HIRSCHMANN

User Manual

Industrial ETHERNET Firewall
EAGLE mGuard

Technical Support
HAC-Support@hirschmann.de

HIRSCHMANN

User Manual

Industrial ETHERNET Firewall
EAGLE mGuard

Technical Support
HAC-Support@hirschmann.de

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany (21.9.06)

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Tel. +49 1805 141538 -01-0806

Table of Contents

Table of Contents

Table of Contents

1 Introduction

The mGuard protects IP data connections. The device supports the following functions:

- Network Card (mGuard PCI), Switch (mGuard delta)
- VPN router (VPN - **V**irtual **P**rivate **N**etwork) for the secure transfer of data via public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol)
- Configurable firewall to provide protection against unauthorized access. The dynamic packet filter inspects the source and destination addresses of data packets and blocks undesired traffic.
- Virus protection with support for the protocols HTTP, FTP, SMTP and POP3.

The device can be conveniently configured using a Web browser.

Network features

- Transparent (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (for DSL) and PPTP (for DSL) connectivity
- VLAN
- DHCP server/relay on the external and internal network interfaces
- DNS cache on the internal network interface
- Administration using HTTPS and SSH

Firewall features

- Stateful packet inspection
- Anti-spoofing
- IP Filtering
- L2 Filtering (only Transparent mode)
- NAT with FTP, IRC and PPTP pass through (only router modes)
- 1:1 NAT (only router modes)
- Port forwarding (only router modes)
- Firewall throughput max. 99MBit/s
- Individual firewall rules for different users (user firewall)

Anti-Virus features

- ClamAV virus protection
- Supported protocols: HTTP, FTP, POP3 and SMTP (sending)
- The virus filter can decompress the following formats:
    - ZIP
    - RAR
    - GZIP
    - BZIP2
    - TAR
    - MS OLE2
    - MS Cabinet Dateien (CAB)
    - MS CHM (Komprimiertes HTML)
    - MS SZDD
    - UPX
    - FSG
    - Petite

VPN features

- Protocol: IPsec (Tunnel and Transport Mode)
- IPsec DES encryption - 56 Bit
- IPsec 3DES encryption - 168 Bit
- IPsec AES encryption - 128, 192 and 256 Bit
- Packet authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with Main and Quick Mode
- Authentication: Pre-Shared Key (PSK), X.509v3 certificate
- DynDNS

- NAT-T
- Dead Peer Detection (DPD)
- Hardware encryption
- up to 250 VPN tunnels (please refer to the feature table)
- VPN throughput max. 35MBits/s on 266MHz or 70MBit/s on 533MHz models.
- IPsec firewall and 1:1 NAT
- Default route over VPN

Additional features

- MAU management
- Remote logging
- Router/Firewall Redundancy
- IPsec/L2TP Server
- LLDP
- Administration by SNMP v1-v3 (please refer to the feature table) and Innominate Device Manager (IDM)

Support

In case of problems with the mGuard please contact your local dealer.
Additional information about the device and relevant changes as well as release notes and software updates can be found on the web site:
- for the EAGLE mGuard under www.hirschmann-ac.com,
- for all other mGuards under http://www.innominate.com/

1.1 Device versions

mGuard is available in the following device versions, which have largely identical functions. All devices can be utilised regardless of the processor technology and operating system the connected computers use.

mGuard smart

Smallest device model. Can, for example, simply be plugged between the computer or local network (on mGuard's LAN port) and an available router (on mGuard's WAN port), without having to change existing system configurations or driver installations. Designed for instant use in the office or when on the go.

mGuard PCI

This card, which can be plugged into a PCI slot, provides the computer it is installed in with all mGuard functions in driver mode and can additionally be utilised as a normal network card. A network card already on hand in the computer or another local computer / local network can be connected in the power-over-PCI mode.

mGuard blade

The mGuard blade Pack includes the mGuard bladeBase, which can be easily installed into standard 3 U racks (19 inches) and accommodate up to 12 mGuard blades. Thus this version is ideally suited for use in an industrial environment where it can protect several server systems individually and independently of one another. An additional serial interface enables remote configuration using a telephone dial-up connection or a terminal.

