

Innominate mGuard

Version 5.1.6 - Release Notes

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin, Germany
Tel.: +49 30 921028-0
e-mail: contact@innominate.com
<http://www.innominate.com/>

Copyright © 2003-2009 Innominate Security Technologies AG

November 2009

“Innominate” and “mGuard” are registered trademarks of the Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.

mGuard technology is protected by the German patents #10138865 and #10305413. Further national and international patent applications are pending.

No part of this documentation may be reproduced or transmitted in any form, by any means without prior written permission of the publisher.

All information contained in this documentation is subject to change without previous notice. Innominate Security Technologies AG offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes.

In addition, Innominate Security Technologies AG is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.

This documentation may not be photocopied, duplicated or translated into another language, either in part or in whole, without the previous written permission of Innominate Security Technologies AG.

Innominate Document Number: RN205162B09-022

Vertical bars to the left mark significant changes in comparison to the release notes for firmware version 5.1.5.

1 Features of this Release

This section documents the features provided by this release.

1.1 Product Description

1.1.1 Supported Hardware

mGuard Industrial RS

- Rail mountable case
- 24V industrial power supply standard
- Intel IXP42x 533MHz network processor
- One serial V.24 interface
- Built-in modem (optional)
- Built-in ISDN terminal adapter (optional)
- 64MB SDRAM
- 16MB Flash
- Operating temperature 0-55 °C
- Two Ethernet interfaces 10/100Mbit/s, RJ45 plug
- Eight indicator LEDs
- Rescue button
- Signal contact
- Contact for CMD button
- Contact for ACK LED

mGuard Smart/Core

- Ultra Compact Single Board Computer
- Intel IXP42x 533 or 266 MHz network processor
- One serial RS232 interface [mGuard Core only]
- 32MB or 64MB SDRAM
- 16MB FLASH
- Power supply via USB port (5V 500mA DC) or external (110 - 230 V AC)
- Operating temperature 0-70 °C (mGuard Core only) 0-40 °C (mGuard Professional, Enterprise)
- Relative humidity: 20-90%, non condensing
- Two Ethernet interfaces 10/100 Mbit/s
- RJ45 plug, short wire with RJ 45 plug (mGuard Professional, Enterprise)
- RJ45 plug, JST KR plug male (mGuard Core only)
- Three indicator LEDs
- Rescue button
- External power supply, USB power supply

mGuard PCI

- 32bit low profile PCI 3.3V/5V universal card, 66MHz capable
- Intel IXP42x 533 or 266MHz network processor
- One serial RS232 interface

- 32MB or 64MB SDRAM
- 16MB Flash
- PCI bus operation with driver or PoPCI (Power over PCI) mode
- Operating temperature 0-70 °C
- Two Ethernet interfaces 10/100Mbit/s, RJ45 plug
- Four indicator LEDs
- Rescue button

mGuard Blade

- mGuard blade ID-Bus system
- Intel IXP42x 533 or 266MHz network processor
- One serial RS232 interface
- 64MB SDRAM
- 16MB Flash
- Operating temperature 0-40 °C
- Two Ethernet interfaces 10/100Mbit/s, RJ45 plug
- Four indicator LEDs
- Rescue button

EAGLE mGuard/mGuard Industrial

- Rail mountable case
- 24V industrial power supply standard
- Intel IXP42x 533MHz network processor
- One serial V.24 interface
- 64MB SDRAM
- 16MB Flash
- Operating temperature 0-55 °C
- Two Ethernet interfaces 10/100Mbit/s, RJ45 plug
- Seven indicator LEDs
- Rescue button

mGuard Delta

- Compact Single Board Computer
- Intel IXP42x 533 or 266 MHz network processor
- One serial RS232 interface
- 64MB or 128MB SDRAM
- 16MB or 32MB FLASH
- Power supply via external adapter (110 - 230 V AC)
- Operating temperature 0-40 °C
- Relative humidity: 20-90%, non condensing
- One Ethernet interface 10/100 Mbit/s, RJ45 plug
- One integrated 4 port Ethernet switch 10/100 Mbit/s, RJ45 plug
- One indicator LED
- Rescue button

1.1.2 Software

VPN Functionality

- Authentication by Pre-Shared Secret Key
- Authentication by X.509 v3 Certificate
- Authentication by CA Certificate and Subject Filter (optional CRL checking)
- Multi point VPN
- VPN Tunnel Groups Support (license controlled)
- Hub-and-Spoke Support
- IPsec DES Encryption 56 bit
- IPsec Triple DES Encryption 168 bit
- IPsec AES Encryption 128bit, 192bit, 256bit
- Hardware encryption support [AES support depending on processor stepping]
- Tunnel and Transport Mode IPsec
- RSA (up to 4096 bit key)
- MD5 128 bit, SHA-1 160 bit check sum
- Main and Quick Procedure for Internet Key Exchange (IKE)
- Perfect Forward Secrecy (PFS)
- NAT-T Support
- Dead Peer Detection (DPD) per RFC3709
- 1:1 Address Rewriting in Tunnel (local and / or remote network)
- Automatic ARP responses for remote net if it is (rewritten to) a subnet of a local net (router mode)
- L2TP (Layer 2 Tunneling Protocol) Support (license controlled)

