL-260E and DFL-860E.<br>13. The RealTek R8169 interface reported wrong link speed for SNMP. The interface has been updated to report the correct speed.<br>Affected models: DFL-260E and DFL-860E.<br>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.<br>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.<br>2. The source port 20 is occupied when combining the SAT Action in an IP rule with the FTP ALG.<br>3. The CLI commands "reset -configuration" and "reset –unit" show incorrect default management IP.<br>4. SIP ALG would close SIP calls two minutes after the call session was established in some network scenario.<br>5. The "Route Type" in "OSPF Actions" was incorrectly interpreted by the firewall when the configuration was activated.<br>6. An unexpected restart could occur during a configuration deployment when new IPSec tunnels were added to the configuration.<br>7. It was not possible to use all address object combinations in places like routes or in the Address Book.<br>8. The severity for the log message sslvpn_max_sessions_reached was incorrectly set to DEBUG, but has been changed to NOTICE.<br>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.<br>10. The TLS ALG rejected SSL HELLOs with zero or more than one compression method.<br>11. Some cipher suite combinations prevented the AES256 algorithm to be used when establishing SSH administration sessions to the firewall.<br>12. Some specially crafted SDP payloads could cause unexpected reboots of the firewall.<br>13. The edit alternative for Comment Groups was not shown.<br>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.<br>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.<br>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.<br>2. References to UserAuth privileges for authenticated users could change when modifying the number of configured privileges.<br>3. The web server could under certain conditions deadlock and print a "500 - Internal Server Error" message when trying to access the web user interface. The web server has been extended with better error handling to prevent this kind of deadlock.<br>4. The interface traffic counters were only of size 32-bit and often wrapped around when the throughput was high. Corresponding 64-bit counters have been added to ensure that wrapping will not occur as often as the corresponding 32-bit values.<br>5. The block list file verification failed for files with a size smaller than one packet. The blocklist now validates the extension for the first packet when the content type could not be determined in the first packet.<br>6. In certain scenarios, the voice transmitted through the SIP ALG terminated suddenly two minutes after the call was established.<br>7. Office "xlsm" files were blocked by the SMTP ALG. Encrypted "xlsm" files are embedded in an "Office 97/2000 Compatible" container which results in an incorrect file typ according to file integrity control. The file integrity control has been updated to handle encrypted "xlsm" files.<br>8. A faulty model check made the Switch Management not display all the switch ports in the WebUI for the DFL-860E model.<br>9. The Realtek 8169 interface reported link down incorrectly. This caused route monitor to not work properly. Affects: DFL-260E and DFL-860E.<br>10. The HTTP ALG failed to load web pages from certain web servers correctly. The HTTP ALG will now respond with a TCP RESET should the server continue to send packets after the client has closed the connection.<br>11. Anti-virus scanning of zip files containing files with a large compressed size could sometimes lead to unexpected behavior.<br>12. Using HTTP web authentication with a RADIUS server as authentication source, could in very rare scenarios cause the firewall to malfunction during |

| | |
|---|---|
| | save & activate (reconfigure).<br>13. Two HTTP ALGs with the same name, but with different case (e.g. "MYHTTPALG" and "myhttpalg"), could sometimes cause the firewall to freeze during save & activate (reconfigure). |
| 2.27.02 | 1. It was not possible to use User Authentication on IP4Group objects.<br>2. Certain SIP server scenarios in REGISTER transactions made the firewall reject incoming SIP calls.<br>3. In some situations when using SMTP ALG with Anti-Virus e-mails with attachments would not be completely transferred, resulting in a timeout. The ALG Anti-Virus feature now specifically logs failure to decompress encrypted zip files. A setting to allow or deny encrypted zip files have also been added.<br>4. The usage bars on the DHCP Server status page were not displayed correctly when leases reached 100% usage.<br>5. ACK messages for non 2xx PBXs responses were not forwarded by the SIP ALG.<br>6. The DHCP Server did not send DHCP NAK messages in all scenarios. This change speeds up the process of receiving a new IP address lease in these scenarios.<br>7. The SMTP ALG always allowed emails where the SMTP "from" address and email header "from" address did not match. A new setting has been added which allows the administrator to deny or tag these mails as spam.<br>8. CLI command "ipsecdefines" has been removed from "techsupport" command.<br>9. During configuration certain values were not reset after parsing an IGMP Report rule, which made the next IGMP Query misbehave. The configuration values are now properly reset after parsing IGMP Report rules.<br>10. Incoming SIP traffic routed through an IPsec tunnel was discarded by the SIP ALG.<br>11. Some empty configuration values were not written to the configuration. After a restart of the firewall the default values were used instead.<br>12. Some buttons in the web user interface had truncated text.<br>13. The reception of 255.255.255.254 as Framed-IP-Address in a RADIUS negotiation wasn't handled correctly in all installations. Now this will always lead to an IP being assigned, to the PPTP-/L2TP-client, from the configured IP pool.<br>14. It was not possible to click on the IDP signature group links in the web user interface page "IDP Factory Signatures". Clicking on the link now lists the signatures in the group.<br>15. The DNS client always dropped DNS replies that had the truncated bit set. |