EAGLE mGuard

EAGLE mGuard was developed in co-operation with the Industrial Security Alliance partner Hirschmann Automation and Control GmbH. The device is designed for top hat rail mounting (according to DIN EN 50 022) and is therefore especially suited for use in industrial environments. The optional configuration connection and the option to establish a telephone dial-up connection via the V.24 interface provide for additional applications options.

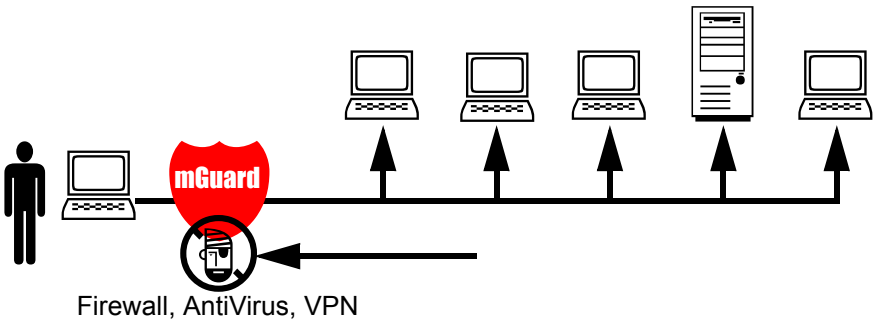
mGuard delta

This device model is a compact LAN switch (Ethernet / Fast Ethernet) designed for connecting up to 4 LAN segments. Thus the device is especially suited for logically segmented network environments where the locally connected computers / networks share the mGuard functions. An additional serial interface enables configuration using a telephone dial-up connection or a terminal. .With its robust metal housing, mGuard delta is not only suitable as a desktop device but also for placement in wiring closets.

2 Typical application scenarios

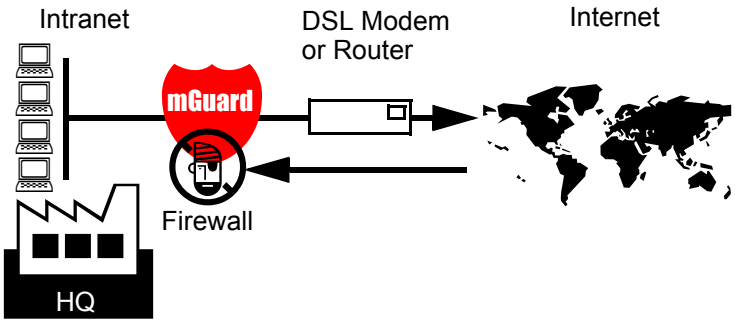
Some of the more common application scenarios may be found below.

Transparent Mode



In *Transparent* Mode (factory default) the mGuard can be installed between an individual computer and the rest of the network.
The settings for Firewall, AntiVirus and VPN can be made with a webbrowser at the URL https://1.1.1.1/.
On the computer itself no configuration changes are required.

Network Router

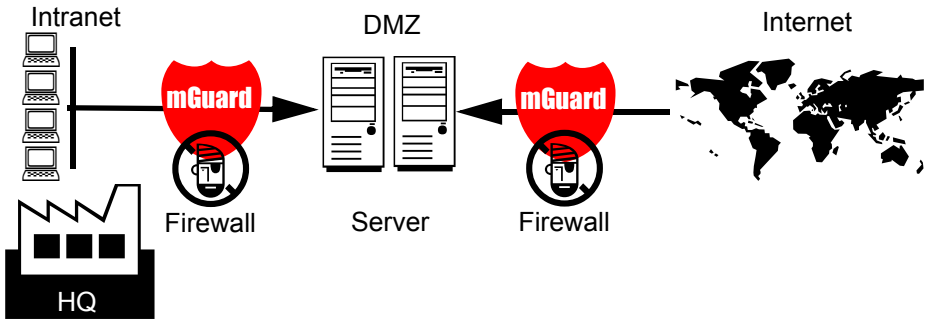


The mGuard is able to provide internet connectivity to a group of computers while protecting the company network with its firewall.
For this purpose one of the following network modes may be used:

- *Router*, if the Internet access is established via a DSL router or dedicated line.
- *PPPoE*, if for example the Internet access is established via a DSL modem using the PPPoE protocol (e.g. in Germany).
- *PPTP*, if for example the Internet access is established via a DSL modem using the PPTP protocol (e.g. in Austria).