Firewall

- Configurable firewall rules for incoming and outgoing traffic with optional logging
- Configurable firewall rules for incoming and outgoing traffic in VPN tunnels with optional logging
- Logging with unique identification of firewall rules
- Generic Sets of Firewall Rules which can be referenced
- Stateful Inspection
- Anti Spoofing
- SYN and ICMP flooding protection
- L2 MAC/Protocol based filtering support (stealth mode)
- Firewall with user authentication feature
- Firewall Redundancy (license controlled)

Networking

- Stealth Modes: single client automatic, single client static, multi-client
- Router Mode
- PPPoE Mode
- PPTP Mode
- Modem Support
- QoS (egress)
- NAT and Port Forwarding

- Static Routing Tables
- Multiple IP addresses on Interfaces
- VLAN support (VLAN tags) in router and stealth mode
- L2 Redundancy (port monitoring) in stealth mode
- optional rewriting of DSCP/TOS values (QoS)

Other Functions

- Automatic Software Update
- Browser Administration
- SSH Administration via Command Line
- PKI support (X.509) for authentication of administrative access
- SNMP Agent v1/2 and v3
- SNMP Traps v1
- Remote Syslog Server Support
- Configuration Profile Handling
- Transparent Bridging
- NTP Support
- DHCP Server and DHCP Relay Agent
- Dynamic DNS Registration
- LLDP Link Layer Discovery Protocol
- Blade: automatic configuration handling by blade controller
- EAGLE mGuard/mGuard Industrial: ACA Auto Configuration Adapter support
- Copy Protected File System
- Hardware Integrity Check
- Software Integrity Check
- Plug and Play Configuration
- Virus protection (optional), see issue “Anti-Virus: operation on hardware with 32MB RAM”

1.2 Changes Since Previous Releases

Due to the severities of CVE-2009-0790, CVE-2009-3547, CVE-2009-3555 Innominate strongly suggests to update every mGuard appliance to firmware versions 7.0.2, 6.1.5 or 5.1.6 respectively.

1.2.1 Changes made between 5.1.5 and 5.1.6

- Fixed Linux kernel NULL pointer dereference: CVE-2009-3547
- Disabled openssl TLS renegotiation: CVE-2009-3555
- Fixed openssl certificate chain validation bypass: CVE-2008-5077
- Fixed ntp stack-based buffer overflow: CVE-2009-0159

All issues handled with version 5.1.6 are also addressed in the 6.1.5 and 7.0.2 releases.

1.2.2 Changes made between 5.1.4 and 5.1.5

- Closed a remote DoS exploit in Openswan: CVE-2009-0790
- Reactivated the support for the encryption algorithm “Null” of the IPsec SA.

All issues handled with version 5.1.5 are also addressed in the 6.1.3 release.

1.2.3 Changes made between 5.1.3 and 5.1.4

- Fixed a security issue in the SNMP daemon, see CVE-2008-4309
- Fixed occasional reboots in stealth modes if the configuration was pulled regularly from a central HTTPS server
- Fixed the operation of the Ethernet interfaces for the stealth modes when a fixed speed with half duplex mode was used; corrects the detection which interface a host is connected to
- Fixed the synchronization of the hardware clock via NTP for the mGuard industrial RS
- Extended the recovery procedure to help if wrong static routes have been defined for the stealth mode

All issues handled with version 5.1.4 are also addressed in the 6.1.2 release.

1.2.4 Changes made between 5.1.2 and 5.1.3

- Fixed security issue in the SNMP daemon, see CVE-2008-0960 or US-CERT VU#878044.
- Fixed rare race condition which caused traffic that should be passed through a VPN channel to be blocked.
- Added security measure to prevent the VPN subsystem (Openswan) from ignoring CA certificates it can't understand.

All issues handled with version 5.1.3 are also addressed in the 6.0.2 release.