| | |
|---|---|
| | The truncated bit indicates that the reply does not contain the complete response and that a new DNS request should be sent using TCP (if the client supports TCP DNS). The DNS client now uses the addresses in the partial response instead of ending up with no address at all. |
| 2.27.01 | 1. Certain SIP PBX configurations blocked media transmission on calls established between devices located on the same interface of the firewall.<br>2. The POP3 ALG did not reset its state after a failed authentication. This could cause the next login attempt to fail.<br>3. Specific Intrusion Detection Protection (IDP) scenarios using hardware acceleration could cause scans to fail.<br>4. Restarting a GRE interface did sometimes trigger an unexpected restart of the firewall.<br>5. The POP3 ALG did not allow Digest-MD5 authentication.<br>6. The SIP ALG could forward malformed SIP messages if a range 0-65535 was used as destination port in the SIP service configuration.<br>7. Specific scenarios using the PPTP ALG could sometimes cause an unexpected restart of the firewall.<br>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.<br>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.<br>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.<br>11. The HTTP ALG MIME type check did not have support for OpenDocument Text Documents (odt).<br>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.<br>2. Certain SIP option messages with high values for the "expires" header field failed to be properly parsed. When that occurred incoming calls to phones |

| | |
|---|---|
| | placed behind the firewall failed.<br>3. Some HTTP headers could cause HTTP connections through the HTTP ALG to be closed down prematurely.<br>4. On DFL-260/ DFL-860, some specific high stressed Intrusion Detection and Protection scenarios using a hardware accelerator could drain the memory of the firewall.<br>5. The SMTP ALG did not accept response codes that only contained numeric data.<br>6. Browsing the Web User Interface over HTTPS would sometimes result in "Error 500 - Internal server error".<br>7. On DFL-1600/DFL-1660/DFL-2500/DFL-2560(G), after a reconfiguration using a HA configuration the interface synchronization list for the Inactive node contained invalid interface references which could cause problems when connections were synchronized before the list was rebuilt. The references are now properly cleared during a reconfiguration.<br>8. In the Web User Interface, when defining an IDP Rule, the check box to enable or disable the option "Protect against insertion/evasion attacks" was not visible.<br>9. The CLI techsupport command always sent a "sesmgr_file_error" log message, even when it worked correctly. The techsupport command now only sends log message when it fails.<br>10. A limitation on the number of simultaneous WebAuth transaction could prevent the authentication of authorized users.<br>11. The IP Rule view in the Web User Interface was slow when viewing large collection of rules. The rendering speed has been improved.<br>12. Dropdown menus in the Web User Interface used a fixed width, which caused objects with long names to push information outsize the window. The dropdowns are now scaled to be able to show all the information. The dropdown also automatically scrolls to the selected item when opened.<br>13. The Mappings and Leases links on the DHCP Server status page in the Web User Interface didn't work.<br>14. Disabling objects with references in the Web User Interface would delete the objects and references instead. The objects are now only disabled when selecting to disable them. |
| 2.26.02 | *[DFL-210/260/800/860/1600/1660/2500/2560/2560G]*<br>1. The "range" parameter in the "rules" CLI command did not work.<br>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.<br>4. When using services with the SYN flood protection (SYN Relay) functionality enabled, reconfigurations could result in unexpected behavior.<br>5. Certain conditions sometimes led to an unexpected behavior when a firewall had IPsec tunnels configured.<br>6. It was not possible to use User Authentication enabled objects in Routing Rules, Threshold Rules, IDP Rules or Pipe Rules.<br>7. The log pages for the Web User Interface were rendered incorrectly resulting in artifacts on some web browsers.<br>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.<br>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.<br>10. The L2TP/PPTP Server overview grid did not have a column for "Server IP".<br>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.<br>12. The validation of the latency setting in the Host Monitor configuration was not correct. The configured value was lowered to an incorrect value.<br>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.<br>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.<br>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.<br><br>*[DFL-160]*<br>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]*<br>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.<br>3. Proposal lists were not properly listed in command line "ipsectunnel -iface" output.<br>4. When using a user authentication rule for HTTPS with LDAP, an SSL socket was sometimes not closed, possibly resulting in instability.<br>5. It was not possible to use certificates that had no alternative name set.<br>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.<br>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.<br>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<br>9. The license page showed an incorrect value for maximum number of PPP tunnels.<br>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.<br>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.<br>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.<br>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.<br>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.<br>15. There was a critical defect in the Web Content Filter functionality that could cause the firewall to reboot unexpectedly.<br><br>*[DFL-160]*<br>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.