

Innominate mGuard

Release 4.x.x

Frequently Asked Questions (FAQ)

October 2006



mGuard smart



mGuard PCI



mGuard blade



EAGLE mGuard



mGuard delta

Table of Contents

1	Configuration	4
1.1	<i>General Questions</i>	4
1.1.1	Does the mGuard support the commands <i>route</i> and <i>netstat</i> ?	4
1.1.2	Do I need to install a driver for the mGuard?	4
1.1.3	I need help in configuring the mGuard (Router, PPPoE, VPN, L2TP)	4
1.1.4	In which case do I need to use which network mode (Stealth, Router, PPPoE/PPTP)?	4
1.1.5	The middle LED flashes red continuously. What happened?	5
1.1.6	Is it possible to change the MTU size?	5
1.1.7	Do I need to use a cross link cable?	5
1.1.8	May I connect ISDN directly to the mGuard?	5
1.1.9	Is it possible to specify a NBNS (WINS) server apart of the DNS server?	5
1.1.10	What is Network Address Translation (NAT)?	5
1.1.11	What is Network Address Translation Traversal (NAT-T)?	6
1.1.12	I have enabled remote access for HTTPS/SSH but it still doesn't work	6
1.1.13	Do I need to enable remote access for configuring the mGuard from the client?	6
1.2	<i>Stealth mode</i>	7
1.2.1	What does Stealth mode mean?	7
1.2.2	Why must a desktop firewall on the client allow ICMP echo requests	7
1.2.3	What is the difference between the Stealth modes autodetect, static and multiple clients?	7
1.2.4	It is not possible to "ping" the client behind the mGuard	8
1.2.5	I can't access the mGuard through https://1.1.1.1	8
1.2.6	Does my computer need to belong to the same net as the mGuard (IP=1.1.1.1)?	8
1.2.7	Why do I need to specify a default gateway?	8
1.2.8	Web browser error message "Unknown host 1.1.1.1"	9
1.2.9	Sometimes no access to the mGuard and interrupted connection to the network	9
1.2.10	Can I configure the mGuard remotely? Which IP do I have to use?	9
1.3	<i>Router Modes (Router, PPPoE/PPTP)</i>	10
1.3.1	It is not possible to "ping" the mGuard's external IP address	10
1.3.2	When do I need to configure additional internal/external routes?	10
1.3.3	I can't access the mGuard from the web browser	10
1.3.4	PPPoE mode: I can't access the Internet	10
1.4	<i>mGuard PCI</i>	10
1.4.1	Why is the Rescue Switch not reachable from outside?	10
1.4.2	Is the mGuard PCI operable with PCI-x and PCI express slots?	10
2	Software Update, Recovery- and Flash Procedure	11
2.1	<i>Software Update</i>	11
2.1.1	Does the mGuard lose its configuration when performing a software update?	11
2.1.2	Offline update error message "tar: Invalid gzip magic"	11
2.1.3	Online update error message "Not a valid hostname or IP address"	11
2.1.4	Online update error message "server returned error 404: HTTP/1.0 404 Not Found"	11
2.1.5	Online update error message "HTTP/1.0 401 Authorization Required"	11
2.1.6	Update message "35 packages not installed completely"	11
2.1.7	Update message "1 package not installed completely – Please reboot"	11
2.2	<i>Recovery Procedure</i>	12
2.2.1	When do I need to execute the Recovery procedure?	12
2.2.2	Does the mGuard lose its configuration when executing the Recovery procedure?	12
2.3	<i>Flash Procedure</i>	13
2.3.1	When do I need to flash the mGuard?	13
2.3.2	How do I flash the mGuard?	13
2.3.3	Problems with Windows TFTP/DHCP server	13
2.3.4	The middle LED flashes red after the DHCP server has sent the IP address	13
2.3.5	Error message "The system cannot find the file specified (rollout.sh)"	13
2.3.6	How do I configure the script rollout.sh?	13