1.2.5 Changes made between 5.1.1 and 5.1.2

- Fixed occasional restarts of all VPN connections due to memory access failures caused by Openswan
- Fixed memory leaks in the VPN subsystem
- Fixed Ethernet driver to not stall administrative connections to the mGuard if no other traffic happened and if packets for the connection have to be retransmitted
- Improved the content of the support snapshot in particular for large configurations

1.2.6 Changes made between 5.1.0 and 5.1.1

- Fixed security issues with ClamAV; see CVE-2007-6336
- Fixed local root exploit for linux kernel > 2.6.17, see CVE-2008-0009/10
- Fixed wrong application of static MAU settings after reboot (HDX instead of FDX) for particular scenarios
- Fixed activation of 1:1 NAT as configured for a VPN connection which was initiated via the CMD contact
- Improved robustness of Stealth mode for multiple clients
- Improved SNMP traps for status changes of VPN connections
- Improved Firewall Redundancy with respect to particular scenarios

1.2.7 Changes made between 5.0.1 and 5.1.0

- Added support for ingress Quality of Service (QoS)
- Added specification of packet rates for Quality of Service (ingress and egress)
- Added support for IKE fragmentation to pass VPN through defect routers
- Added support for establishment and supervision of a VPN connection via CMD

- contact and ACK LED (mGuard industrial RS only)
- Added capability to structure firewall rule records (sets of rules) hierarchically; every rule in a rule record can refer to another rule record now
- Added sending of SNMP traps in case of VPN events
- Fixed HTTPS status query via `nph-vpn.cgi` for VPN connections to return “ready” if the connection is ready to establish channels but has not yet established one
- Fixed HTTPS query via `nph-vpn.cgi` to allow activation of VPN connections with the user “user”
- Fixed issue “AES not supported for transport mode VPN channels”

1.2.8 Changes made between 5.0.0 and 5.0.1

- Fixed issue “SHA2 algorithms not supported for VPN with CA based authentication”
- Fixed issue “PuTTY (version 0.59 and 0.60) does not connect reliably”
- Fixed issue “Wrong log prefix for connections established to the mGuard”
- Fixed security issues with the Linux kernel: CVE-2007-2453 and CVE-2007-3642
- Fixed security issues with ClamAV: CVE-2007-2650
- Fixed 1:1 NAT for remote networks of VPN connections
- Fixed Dead Peer Detection (DPD) for multiple connections between same sites
- Fixed dropping of VPN tunnels when configured without number of significant bits for the network address
- Fixed setting of system time for mGuard delta (might have disabled the device's DHCP client – among other effects).

1.2.9 Changes made between 4.2.1 and 5.0.0

- Changed firmware upgrade policy (see „Updating from previous Releases“)
- Upgraded to Linux kernel 2.6
- Added support of egress Quality of Service (QoS)
- Added PKI support for authentication of administrative access (HTTP/SSH)
- Extended PKI support for VPN connections (CA certificates and CRLs)
- Added support for Hub-and-Spoke topologies to VPN settings
- Added support for VPN tunnel groups (license controlled)
- Extended VPN configuration to allow channels to share several settings
- Extended initiation of VPN connections: any initiation scheme can be used in any network mode
- Extended configuration pull feature to support installation of licenses, firmware updates, automatic rollback of configuration profiles and time based scheduling
- Added network mode „modem“ using the serial interface as WAN connection
- Added generic Sets of Firewall Rules
- Added static routing table to stealth modes for traffic generated by the mGuard
- Added auto configuration of client's MAC in static stealth mode
- Fixed reachability of management IP in stealth mode if client is down
- Added optional blocking of TCP connections for which no SYN packet has been seen
- Added tools to the GUI for diagnosis: DNS lookup, ping, traceroute, IKE-ping
- Added centralized proxy settings (HTTP/HTTPS)
- Extended support of special characters in passwords

- Added scheduled PPPoE (DSL) disconnects
- Added optional session timeout for shell access
- Fixed security issues with ClamAV; see CVE-2007-0897 to CVE-2007-0899
- Fixed support of VLAN for the management IP in multi stealth mode
- Fixed pull configuration problems with Microsoft HTTP server

1.3 Updating from previous releases

Updating to 5.1.6 is supported from the 4.2.0, 4.2.1, 4.2.2, 4.2.3, 5.0.0, 5.0.1, 5.1.0, 5.1.1, 5.1.2, 5.1.3, 5.1.4 and 5.1.5 release. Devices still operating with older software versions must either be updated to 4.2.x first or may be installed from scratch using the flash mechanism. Please refer to the User Manual and the information coming with the update file for details.

- The “update-4.2.x-5.1.6” allows to update directly from the listed 4.2.x versions to 5.1.6.
- The “update-5.0.x-5.1.6” allows to update directly from the listed 5.0.x versions to 5.1.6.
- The “update-5.1.x-5.1.6” allows to update directly from the listed 5.1.x versions to 5.1.6.

The “Automatic Update” feature may be used.

- From 4.2.x the 5.1.6 release is automatically chosen when using the “Install next major version” function.
- From 5.0.0 and 5.0.1 the 5.1.6 release is automatically chosen when using the “Install latest minor release” function.
- From 5.1.0, 5.1.1, 5.1.2, 5.1.3, 5.1.4 and 5.1.5 the 5.1.6 release is automatically chosen when using the “Install latest patches” function.