<br>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.<br>2. Deploying a configuration during heavy traffic load could cause a watchdog reboot.<br>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.<br>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.<br>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.<br>6. It was not possible to move a rule up or down in the list if the rule was disabled.<br>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.<br>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.<br>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.<br>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.<br>11. The SIP-ALG didn't handle "183 Session Message" when initiating a new SIP call.<br>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.<br>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.<br>14. The firewall did not accept certificates signed with RSA-SHA256.<br>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.<br>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.<br>17. It was not possible to connect to the firewall using SSH if lots of public keys were registered in the SSH client.<br>18. The firewall could unexpectedly restart when disabling automatic updates of anti-virus and IDP updates.<br>19. IPsec tunnels with a DNS name as remote endpoint would cease to function after a remote endpoint IP address change.<br>20. Blacklist could potentially write to media up to five times each minute. The delay between possible writes has been increased to two hours.<br>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.<br>22. There was a problem when multiple IPsec SAs referenced the same XAuth context.<br>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.<br>24. The UDP checksum was not correctly updated when the multiplex rule was used together with address translation (SAT SETDEST / NAT).<br>25. On some models, a data alignment error in the Route Load Balancing system could cause the firewall to malfunction.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>2. UpdateCenter caused problems in HA setups, sometimes locking up an HA node. HA alsocaused some problems for pseudo-reassembly<br>3. The behavior of the TCP reassembly has been changed slightly to avoid causing orcontributing to ACK loops<br>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.<br>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.<br>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.<br>8. Redirecting HTTP users to the web authentication login page did not work correctly.<br>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.<br>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.<br>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.<br>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".<br>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).<br>14. Previously, ARP monitoring would be disabled if there was no gateway to monitor.<br>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.<br>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.<br>17. At shut down of the unit, connected SSH clients were not disconnected<br>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.<br>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.<br>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.<br>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.<br>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.<br>23. An HA node sometimes froze and had to be physically rebooted after updating IDP signatures via updatecenter.<br>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.<br>25. Microsoft Windows LT2P over IPsec sessions could fail in the sequence of re-keys.<br>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.<br>26. The User Authentication logs sometimes contained faulty authentication information. Log events were also missing in some authentication scenarios<br>27. A file transfer scanned by the HTTP ALG with anti-virus activated could be aborted after a WindowZero event from the client.<br>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'.<br>29. PCAP captures on non-Ethernet interfaces were missing Ethernet headers causing Wireshark to fail opening the files.<br>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.<br>31. In rare cases, the Web Content Filtering feature could trigger an unexpected restart of the firewall.<br>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.<br>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 '?'.<br>34. Outdated information was sometimes used when generating log events from the ALGs which could cause the device to restart.<br>35. It was not possible to select Local ID for certificates. Added configuration support for Local ID.<br>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.<br>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.<br>38. Changing the high availability setting "use unique shared MAC" could make both nodes of a high availability cluster go active.<br>39. There was a dependency between link monitors which resulted in that the effective ping interval was reduced for each new link monitor configured.<br>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.<br>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.<br>42. Netobject groups were not updated if the groups contained a dynamically changed (DHCP, PPPoE etc.) address.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>51. The firewall did not respond to TCP Keep-Alive packets.<br>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.<br>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.<br>54. IPsec config mode configured with a static IP pool did not, in general, hand out the last address in a range to clients.<br>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.<br>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.<br>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.<br>58. The HTTP-ALG blocked web pages with malformed charset statement in HTTP headers.<br>59. A misconfigured IPsec tunnel could in some scenarios cause the firewall to |