3	VPN	14
3.1	<i>General Questions</i>	14
3.1.1	License for 10 VPN tunnels: Does it mean a maximum of 10 VPN tunnels or 10 IP connections?	14
3.1.2	In which cases can I use pre-shared secret keys (PSK) as authentication method?	14
3.1.3	How do I obtain X.509 certificates?	14
3.1.4	What do I need to consider when creating X.509 certificates?	14
3.1.5	The upload of the machine certificate doesn't work	14
3.1.6	How does Dead Peer Detection (DPD) work?	14
3.1.7	Does the remote peer support Dead Peer Detection (DPD)?	14
3.1.8	What do I need to consider if both mGuards are located behind NAT gateways?	15
3.1.9	When do I need to use VPN 1:1 NAT?	15
3.1.10	The script nph-vpn.cgi for activating a VPN tunnel doesn't work with MS Internet Explorer	15
3.2	<i>VPN tunnel problems</i>	16
3.2.1	VPN tunnel using DynDNS can't be established or fails after a while	16
3.2.2	VPN tunnel using DynDNS gets interrupted after a couple of hours	16
3.2.3	PPPoE mode: Problems transferring huge data (e.g. database, email) through a VPN tunnel	16
3.2.4	VPN tunnel works in one direction only	16
3.2.5	A VPN tunnel can't be established. What could be the reason?	16
3.2.6	VPN connection can't be established, the ipsec daemon isn't started	17
3.2.7	IPsec status: The displayed lifetimes differ from the settings	17
3.2.8	Stealth mode: Pluto restarts continuously (displayed in the VPN log)	17
3.2.9	Error message "cannot initiate connection without knowing peer IP address"	17
3.2.10	Poor VPN throughput in a Windows environment	18
3.3	<i>L2TP</i>	19
3.3.1	L2TP connection doesn't work anymore after applying a Windows update/SP	19
3.3.2	How do I setup an L2TP connection between a Windows client and the mGuard?	19
3.3.3	Windows client error #789	19
3.3.4	Windows client error #792	19
3.4	<i>Interoperability</i>	20
3.4.1	Astaro 5/6	20
3.4.2	Astaro Security Gateway 220?	20
3.4.3	Bintec VPN Access 25?	20
3.4.4	Check Point NGX (R60)	20
3.4.5	Cisco PIX	20
3.4.6	Cisco VPN3000 Concentrator Series	20
3.4.7	Fortigate-60	20
3.4.8	Netgear FVS338	20
3.4.9	Netscreen 5GT/204/5400	20
3.4.10	TrustGate5	21
3.4.11	VPN problems with Cisco devices	21
3.4.12	Problems establishing a VPN across a Lancom router (model 1611)	21
3.4.13	VPN tunnel between mGuard and Astaro doesn't work	21
4	Firewall	22
4.1	<i>Which rules do I need to follow when configuring the firewall?</i>	22
4.2	<i>Do I also need to configure incoming firewall rules?</i>	22
4.3	<i>I'd like to prevent access to the Internet but it doesn't work</i>	22
4.4	<i>What's the meaning of the abbreviations in the firewall log?</i>	22
4.5	<i>ICMP echo requests from the client to the mGuard do not appear in the FW log</i>	22
4.6	<i>I can reach the clients of the internal network through port forwarding although the incoming FW should prevent it</i>	22
4.7	<i>Port scanner reports "Port xxxx CLOSED" though I've allowed this port</i>	22
4.8	<i>MAC filter: Restricted IPv4 access doesn't work</i>	22
4.9	<i>When do I need to use 1:1 NAT?</i>	23
4.10	<i>Poor firewall throughput</i>	23

mGuard – Frequently Asked Questions

5	Services	24
5.1	<i>I have entered a NTP server and enabled this service but it doesn't work</i>	24
5.2	<i>Problems with DHCP Relay</i>	24
5.3	<i>How do I need to configure the mGuard for using DynDNS.org?</i>	24
6	Anti Virus Protection (AVP)	25
6.1	<i>I have requested the AVP license but I still don't have received it</i>	25
6.2	<i>License request: The screen for confirming the entered data does not appear</i>	25
6.3	<i>Email with attachment can't be scanned and blocks subsequent emails</i>	25
7	Third Party Products	26
7.1	<i>Stealth mode: Cisco firmware upgrade through TFTP doesn't work</i>	26
7.2	<i>Stealth mode: Access to Lotus Notes server with mGuard 10-20 times slower</i>	26
7.3	<i>Does the mGuard support Novell IPX?</i>	26
7.4	<i>Stealth mode: Problems with Microsoft Server and Network Load Balancing (NLB)</i>	26
8	Related Documentation	27
8.1	<i>User's Manual</i>	27
8.2	<i>Application Notes</i>	27
8.3	<i>Additional Documentation</i>	27
8.4	<i>Interoperability</i>	27

1 Configuration

1.1 General Questions

1.1.1 Does the mGuard support the commands *route* and *netstat*?

Command *route*: The mGuard does not support this command. It provides the more efficient *iproute2* package, which includes the command *ip route*.