The mGuard must be set as the default gateway on the locally connected client system(s).

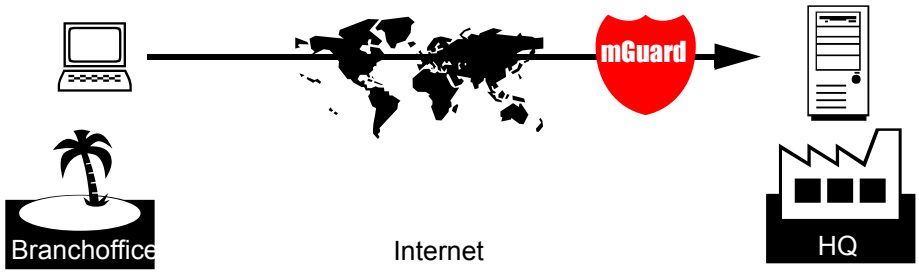
DMZ



A DMZ (Demilitarized Zone) is a protected network, which sits between an tusted network and untrusted networks. For example a company's website may be inside a DMZ, granting FTP write access to computers in the intranet and HTTP read-only access to both networks.
The IP addresses within the DMZ can be public or private. In the latter case, pub-

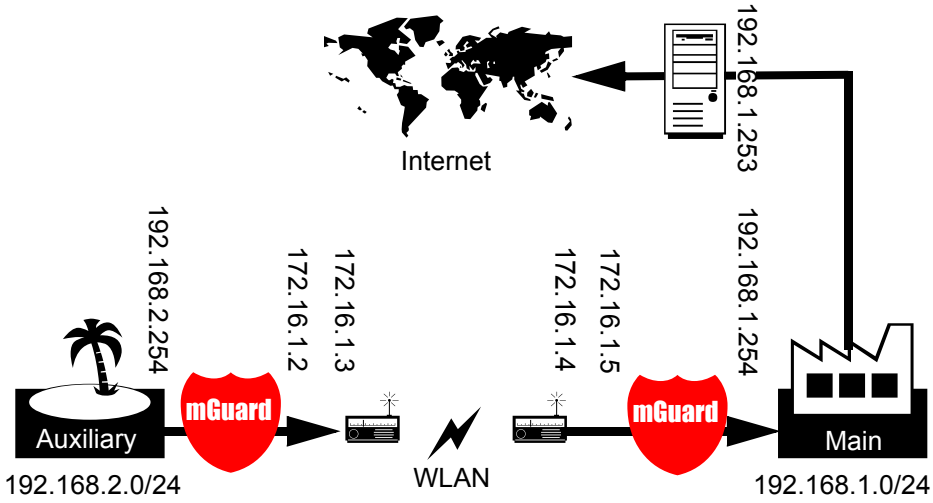
lic IPs would be mapped by means of portforwarding to the private addresses within the DMZ.

VPN Gateway



An encrypted access to the company's network is to be provided to employees at home or in the field. The mGuard thereby provides the services of a VPN gateway.
On the untrusted computers an IPsec capable VPN client must be installed in case the computers operating system does not provide such a service, like Windows 2000 or XP do.

WLAN over VPN



Two buildings of a company are to be connected with an IPsec protected WLAN connection. From the auxiliary building it shall also be possible to use the main building's internet connection.

In this example the mGuards were switched into router mode and a separate network with addresses of 172.16.1.x was created for the WLAN. Since the internet should be also available via the VPN from the auxiliary building, a "Default route over VPN" must be configured.