Beginning with firmware 5.0.0, devices having an A0 stepping CPU are no longer supported.

1.3.1 Important update information (updating from 5.0.0, 5.0.1, 5.1.0, 5.1.1, 5.1.2, 5.1.3, 5.1.4 and 5.1.5)

- The update to the 5.1.6 release requires a reboot at the end of the installation. It is recommended to reboot as soon as the update procedure is finished and before making changes to the configuration.
- During the update from 5.0.x and 5.1.x to the 5.1.6 release, the Anti-Virus scanner will be stopped and the Anti-Virus database is moved to a temporary location.
 - Connections normally protected by the Anti-Virus scanner will be blocked while the firmware update is in progress, such that no virus infected content can pass by.
 - During that time clients might display a message reading “Anti-Virus database update is locked and no Anti-Virus database is currently installed”.
 - In rare occasions it is possible, that the Anti-Virus database needs to be erased for the update to pass without errors. The device will then download the database again after the update and reboot, as long as the update schedule is not set to “Never”.
- Any private extensions (like a tcpdump) you might have stored on the mGuard's file system must be removed before the update.

- During the update to the 5.1.6 release VPN channels may be stopped and restarted.
- Devices with 32 MB of RAM cannot be updated from version 5.0.0 with the “Local Update” feature, see issue “Local Update from 5.0.0 not supported for hardware with 32 MB RAM”.
- In rare occasions the message “internal error, failed to open connection to session daemon” might be displayed after pressing the “refresh” button within the update progress window. Please reconnect to the mGuard then using your browser and login again through the new login window.

1.3.2 Important update information (updating from 4.2.0, 4.2.1, 4.2.2 or 4.2.3)

- The update from 4.2.x to 5.1.6 requires a Major Upgrade License to be installed on the device before the update is started, if the device was produced before 2007.
 - To obtain a Major Upgrade License, a Major Upgrade Voucher needs to be purchased and redeemed first.
 - The voucher can be redeemed with the help of the “Management / Licensing” menu while the device is connected to the Internet.
- Any private extensions (like a tcpdump) you might have stored on the mGuard's file system must be removed before the update.
- Because the Linux kernel version 2.4 is replaced by kernel version 2.6, the update behaves differently from former firmware updates:
 - During the update the device becomes unaccessible and blocks network traffic. The update takes approximately 20 minutes. It may take longer for complex configurations.
 - The device reboots two times during the update.
 - VPN connections are terminated at the beginning of the update but they are re-established after the update.
 - An existing Anti-Virus database is deleted during the update and downloaded again after the update is completed. Connections normally protected by the Anti-Virus scanner are blocked during that time.
 - Logs about the update progress are not available.
- Devices with 32 MB of RAM must be updated to a 4.2.2 or 4.2.3 release first if a Local Update needs to be performed.

1.3.3 Important installation information (flashing with 5.1.6)

- Devices which have been shipped with firmware version 2.x.y or earlier need to be flashed or updated to firmware 4.1.x or 4.2.x first to get the boot loader updated.
- Devices produced before 2007 require a Major Upgrade License before the 5.1.6 firmware image can be installed using the flash mechanism.
 - If the device is flashed with 5.1.6 without license its error LED will signal the morse code “SOS” whenever it is started.
 - The Major Upgrade License must be obtained for each device while it still operates firmware version 4.1.x or 4.2.x. Flash it with firmware 4.1.x or 4.2.x first if needed.
 - To obtain a Major Upgrade License, a Major Upgrade Voucher needs to be purchased and redeemed first. The voucher must be cached with the help of the “Edit License Request Form” feature available within the

“Management / Licensing” menu of the device. The device must therefore be connected to the Internet, for example by operating it in auto stealth mode and attaching it to a PC which is connected.

- The Major Upgrade License must be stored as a file.
- The license file needs to be copied to the tftp directory as a file named “licence.lic” in the same directory as the firmware image (file “jffs2.img.p7s”).
- Once a device has been flashed with firmware 5.0.x or 5.1.x successfully further flashing of that device with firmware versions 5.0.x or 5.1.x or older will not require any license file to be present within the tftp directory.
- The installation of the 5.1.6 firmware image (file “jffs2.img.p7s”) must be performed with exactly the file “install.p7s” it was shipped with.
- If a device needs to be downgraded from 5.1.6 to an older firmware version prior to 5.0.0, the file “install.p7s” from 5.1.6 must be used in combination with the older version's file “jffs2.img.p7s”.

1.3.4 Obtaining the update files

As of release 3.0.0 customers must register before downloading the update files for offline download or to access the online update server. Please refer to

http://www.innominate.com/register_software

http://www.innominate.de/register_software.

After registration user and password information is sent. Please note that the update server is operating using the “https” protocol.

