

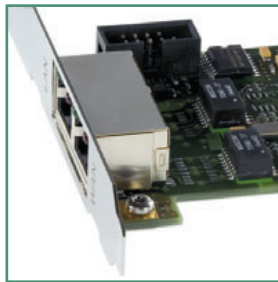
# Innominate **mGuard** Firmware – Major Release 7

## The Embedded Secure Linux System for all mGuard Appliances

### The Innominate mGuard System: Security for Industrial Networks

The Innominate mGuard firmware is the shared core of all mGuard network security appliances. The innovative and yet technically mature system, now avail-

able, is managed by the Innominate Device Manager, and many sophisticated details help to efficiently master the complexity of operation „Industrial Network Security“, providing users with a trouble-free „plug & protect“ experience.



able in major release 7, is the answer to market and customer requirements for security in networked industrial systems, enabling robust functions for everyday practice. The system is integrated in mGuard appliances, which come in various form factors optimized for a range of different environments. It provides autonomous and customized protection to systems requiring decentral endpoint security: in the manufacturing and process industries, in transport and utilities infrastructure applications, and in products of the machine building and plant construction industry. A central device management component,

### More Platforms, and even more Speed

With mGuard 7, Innominate's consequent design efforts for portability and multi-platform support are yielding fruit: the firmware is now available for ARM, x86, and PowerPC processor architectures, making mGuard technology a future-proof investment and most attractive option for embedded security OEM solutions. Already well known for the top-notch performance of its primary security functions, it has undergone further optimization and acceleration of many support functions, letting you flash, rollout, boot, and reconfigure mGuard appliances faster than ever.

### Stateful Packet Inspection Firewall

Based on defined rules, incoming and outgoing data packets can be filtered in both directions, i.e., from external networks into protected internal networks and vice versa. Based on protocols, source addresses and ports as well as destination addresses and ports, network communication can be systematically limited to the extent required for production. In the process, response packets from approved existing connections are recognized and accepted through connection tracking (i.e., the stateful inspection principle). The firewall rules can be structured into hierarchical rule sets, facilitating the configuration of identical protocol groups between various sub-networks.

## Highlights

- Top performance, boots and configures faster than ever
- Stateful Packet Inspection (SPI) Firewall
- Routing with NAT and 1:1 NAT
- Virtual Private Networks (IPsec VPNs) with full PKI support and optional tunneling through TCP and web proxy servers
- Quality of Service (QoS)
- Optional integrity monitoring of Windows file shares against malware infestation
- Plug & protect: optimal network integration through flexible modes of operation
- Parallel or failover communication via Ethernet and serial dial-up connection
- Extremely flexible and accelerated flash and rollout procedure based on DHCP and TFTP
- Configuration and management via central Innominate Device Manager or local WebGUI and command line interface
- Now with multi-platform support for ARM, x86, and PowerPC architectures

## User Firewall

Frequently, network access needs to be limited to authorized users or user groups. If these users work with dynamic IP addresses or from alternating consoles, static firewall rules are not up to the task anymore. The mGuard solution: a „user firewall“, which dynamically activates additional firewall rules for authorized users according to local or RADIUS based authentication using a user- or group-specific template.

## Routing with NAT and 1:1 NAT

The structuring of complex production processes into networked, yet largely independent cells is very common. To ensure these cells or machines are efficiently engineered, documented and operated, it is advantageous to design the IP-based portion of their internal networks homogeneously, in other words, with uniform assignment of identical addresses to each machine of a particular type. If all communication is initiated from the internal cell networks, even multiple of these identical machines can be connected to an operator's production network with simple masquerading NAT routers. If, however, connections are supposed to be initiated from a superordinate network to individual cell nodes, simple NAT is not enough, as the cell nodes would not be addressable from outside. Instead, you need a router which can map internal machine networks completely or selectively onto unique virtual external networks (otherwise unused subnets of the superordinate network) using 1:1 network address translation. Therefore, in addition to plain NAT routing, Innominate's mGuard firmware also performs this 1:1 NAT routing function.

## Virtual Private Networks (VPNs)

The mGuard firmware enables VPN connections to be set up in every network mode and to every mGuard interface based on the open and internationally established Internet standard IPsec. Where available, it supports hardware-accelerated encryption to achieve outstanding VPN data throughput. IKE fragmentation support ensures that connections are reliably established, even for transmissions with UDP fragment losses. And for scenarios with restricted Internet

access, mGuard VPN connections can even be tunneled through arbitrary TCP ports and web proxy servers with authentication. As another distinctive feature, mGuard allows to apply dedicated firewall rules within each VPN tunnel to filter respective data traffic. VPN connections can be (de)activated by a choice of software interface or electrical switching contact – ideal for equipping or retrofitting machinery and equipment for secure remote maintenance via the Internet.