Auxiliary building tunnel configuration

Connection type	Tunnel (Net <-> Net)
Local network address	192.168.2.0/24
Remote network address	0.0.0.0/0

In main building the appropriate counterpart to the connection is to be configured:

Main building tunnel configuration

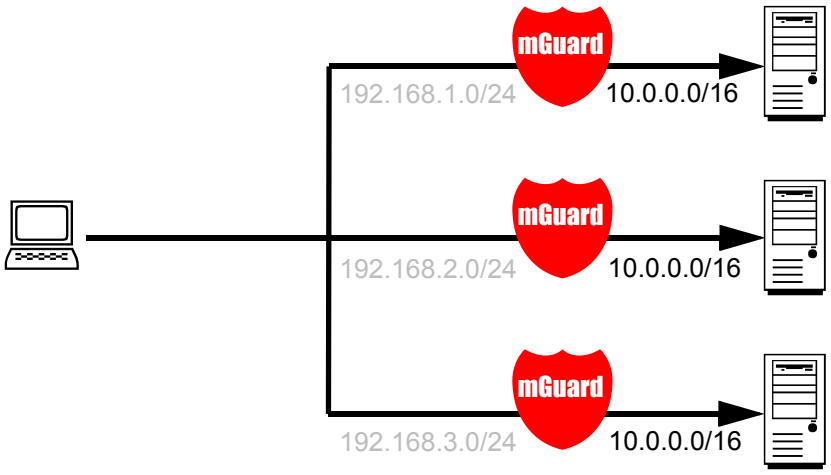
Connection type	Tunnel (Net <-> Net)
Local network address	0.0.0.0/0
Remote network address	192.168.2.0/24

The default route of an mGuard is usually directed over its WAN port. But in this case the internet is reachable via the LAN port:

Main building default gateway

IP of the default gateway	192.168.1.253

Solving Network Conflicts

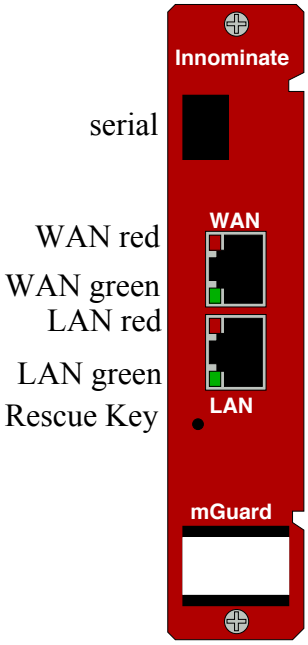


In the illustration above, it is desired that the networks on the right-hand side are accessible from the network or the computer on the left-hand side. For historical or technical reasons, however, the computer networks overlap on the right-hand side.
With the help of mGuards and their 1:1 NAT feature, these networks can be redefined so that the conflict is solved.

(1:1 NAT can be used in normal routing and in IPsec VPN tunnels.)