2 Identified Issues and Workarounds

Issue “Anti-Virus: update of local virus scanner”

	Description
Synopsis	Update of local virus scanner may fail with mGuard HTTP scan enabled
Symptom	The update/download of a virus scanner installed on one of the client PCs may fail, since the mGuard may detect virus patterns in the signature files and interrupts the download.
Workaround / action	Disable the HTTP-scanning (set Anti-Virus->HTTP-Options->Enable content scanning for HTTP to “No”) for the time of the download or apply a corresponding rule for the download/upload server to allow this traffic to pass unscanned.

Issue “Anti-Virus: active FTP in stealth mode with management IP”

	Description
Synopsis	In stealth mode with management IP the control connection is using the management IP of the mGuard while the data connection shall use the real IP of the client on the protected side. Some FTP servers (known: WU-FTPD) refuse to use different IP addresses for data and control connections with active FTP.
Symptom	The download/upload fails and the port command is rejected with '500 invalid PORT command' or a similar error (and a respective message may be logged on the FTP server).
Workaround / action	Use passive FTP instead.

Issue “Anti-Virus: multi stealth mode with logical subnetting”

	Description
Synopsis	In multi stealth mode the management IP is used by the mGuard to connect to (remote) locations. The Anti-Virus proxy uses this technique to open the connection to the requested server. If this server is located on the <i>same physical</i> network but a <i>different logical</i> network it is possible that the mGuard cannot reach the server from its management IP due to non-overlapping address ranges. In this case the Anti-Virus component fails.
Symptom	The connection attempt fails.
Workaround / action	Set up the list of servers to not include those on such logical subnets by adding the subnets with the “No Scan” option.

Issue “Anti-Virus: false virus detection”

	Description
Synopsis	Update or installation of software fails when loaded from network resources with false virus detection alarms
Symptom	<p>A software or update package shall be installed from a network resource (for example the Internet). The download of the software fails and a virus detection is logged even though no virus is contained in the corresponding resource.</p> <p>This problem has been observed with binary packages for Windows and Linux operating systems.</p> <p>Note: some programs used to install software packages do not issue a suitable warning but just fail without proper diagnostics. Please check the Anti-Virus logs on the mGuard in this case.</p> <p>Note: this issue is equivalent to the issue "Anti-Virus: update of local virus scanner".</p>
Workaround / action	<p>Disable the HTTP-scanning (set Anti-Virus->HTTP-Options->Enable content scanning for HTTP to “No”) for the time of the download or apply a corresponding rule for the download/upload server to allow this traffic to pass unscanned.</p>

Issue “Static Stealth reconfiguration”

	Description
Synopsis	Changes are not correctly picked up in static Stealth Mode
Symptom	When changing the settings in static stealth mode, the changes are not honored after the OK button is pressed.
Workaround / action	Reboot the mGuard after making changes to the static Stealth configuration

Issue “AVP component: freeing connection slot”

	Description
Synopsis	The AVP (Anti Virus Protection) component does only allow a limited number of connections in parallel. Unused HTTP connections may be closed to improve mGuard resource usage.
Symptom	HTTP browsers (Internet Explorer, Opera, Netscape, ...) do open connections in parallel to download embedded information (images). For efficiency reasons these connections are kept open by the browsers (“keep alive” feature) to improve download speed for further pages from the same site. mGuard does only allow a limited number of concurrent virus scanned connections. If a new connection shall be opened and no connection slot is available anymore, mGuard will detect currently unused HTTP connections and close them in order to allow the new connection to succeed. Such event is logged as “freeing connection slot”.
Workaround / action	The ability to surf the Internet is not limited by the resource optimization handling. Most browsers allow to adjust the maximum number of concurrent connections a browser keeps open. The default settings typically will not lead to connection slot shortage.

Issue “No Access To 1.1.1.1 With Management IP Address Set”

	Description
Synopsis	If a management IP address is set in stealth mode(s), access via 1.1.1.1 fails.
Symptom	Access via 1.1.1.1 is not supported in static stealth or multiple client stealth mode, if a management IP address is configured.
Workaround / action	Use the management IP address also from intern (protected port) to access the mGuard.

Issue “Power OK shown late on mGuard Blade”

	Description
Synopsis	The circuit checking the states of the redundant power supply units in the mGuard Blade does include filter capacitances. Due to these capacitances state changes are not signaled immediately. Power failure is signaled with a delay of 3-4 seconds, replacement of a power supply (now OK) is only signaled with a delay of 90 seconds.
Symptom	Display of the state of the power supply may still show failure even after the power supply has been re-enabled for 90s.
Workaround / action	None.