## Public Key Infrastructures (PKIs)

The mGuard firmware distinguishes itself through full-fledged public key infrastructure support. Certificates for use on a specific appliance or from trusted remote stations, as well as from signing certificate authorities (CAs), can be managed and used for authentication. Certificate revocation lists (CRLs) can also be taken into account. In addition, the temporal validity of certificates and CRLs can be verified.

## Quality of Service (QoS)

QoS functionality allows the data packet rates or bandwidth of traffic through an mGuard appliance to be limited to the degree necessary, thus enabling connecting paths and components involved in the communication to reliably transmit and process data. If respective thresholds are exceeded, QoS ensures appropriate prioritization of data packets and can also guarantee minimum throughput rates for defined protocols – ensuring that time-critical connections are not disturbed by less important data let alone by deliberately damaging packets involved in a network attack. This makes QoS suitable for the protection of controls that are at risk of overload and for bandwidth management in remote service applications, e.g., when using delay sensitive protocols such as Voice over IP (VoIP).

## Integrity Monitoring against Malware

Industrial automation components based on Microsoft Windows operating systems are in widespread use today and threatened by a plethora of worms, viruses, and other malware like their counterparts in office networks. Unfortunately, however, local installation

of antivirus software onto these industrial components is typically excluded due to lack of hardware resources and unpredictable real-time behavior. And appliance-based antivirus scanning of network traffic cannot technically control the important Server Message Block (SMB) or Common Internet File System (CIFS) protocol in frequent use for the connection to Windows file shares.

With mGuard 7, Innominate therefore introduces CIFS Integrity Monitoring, an innovative and industry suitable solution to protect Windows-based automation components. It combines CIFS Antivirus Scan Connector, allowing network folders in use for data exchange to be regularly analyzed by your preferred external antivirus scanner, with configurable CIFS Integrity Checking, supervising file systems against unexpected modification or addition of programs, dynamic link libraries, and other executable code. The latter is purely based on the computation of hash code signatures with no need for virus patterns and their permanent update. Discovery of integrity violations can then result in an alarm by SNMP trap or e-mail to an administrator. While all this cannot provide the real-time protection of a locally installed scan engine, it does achieve the best possible under the circumstances: not letting infections go undiscovered for long, not risking to shut down critical communication on false positives, and actually find damages from zero day exploits that virus patterns don't even exist for yet.

### Flexible Network Integration

The mGuard firmware supports the operation of mGuard appliances in a full range of modes for various network scenarios. Ethernet MAU configuration (10/100/1000 MBit/s, half/full duplex) is optionally carried out automatically or manually. In the patented Single Stealth Mode, the system protects an individual network node transparently without using an IP address of its own; in Multi Stealth Mode, the system protects an entire sub-network transparently using its own management IP address.

In Router Mode, the mGuard ensures the desired network separation of internal and external networks with freely definable, additional internal and external routes. Special Router Modes include PPPoE (DSL router) as well as the „Modem“ Mode, in which the mGuard functions as a serial router via dial-up connections using an analog modem or ISDN terminal adapter. Dial-up connections through a serial interface can also be used in parallel or as failover to operation via Ethernet. The external network interface can be configured using DHCP. The mGuard system can also operate as a DHCP server or relay on the internal and/or external interface. When using dynamic IP addresses, the automatic DynDNS registration is useful.

### Device Management

With the Innominate Device Manager (IDM), mGuard supports a centralized device management using a push or pull procedure. Configurations generated by the IDM can be automatically loaded and activated by the mGuard systems via configuration pull from a secure web server either in a scheduled manner or at boot time. Firmware updates and the deployment of licenses can also be initiated in this manner. Should any errors occur with the new configuration, an automatic rollback procedure can restore the previous status and secure access to the device. Locally, the mGuard systems can be administered via a secure web interface as well as a secure command line interface. The latter also forms the basis of configuration push from IDM server to mGuard appliances. Naturally, these administrative accesses are protected by firewall rules and authentication procedures. Administration via VPN connections to the respective mGuard is supported, too. In connection with IDM, five user roles with tiered privileges are offered: root, admin, netadmin, user and audit. As a backup or variant, configuration profiles can be saved on the appliances and restored or downloaded from there at any time.