| | |
|---|---|
| | malfunction.<br>60. The firewall sometimes restarted unexpectedly when using IDP Pipes.<br>61. The LDAP client now handles authentication using PPP with CHAP, MS-CHAPv1 and MS-CHAPv2.<br>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.<br>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.<br>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.<br>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.<br>66. The PPPoE client option "Force Unnumbered PPPoE" did not force Unnumbered PPPoE to be used.<br>67. Under certain Traffic Sapping settings, lower precedences stop forwarding traffic when higher precedences start forwarding traffic.<br>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.<br>2. Web authentication and web server connections were not closed correctly at reconfiguration.<br>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).<br>4. HA setups with IDP scanning enabled, packets could be lost during a failover.<br>5. Some services were using the private IP in HA setups for communicating. This is now changed and the shared IP is used.<br>6. The DNS lookup of the IP address to a remote gateway failed under certain circumstances for IPSec interfaces.<br>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.<br>18. Email attachments with very long file names could cause memory corruption in the SMTP-ALG.<br>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.<br>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.<br>21. Connections were, under certain circumstances, incorrectly dropped by the IDP scanning engine when audit mode was used.<br>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.<br>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.<br>24. TCP connections with SYN relay were not synchronized correctly. In case of HA failover, traffic on these connections would freeze.<br>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.<br>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.<br>27. The Fail Mode setting in the HTTP-ALG was not honored by the Dynamic Web Content Filtering.<br>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.<br>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.<br>30. It was not possible to configure the primary NBNS server for L2TP/PPTP server interfaces in the web user interface.<br>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.<br>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.<br>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.<br>34. The description text for IP Pools incorrectly specified that IP Pools could be used by L2TP and PPTP.<br>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.<br>2. Web authentication and web server connections were not closed correctly at reconfiguration.<br>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).<br>4. HA setups with IDP scanning enabled, packets could be lost during a failover.<br>5. Some services were using the private IP in HA setups for communicating. This is now changed and the shared IP is used.<br>6. The DNS lookup of the IP address to a remote gateway failed under certain circumstances for IPSec interfaces.<br>7. The CLI command for displaying updatecenter AV/IDP update status did not show enough information. It has now been improved.<br>8. TCP connections could sometimes fail due to an incorrect sequence number check.<br>9. A missing Content-Transfer-Encoding header field in e-mails could sometimes cause the SMTP-ALG session to malfunction.<br>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.<br>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.<br>12. IP address with suffixes .0 and/or .255 could incorrectly be assigned to IPSec config mode clients.<br>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.<br>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.<br>15. The web user interface, the properties in "Dynamic Black Listing" were incorrectly enabled when action was set to something else than "protect".<br>16. The icon for removing IKE SA was missing, hence making it impossible to remove an IKE SA using the web user interface.<br>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.<br>18. Email attachments with very long file names could cause memory corruption in the SMTP-ALG.<br>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.<br>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.<br>21. Connections were, under certain circumstances, incorrectly dropped by the IDP scanning engine when audit mode was used.<br>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.<br>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.<br>24. TCP connections with SYN relay were not synchronized correctly. In case of HA failover, traffic on these connections would freeze.<br>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.<br>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.<br>27. The Fail Mode setting in the HTTP-ALG was not honored by the Dynamic Web Content Filtering.<br>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.<br>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.<br>30. It was not possible to configure the primary NBNS server for L2TP/PPTP server interfaces in the web user interface.<br>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.<br>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.<br>34. The description text for IP Pools incorrectly specified that IP Pools could be used by L2TP and PPTP.<br>35. A confusing Anti-Virus status message was visible in status page on non UTM capable devices. The message has been removed. |