Issue “ICMP failure with transport VPN in Stealth Mode with SNMP”

	Description
Synopsis	ICMP echo requests are not answered through a transport mode VPN connection if the device is in Stealth Mode and SNMP is activated
Symptom	From a remote peer a client protected by an mGuard shall be pinged through a transport mode VPN. The tunnel is up and other traffic succeeds but ICMP echo requests are not answered. This problem only occurs if SNMP is enabled on the mGuard.
Workaround / action	None.

Issue “VPN firewall rule application for wrong tunnel”

	Description
Synopsis	If multiple tunnels are established to the same remote subnet originating from different local subnets, the firewall rules defined for the distinct tunnels are not handled correctly and interfere with each other. This interference only occurs between tunnels to the same remote subnet.
Symptom	Firewall rules intended to be used within one tunnel are applied to connections of another one.
Workaround / action	Use specific rules for the subnets used in the tunnel configuration instead of generic “0.0.0.0/0” type rules.

Issue “Administrative Access From Moved Client in Single Stealth”

	Description
Synopsis	In single stealth auto detect and static modes the client cannot access the mGuard if the client was moved to the extern (unprotected) side.
Symptom	In single stealth mode the mGuard records the client computer's IP and MAC address at the internal (protected) interface and uses it to direct traffic to the client. If the client computer is moved to the extern (unprotected) side and tries to communicate with the mGuard (even using the management IP address) communication is not possible, as the mGuard still tries to direct the traffic to the internal (protected) side.
Workaround / action	Do connect another client computer to the internal (protected) interface so that mGuard can learn new addresses for IP and MAC or reboot the mGuard.

Issue “Traffic bypasses VPN during reconfiguration”

	Description
Synopsis	If a VPN connection is reconfigured (due to configuration changes) traffic may leave the mGuard unencrypted. This does not happen during firmware update. Firmware versions before 4.2.0 are affected unconditionally. Starting with firmware 4.2.0 it can happen under special conditions only: a) in stealth mode combined with transport mode connections and an open outgoing firewall (packet filter) and b) in stealth mode combined with tunnel mode connections, an open outgoing firewall (packet filter) and %any as the remote side it happens if the tunnel had been established and is taken down afterwards (for example by reconfiguration or restart of the peer).
Symptom	Traffic which is intended to be routed through a VPN connection occurs at the mGuard's external interface unencrypted and without VPN specific network translation applied.
Workaround / action	Add specific outgoing firewall rules to the main firewall configuration which drop or reject traffic to the remote networks which must be routed through a VPN connection only. Such rules will not match encrypted VPN traffic because VPN connections have separate firewall configurations.

Issue “Config pull feedback incompatible with IDM 1.1.0 and 1.1.1”

	Description
Synopsis	Starting with firmware 5.0.0 the format of the HTTP queries used by the config pull procedure has changed. The new format cannot be understood by any Innominate Device Manager (IDM) version prior to 1.1.2.
Symptom	If devices operating firmware 5.0.0 are managed with an IDM prior to version 1.1.2, those devices's update status is not displayed correctly within IDM's device overview table. The update status does not change at all.
Workaround / action	Please update your IDM to version 1.1.2 or later.

Issue “Reconfiguration of the firewall does not block existing connections.”

	Description
Synopsis	Reconfiguration of firewall rules and similar changes do not affect established connections. The mGuard uses connection tracking tables to efficiently handle packets associated with connections which have already been accepted by the firewall. Upon reconfiguration of the firewall the connection tracking table is not flushed. Thus once allowed packets associated with established connections may still pass, though the current firewall rules block the establishment of like connections. Once a connection is terminated its related entry is removed from the connection tracking table and further traffic is blocked.
Symptom	Traffic associated with established connections may still pass, though the firewall was reconfigured to block it. New connection attempts are blocked as configured.
Workaround / action	Restart the mGuard after changing firewall rules and other configuration items which have to block traffic.

Issue “Particular self signed certificates not accepted as HTTPS client certificates”

	Description
Synopsis	Self signed certificates can be configured as acceptable certificates “per definition” if they are used by browsers to authenticate administrative access to the mGuard's GUI. Nonetheless such certificates are rejected if the command “openssl verify -CAfile cert.crt -purpose sslclient cert.crt” would verify them as invalid.
Symptom	Access is rejected by the mGuard, although the configured self-signed certificate is used by the browser.
Workaround / action	Create a different certificate having an appropriate or no key usage extension. For hints about which key usage extensions are missing, please check the output of the command “openssl verify -issuer_checks -CAfile cert.crt -purpose sslclient cert.crt“

Issue “Changed Flood Protection Settings delayed for VPN connections”

	Description
Synopsis	When settings are changed within the menu “Network Security / DOS Protection”, these do not become effective for VPN connections immediately, while they do for the incoming and outgoing firewall. The changed settings become effective as soon as VPN connections are restarted.
Symptom	Changed flood protection settings have no effect for established VPN connections.
Workaround / action	Restart the VPN connections or reboot the device.