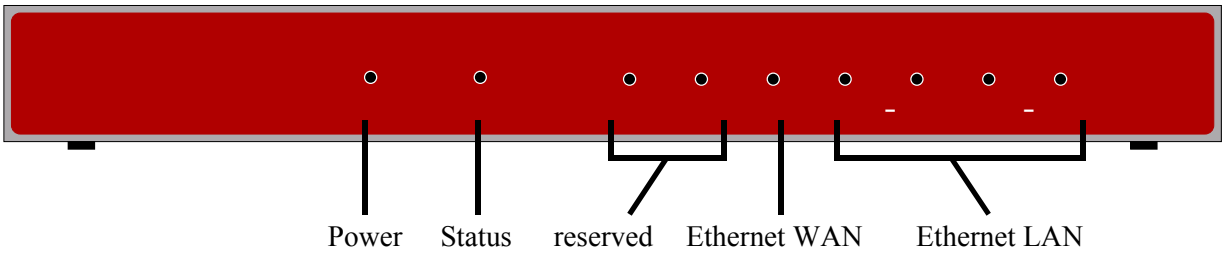
3 Control and LEDs

3.1 mGuard blade



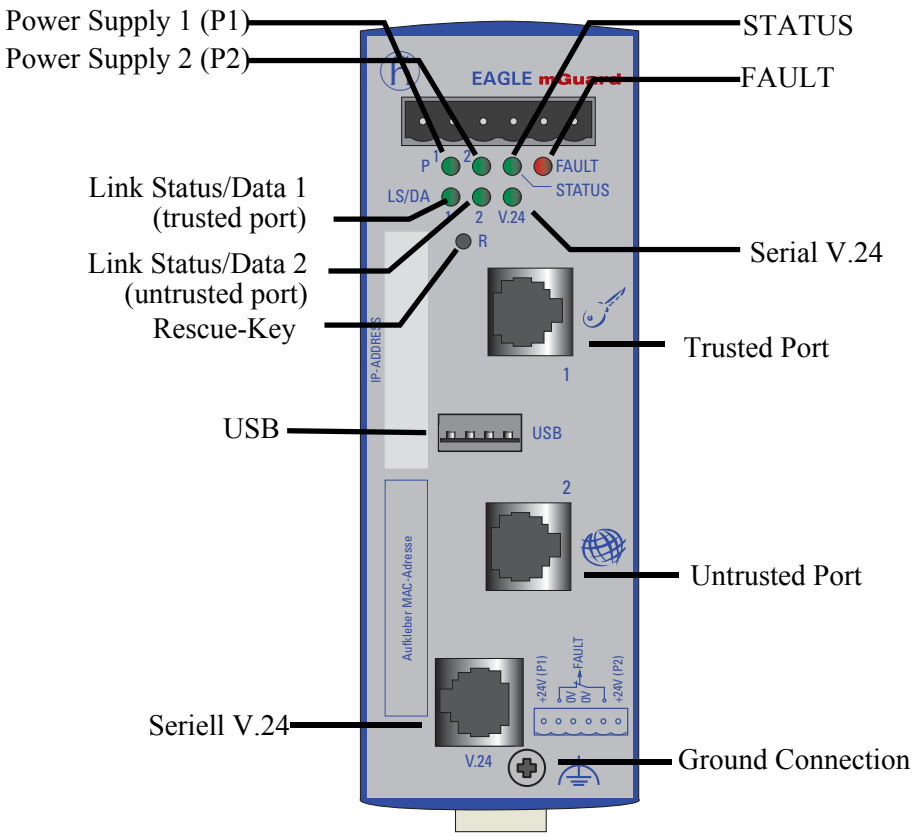
LEDs	State	Meaning
WAN Red, LAN Red	flashing	**Booting up**. After starting or restarting the computer.
WAN Red	flashing	**System error**. ⌧ Perform a system restart. To accomplish this, briefly press the Rescue button (1.5 sec.) If the error occurs again, start the *Recovery procedure* (see "Performing a Recovery" on page 142) or contact Support.
WAN Green, LAN Green	on or flashing	**Ethernet status**. Shows the status of the LAN and WAN interface. As soon as the device is connected to the network, the LEDs will be on continuously to indicate that there is a connection. The LEDs will flash when data packets are transferred.
WAN Green, WAN Red, LAN Green	various LED codes	**Recovery mode**. After pressing the **Rescue key** See "The Rescue Button – restart, recovery procedure and to flash the firmware" on page 142.

3.2 mGuard delta



LEDs	State	Meaning
Power	on	The power supply is active.
Status	on	The mGuard is booting.
	heartbeat (flash, flash, pause, ...)	The mGuard is ready.
1,2	-	Reserved.
3 (WAN)	on	Link detected.
	flashing	Data transfer.
4-7 (LAN)	on	Link detected.
	flashing	Data transfer.

3.3 EAGLE mGuard

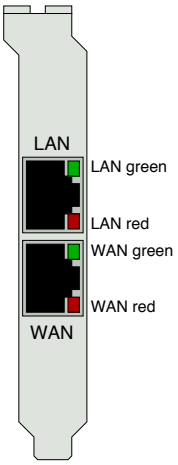


LEDs	State	Meaning
P1, P2	green	The power supply 1 or 2 is active.
STATUS	green blinking	The EAGLE mGuard is booting.
	green	The mGuard is ready.
	yellow blinking slowly	The mGuard is in Router Redundancy Backup mode.
FAULT	red	The signal contact is open in case of an error.
LS/DA 1/2 V.24	green	Link detected.
	green blinking (3 times per period)	The port is disabled.
	yellow flashing	Receiving data.
	running light	Initialization phase after a reset.
Display of ACA function STATUS and V.24	both LEDs blinking simultaneously (slow)	ACA writing process.
	both LEDs blinking simultaneously (slow)	ACA reading process.
	both LEDs blinking alternated (fast)	ACA error.