### Optimized Update Process

Appliances connected to a firmware update web server can be automatically updated at the push of a button to the current patch or minor release or the next major release of the mGuard firmware. With these incremental updates, which can be conducted during continuous operation and possibly do not even require the device to be rebooted, the respective device configuration is preserved unchanged. Subsequently deployed licenses for optional features also remain on the devices and are persistently available, even after a complete flashing with another firmware version. Proxy servers including authentication are supported for the firmware download, as is the case for the configuration pull described above.

### Network Management Support

mGuard supports SNMP v1 /v2 /v3 with respective MIBs for queries and traps of important events, e. g., link up/down or VPN status changes. System and firewall/VPN events can be logged either locally or on a remote syslog server. The system time can be synchronized with a central time source via NTP. In addition, the discovery protocol LLDP is supported for the automatic detection of appliances in the network.

Categories / Features	Standard function (•) or option	New in mGuard version Supported network modes
<b>Supported network modes</b>		
Stealth, Multi-Stealth, Router, PPPoE, PPTP; static IP or DHCP client	•	
Modem (external and internal)	•	5.0/5.1
Secondary external interface (serial)	•	6.0
<b>Network services</b>		
DHCP support: server or relay agent	•	
DNS cache and local DNS server	•	6.1
Dyn. DNS	•	
NTP client and server	•	6.0
LLDP (link layer discovery protocol)	•	
VLAN (802.1Q)	•	
QoS (quality of service): bandwidth management and prioritization	•	5.0/5.1
<b>System management</b>		
Accelerated firmware flash and rollout procedure	•	7.0
Online updates	•	
User-defined configuration profiles and custom default profile	•	6.0
Web-based management (HTTPS)	•	
Command line interface (SSH)	•	
SNMP v1, v2, v3	•	
Extended support for Innominate Device Manager	•	5.0/6.0
Administration via VPN	•	6.0
Remote syslog logging	•	
<b>Firewall</b>		
Stateful Inspection Firewall	•	
User licenses (nodes)	Unlimited	
NAT, 1:1 NAT	•	
Port forwarding	•	
MAC filtering	•	
Firewall rules in VPN connections	•	
User Firewall	•	
Hierarchical rule sets	•	5.0
IP spoofing protection	•	
Configurable SYN flood and DoS protection (against denial of service)	•	
<b>Virtual Private Networks (IPsec VPNs)</b>		
Max. number of concurrent VPN tunnels (depending on appliance and/or software license)	10/250/1000	7.0
Encryption algorithms: DES, 3DES, AES-128/-192/-256, Null	•	
Hardware-accelerated encryption	•	
IPsec modes: ESP tunnel/ESP transport; IPsec NAT-Traversal	•	
IPsec tunneling through TCP and web proxy servers with authentication	•	6.1
Authentication: X.509v3 certificates with RSA or PSK	•	
PKI support: certificate management, CA certificates, CRLs	•	5.0/6.0
Data integrity: MD5, SHA-1	•	
Internet Key Exchange (IKE): quick mode, main mode, PFS	•	
IKE fragmentation support	•	5.1
IPsec L2TP server	•	
Dead peer detection (RFC 3706)	•	
DynDNS support for VPNs	•	
VPN connections to every mGuard interface	•	6.0
VPN in every network mode incl. Single and Multi Stealth Mode	•	6.0
1:1 NAT in VPNs (local and remote network)	•	
NAT masquerading in VPNs (local network)	•	6.1
(De)activation of VPN tunnels via HTTPS	•	
(De)activation of VPN tunnels via electrical signal contact	•	5.1/6.0
SNMP traps for VPN events (tunnel up/down)	•	5.1
Extended VPN diagnostics and status queries via CGI	•	6.1
<b>Integrity Protection against Malware</b>		
CIFS Integrity Monitoring, including CIFS Antivirus Scan Connector and CIFS Integrity Checking for Windows file shares	Option	7.0

### Hardware Platform Support

The mGuard 7 firmware is available for

- ARM,
  - x86
  - and PowerPC
- processor architectures, and supports the following mGuard security appliances:
- mGuard blade
  - mGuard centerport
  - mGuard delta
  - mGuard industrial RS (Analog/ISDN)
  - mGuard PCI
  - mGuard smart
  - EAGLE mGuard.