Issue “Changed 'IPsec MTU' requires a reboot”

	Description
Synopsis	When the configuration for the 'IPsec MTU' (see menu IPsec VPN >> Global) respectively the configuration variable VPN_IPSEC0_MTU is changed it becomes effective only after a reboot of the device.
Symptom	Packets to be sent through a VPN connection are still fragmented according to the old setting. Increasing the setting does not avoid fragmentation prior to encryption (enhances VPN performance) and decreasing it does not avoid fragmentation after encryption (may be needed to traverse NAT devices).
Workaround / action	Reboot the device after changing the value.

Issue “Reconfiguration of VLAN ID not noticed by DHCP server”

	Description
Synopsis	If an mGuard is operated in <i>stealth mode</i> with a <i>DHCP</i> server on the <i>internal interface</i> , a reconfiguration of the VLAN ID is not noticed by the DHCP server. The DHCP server continues to use the old VLAN ID.
Symptom	After reconfiguration of the VLAN ID the internal DHCP server does no longer respond to requests from clients.
Workaround / action	Please disable and re-enable the DHCP server or restart the mGuard after such a configuration change.

Issue “Anti-Virus scanning incompatible with VLAN in multi stealth mode”

	Description
Synopsis	If an mGuard is operated in multi stealth mode, is embedded into a VLAN (VLAN ID assigned to its management IP), and Anti-Virus scanning is enabled for at least one protocol, traffic for the scanned protocols is blocked by the mGuard.
Symptom	Once Anti-Virus scanning is enabled matching connections can no longer be established.
Workaround / action	None

Issue “ICMP only traffic prolongs takeover for layer 2 redundancy”

	Description
Synopsis	If two mGuards are operated in stealth mode with layer 2 redundancy enabled, the takeover of traffic between two hosts may take longer than specified (60 seconds instead of 3) if the traffic between the hosts consist of ICMP packets only.
Symptom	This is a common pitfall when redundancy is tested within a lab: If layer 2 redundancy is tested with ICMP packets only, this does not cause any synchronization of connection tracking tables between the redundant pair of mGuards. It looks like takeover by the slave lasts long once the network connection of the master is broken. Approximately 60 ICMP echo requests are not replied to.
Workaround / action	Use TCP or UDP while testing.

Issue “External DHCP server not operative in multi stealth mode with VLAN”

	Description
Synopsis	If an mGuard is operated in multi stealth mode, has a VLAN ID assigned to its management IP, and is configured to operate a DHCP server on its external interface, the mGuard does not answer DHCP requests originating from the network attached to its external interface.
Symptom	DHCP clients attached to the mGuard's external interface do not receive their IP configuration. DHCP requests are passed on to the internal network.
Workaround / action	Please (continue to) use firmware version 4.2.x if you need to operate a DHCP server within a VLAN environment.

Issue “ Local Update from 5.0.0 not supported for hardware with 32 MB RAM”

	Description
Synopsis	<p>Devices having 32 MB RAM and operating firmware version 5.0.0 cannot be updated to firmware version 5.1.6 with the “Local Update” feature. Devices operating firmware version 5.0.1 or higher are not affected. The local update from 5.0.0 is never started and the firmware remains untouched. In most cases the devices continue their operation properly. In rare cases temporary shortage of memory can cause malfunction and / or the device performs a reboot automatically.</p>
Symptom	<p>Different symptoms are possible upon an update attempt:</p> <ul style="list-style-type: none"> a) The browser displays an otherwise blank page with the message “Gateway broken or unavailable.” But the administrator can log in to the GUI again by pressing the reload button. b) The device performs a reboot automatically before any feedback is sent to the browser. c) The update terminates and after pressing the “refresh” button the following message is displayed within the update window: “The push update method is not supported for devices with 32 MB. Please use the online update method instead.”
Workaround / action	<p>Please reboot your device once if you attempted the “Local Update” for your 32 MB device.</p> <p>Use the “Online Update” or “Automatic Update” feature, use the flash mechanism to install the 5.1.6 release on your device or use the “Local Update” feature to upgrade to 5.0.1 first.</p>

Issue “Identical VPN connections just with different machine cert do no work”

	Description
Synopsis	If several VPN connections (at least two) are configured to use the same settings except for the local machine certificate and if they use a CA-certificate to authenticate remote sides the mGuard might assign incoming connections the wrong way.
Symptom	All incoming VPN connections are always assigned to the first VPN connection which matches the credentials provided by the peer. Thus the mGuard always uses the first machine certificate to authenticate itself to the remote side – even if the remote side is configured to accept the other machine certificate only. The connection attempt fails.
Workaround / action	Please distinguish your remote sites by issuing certificates from a different (sub-)certification authority for them. A different (sub-)CA-certificate is required per VPN connection. Sites to connect to the same connection must use certificates issued by the same CA-Certificate.