3.4 mGuard smart

LEDs	Colour	State	Meaning
2	Red/Green	red/green flashing	**Booting up**. After connecting the device to the power supply. After a few seconds, the LED will switch to a heartbeat.
	Green	flashing	**Heartbeat**. The device is correctly connected and functioning.
	Red	flashing	**System error**. ⌧ Perform a system restart. To accomplish this, briefly press the **Rescue key** (1.5 sec.) OR Disconnect the device from its power supply briefly and then reconnect it. If the error occurs again, start the *Recovery procedure* (see “Performing a Recovery” on page 142) or contact Support.
1 and **3**	Green	on or flashing	**Ethernet status**. LED 1 shows the status of the internal interface, LED 3 the status of the external interface. As soon as the device is connected to the interface, the LEDs will be on continuously to indicate that there is a connection to the network. The LEDs will flash when data packets are transferred.
1, 2, 3	various LED codes		**Recovery mode**. After pressing the **Rescue key** See “The Rescue Button – restart, recovery procedure and to flash the firmware” on page 142.

3.5 mGuard PCI



LEDs	State	Meaning
WAN Red, LAN Red	flashing	**Booting up**. After starting or restarting the computer.
WAN Red	flashing	**System error**. ⌧ Perform a system restart. To accomplish this, briefly press the **Rescue key** (1.5 sec.) OR Restart your computer. If the error occurs again, start the *Recovery procedure* (see "Performing a Recovery" on page 142) or contact Support.
WAN Green, LAN Green	on or flashing	**Ethernet status**. Shows the status of the LAN and WAN interface. As soon as the device is connected to the network, the LEDs will be on continuously to indicate that there is a connection. The LEDs will flash when data packets are transferred.
WAN Green, WAN Red, LAN Green	various LED codes	**Recovery mode**. After pressing the **Rescue key** See "The Rescue Button – restart, recovery procedure and to flash the firmware" on page 142.

4 Startup

Safety instructions

The mGuard is intended for (protective) low voltage operation. Only connect the mGuard's network interfaces to LAN installations. Some telephone lines also use RJ45 jacks. The mGuard may not be operated on a telephone line.

Warning mGuard PCI! Before handling the mGuard PCI, touch the bare metal case of your PC to discharge static electricity from your body.

Warning! This is a Class A device. It may cause radio interference in a living area, in which case, the operator may be requested to take appropriate measures.

General notes regarding usage

- mGuard PCI: Your PC must provide a free PCI slot (3.3V or 5V).
- Use a soft cloth to clean the case of the device. Do not use any aggressive solvents!
- Environmental conditions:
  0 to +40°C (blade, smart) 55°C (PCI) 60° (EAGLE)
  max. 90% (EAGLE: 95%), non-condensing humidity
- To avoid overheating, do not leave it in direct sunlight or expose it to any other source of heat.
- Do not bend the cables sharply. Only use network cables to connect to a network.

Steps for starting up the device

To startup the device, perform the following steps in the order listed:

Step	Objectives	Page
1	Check the package contents and read the Release Notes	"Package contents" on page 18
2	Connect the Device	• "Connect the mGuard blade" on page 19 • "Connect the mGuard delta" on page 21 • "Connect the EAGLE mGuard" on page 22 • "Connect the mGuard smart" on page 24 • "Connect the mGuard PCI" on page 25
3	Configure the device to the extent necessary. To accomplish this, select from the various options offered in the mGuard's configuration menus. For more information regarding which options and settings are required (or desirable) for your operating environment, please read the relevant sections in this manual.	"Local Configuration: At startup" on page 34