## Known Issues:

| Firmware Version | Known Issues |
|---|---|
| 11.04.01 | **1. HA: Transparent Mode won't work in HA mode:**<br>There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>**2. HA: No state synchronization for Application Layer Gateways:**<br>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.<br>**3. HA: Tunnels unreachable from inactive node:**<br>The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>• Inactive HA member cannot send log events over tunnels.<br>• Inactive HA member cannot be managed / monitored over tunnels.<br>• OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>**4. HA: No state synchronization for L2TP and PPTP tunnels:**<br>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.<br>**5. HA: No state synchronization for IDP signature scan states:**<br>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:**<br>DFL will not add a switch route for L2TPv3 remote client.<br>**2. Radius server redundancy issue :**<br>DFL will not rollback to primary Radius server till Secondary Radius server is down.<br>**3. Unable to support Radius setting via CLI.** |
| 10.21.02 | **1. HA: Transparent Mode won't work in HA mode:**<br>There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>**2. HA: No state synchronization for Application Layer Gateways:**<br>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.<br>**3. HA: Tunnels unreachable from inactive node:**<br>The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>• Inactive HA member cannot send log events over tunnels.<br>• Inactive HA member cannot be managed / monitored over tunnels.<br>• OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>**4. HA: No state synchronization for L2TP and PPTP tunnels:**<br>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.<br>**5. HA: No state synchronization for IDP signature scan states:**<br>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<br>2. HA: Transparent Mode won't work in HA mode: There is no state |

| | |
|---|---|
| | synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs: No 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.<br>4. HA: Tunnels unreachable from inactive node: The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>A. Inactive HA member cannot send log events over tunnels.<br>B. Inactive HA member cannot be managed / monitored over tunnels.<br>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.<br>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.<br>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.<br>2. The Oray.net Peanut Hull client does not work after they changed the protocol<br>3. HA: Transparent Mode won't work in HA mode: There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>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.<br>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.<br>D. Inactive HA member cannot send log events over tunnels.<br>E. Inactive HA member cannot be managed / monitored over tunnels.<br>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.<br>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.<br>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.<br>2. Don’t support the latest protocol used by oray.net Peanut Hull clients.<br>3. Transparent Mode won’t in HA mode.<br>4. ALGs won’t synchronize states in HA mode.<br>5. L2TP, PPTP, IPSec won’t synchronize states in HA mode.<br>6. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, L2TP and GRE tunnels.<br>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.<br>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.<br>2. Don’t support the latest protocol used by oray.net Peanut Hull clients.<br>3. Transparent Mode won’t in HA mode.<br>4. ALGs won’t synchronize states in HA mode.<br>5. L2TP, PPTP, IPSec won’t synchronize states in HA mode.<br>6. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, |

| | |
|---|---|
| | L2TP and GRE tunnels.<br>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.<br>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.<br>2. Transparent Mode won't in HA mode.<br>3. ALGs won't synchronize states in HA mode.<br>4. L2TP, PPTP, IPSec won't synchronize states in HA mode.<br>5. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, L2TP and GRE tunnels.<br>7. DFL cannot support redirecting L2TP/IPSec tunnels to another DFL working in LAN.<br>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.<br>2. Transparent Mode won't in HA mode.<br>3. ALGs won't synchronize states in HA mode.<br>4. L2TP, PPTP, IPSec won't synchronize states in HA mode.<br>5. The inactive node in an HA cluster cannot be reachable over IPSec, PPTP, L2TP and GRE tunnels.<br>7. DFL cannot support redirecting L2TP/IPSec tunnels to another DFL working in LAN.<br>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<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs. No aspects of ALGs are state synchronized. This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. if, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.<br>4. HA: Tunnels unreachable from inactive node. The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node. |