Issue “Transport mode VPN with %any as gateway not supported in stealth mode”

	Description
Synopsis	For any stealth mode operation the mGuard does not support the a VPN connection in transport mode with %any as gateway and CA authentication of several peers at once. Such scenarios do work only if just one peer connects.
Symptom	If more than one peer establishes a connection to the same transport mode VPN connection of the mGuard operating in stealth mode then packets might not get through the channel.
Workaround / action	Please use tunnel mode VPN connections.

Issue “Each firewall redundancy pair needs its own internal network”

	Description
Synopsis	If firewall redundancy is used, just one pair of mGuards can be connected to the same internal network.
Symptom	If more than one redundancy pair is connected to the same internal network, then they will not work as specified. One pair may learn information about active network connections from the other pair (and vice versa). This may allow network traffic to pass which actually should be forbidden through firewall rules.
Workaround / action	Connect each firewall redundancy pair to its own internet network.

Issue “mGuard's SNMP implementation is not idempotent”

	Description
Synopsis	SNMP clients are designed to repeat their request to the SNMP server unless the server sends a response in time. The mGuard may take longer to respond and might misunderstand some repeated requests as new requests.
Symptom	The mGuard might process a repeated SNMP request another time. For example with a “delete row” command this may result in several rows being deleted.
Workaround / action	SNMP clients should be configured to use a larger timeout (10 or 20 seconds for example) and they must not repeat requests. For NET SNMP the options “-t” and “-r” can be used. Please see the corresponding manual for details.

Issue “DHCP server does not use the complete dynamic pool”

	Description
Synopsis	If the mGuard acts as DHCP server (for the internal or/and external network) and is configured to assign IP addresses from a dynamic pool, it never uses all the IP addresses from the pool but one less.
Symptom	If all the IP addresses from the dynamic pool but one are assigned, no more IP addresses will be offered to requestors. The following message is logged then: “warning, lease pool is full – OFFER abandoned”. In particular, if the dynamic pool is configured to comprise one IP address only, then no IP address is offered.
Workaround / action	Increase the size of the pool. If the pool should comprise just one IP address, use a static assignment instead.

3 Known Restrictions

- Anti-Virus operation is not supported on devices with 32 MB RAM.
- The Safari browser needs to have all sub-CA certificates installed in their trust store if they are used to authenticate for administrative access to the mGuard via X.509 certificate.
- The same browser instance can not be used to administrate the mGuard with X.509 authentication and to login into the mGuard's user firewall at the same time.
- Configuration of the mGuard via its GUI (web access), via its Command Line Interface (shell access), and via SNMP must not happen concurrently. Concurrent configuration operations via different access methods may cause unexpected results.

4 Documentation Updates / Errata

- Regarding section 6.2.4: All configured update servers need to serve the exact same update files.
- Regarding section 6.4.1: If the network mode is configured to “Modem” or “Built-in modem” and “Dial on demand” set to “yes” please mind that traffic generated by the mGuard will as well cause the modem connection to be established respectively will cause the connection to be prolonged by the idle timeout. The mGuard might generate traffic via the modem for the following occasions:
 - frequently if the mGuard is configured to sync its system time from an external NTP server,
 - sporadically if the mGuard acts as DNS server for any client and needs to perform a DNS query on behalf of it,
 - right after boot if the connection startup is set to “Initiate” for any enabled VPN connection,
 - right after boot if the remote sites VPN gateway is configured as hostname for any enabled VPN connection (the hostname will be looked up via DNS)
 - frequently if VPN connections are established (at least messages for Dead Peer Detection – DPD in short – are sent frequently),
 - frequently if the mGuard is configured to register its external IP address with a dynamic name service (for example DynDNS),
 - frequently if the DynDNS Monitoring is configured for remote VPN gateways,
 - occasionally if SNMP traps are configured to be sent to a remote server,
 - occasionally if remote access to the mGuard via HTTPS, SSH or SNMP is enabled and accepted (the mGuard will send packets in response to connection attempts from any IP address which is granted access by the corresponding firewall rules) and
 - frequently if the “Configuration Pull” feature is configured to fetch a configuration profile from a remote HTTPS server.
- Regarding section 6.6.4: Users can login into the user firewall from IP addresses reachable from the external network interface of the mGuard if the web access to the mGuard is granted from a remote system. If the external network interface is connected to the internet this might mean that a firewall user could login from a dial-up account where he/she gets a temporary IP address assigned. If that user forgets to sign off the next one who gets that IP address assigned might gain access to the same internal sites as the authorized user. Please use this feature with caution.
- Regarding section 7.2: The Recovery Procedure also clears all static routes which may have been defined for the Stealth Mode (cf. section 6.4.1).