| | |
|---|---|
| | 5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels. There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states. No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.<br>10. The function "StateKeepAlive" of NAT Pool is not working.<br>11. SIP ALG: Limited functionality on SIP ALG. It supports three scenarios: (a) Protecting local clients - Proxy located on the Internet; (b) Protecting proxy and local clients - Proxy on the same network as clients; (c) Protecting proxy and local clients - Proxy on a DMZ interface. A more detailed description and network topologies can be found in the Admin Guide. Any scenario different from these three might be difficult to deploy.<br>12. SIP ALG: Limited functionality on IP telephony. It is not support all functionality in RFC-3261 or other RFC's that is referred to from RC-3261. There may be third party SIP-aware units that cannot be configured to be compatible with the SIP-ALG. |
| 2.27.02 | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs. No aspects of ALGs are state synchronized. This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. if, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.<br>4. HA: Tunnels unreachable from inactive node. The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>5. Inactive HA member cannot send log events over tunnels. |

| | |
|---|---|
| | 6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels. There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states. No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.<br>10. The function "StateKeepAlive" of NAT Pool is not working. |
| 2.27.01 | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs. No aspects of ALGs are state synchronized. This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. if, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.<br>4. HA: Tunnels unreachable from inactive node. The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels. There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states. No aspects of the |

| | |
|---|---|
| | IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.<br>10. The function "StateKeepAlive" of NAT Pool is not working. |
| 2.27.00 | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs. No aspects of ALGs are state synchronized. This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. if, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.<br>4. HA: Tunnels unreachable from inactive node. The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels. There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states. No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.<br>10. The function "StateKeepAlive" of NAT Pool is not working. |
| 2.26.02 | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs. No aspects of ALGs are state synchronized. This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. if, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated |

| | |
|---|---|
| | transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.<br>4. HA: Tunnels unreachable from inactive node. The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels. There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states. No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.<br>10. The function "StateKeepAlive" of NAT Pool is not working.<br>11. 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<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs. No aspects of ALGs are state synchronized. This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. if, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.<br>4. HA: Tunnels unreachable from inactive node. The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 |

| | |
|---|---|
| | seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels. There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states. No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover. |
| 2.26.00 | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode. There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs. No 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.<br>4. HA: Tunnels unreachable from inactive node. The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels. There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states. No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover. |
| 2.25.01.28 | 1. The Oray.net Peanut Hull client does not work after they changed the protocol<br>2. HA: Transparent Mode won't work in HA mode There is no state |

| | |
|---|---|
| | synchronization for Transparent Mode and there is no loop avoidance.<br>3. HA: No state synchronization for ALGs No 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.<br>4. HA: Tunnels unreachable from inactive node The inactive node in an HA cluster cannot communicate over IPsec, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.<br>5. Inactive HA member cannot send log events over tunnels.<br>6. Inactive HA member cannot be managed / monitored over tunnels.<br>7. OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>8. HA: No state synchronization for L2TP, PPTP and IPsec tunnels There is no state synchronization for L2TP, PPTP and IPsec tunnels. On failover, incoming clients will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.<br>9. HA: No state synchronization for IDP signature scan states No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover. |
| 2.25.01.22 | 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.<br>2. The Oray.net Peanut Hull client does not work after they changed the protocol<br>3. HA: Transparent Mode won't work in HA mode There is no state synchronization for Transparent Mode and there is no loop avoidance.<br>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.<br>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.<br>6. Inactive HA member cannot send log events over tunnels.<br>7. Inactive HA member cannot be managed / monitored over tunnels.<br>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.<br>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.<br>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.<br>2. HA: Transparent Mode won't work in HA modeThere is no state synchronization for Transparent Mode and there is no loop avoidance.<br>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.<br>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.<br>• Inactive HA member cannot send log events over tunnels.<br>• Inactive HA member cannot be managed / monitored over tunnels.<br>• OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.<br>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.<br>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 v11.04.01
- NetDefend Firewall CLI Reference Guide v11.04.01
- NetDefend Firewall Logging Reference Guide v11.04.01
- NetDefend Firewall Application Control Sigs v11.04.01