Command *netstat*: The mGuard does not support this command. We didn't see a need for supporting this utility during our development and support activities. The related information may be retrieved from the directory */proc/net* and from other locations.

1.1.2 Do I need to install a driver for the mGuard?

The installation of a driver is only required when using the mGuard PCI in *Driver* mode. In this case a driver for the PCI interface of the mGuard PCI (available for Windows XP/2000 and Linux) needs to be installed on the computer which will provide a "regular" network interface with additional security functions.

All other products will be configured completely through their web interface.

1.1.3 I need help in configuring the mGuard (Router, PPPoE, VPN, L2TP)

Please download the document *mGuard Configuration Examples* from our homepage (www.innominat.com, *Download Documentation*). This document contains configuration examples how to configure the mGuard for different operating modes (Router, PPPoE, VPN, L2TP) and scenarios (firewall redundancy, router redundancy, 1.1 NAT, etc.).

1.1.4 In which case do I need to use which network mode (Stealth, Router, PPPoE/PPTP)?

Stealth mode:

If the mGuard is operated in *Stealth* mode you don't need to reconfigure the clients which are connected to the internal interface of the mGuard. You simply need to interconnect the mGuard between the clients which need to be protected and the network. The IP addresses of the clients do not change. All processes, which are listening on a port, are hidden to the network and won't be detected by a port scanner. The mGuard works completely transparent.

Stealth - autodetect and static:

The *Stealth* modes *autodetect* or *static* can be used if the mGuard should protect one single entity (e.g. server) and if the NIC of the client has only one IP address. Otherwise the *multiple clients Stealth* mode needs to be used.

When using *autodetect Stealth* mode, the mGuard detects its IP address automatically by analyzing the traffic which comes from the internal network and adopts the IP address of the client.


Some entities do not generate traffic by itself (e.g. server, webcam) so the mGuard will never get its IP settings. In this case you need to use *static Stealth* mode and specify the clients IP and MAC address and the corresponding netmask in the menu *Network -> Interfaces*, tab *General*.

The WebUI of the mGuard can be accessed from the internal network through the URL <https://1.1.1.1> and from the external network by using <https://<IP address of the client>> assuming that HTTPS remote access is enabled (menu *Management -> Web Settings*, tab *Access*).

Stealth - multiple clients:

This mode is used if the mGuard should protect multiple clients or if the NIC of a single client has more than one IP address.

The WebUI of the mGuard can be accessed from the internal network by using the URL <https://1.1.1.1> as long as no *Management IP* was specified. If the WebUI should be accessible from the external network, enable HTTPS remote access (menu *Management -> Web Settings*, tab *Access*) and specify a *Management IP* in the menu *Network -> Interfaces*, tab *General*. Now you can access the mGuard through the URL <https://<Management IP>> from the internal and external network.

 **Note:** VPN is not supported in *Multiple Clients Stealth* mode.

Router mode:

In *Router* mode the mGuard acts as a router between two networks. You need to configure the internal and external interface.

The WebUI of the mGuard can be accessed from the internal network through the URL <https://<internal IP of the mGuard>> and from the external network by using <https://<external IP of the mGuard>> (assuming that HTTPS remote access is enabled, menu *Management* -> *Web Settings*, tab *Access*).

PPPoE/PPTP mode:

In *PPPoE* mode the mGuard acts as a DSL router between the internal network and the Internet. The external interface of the mGuard needs to be connected to a DSL modem. You need to configure the internal interface. The mGuard will receive its external settings from the Internet Service Provider (ISP).

PPTP is the equivalent to *PPPoE* which is used for example in Austria.

The WebUI of the mGuard can be accessed from the internal network through the URL <https://<internal IP of the mGuard>> and from the external network by using <https://<public IP of the mGuard>> (assuming that HTTPS remote access is enabled, menu *Management* -> *Web Settings*, tab *Access*).

1.1.5 The middle LED flashes red continuously. What happened?

If the middle LED flashes red continuously then the mGuard couldn't start because some files used by the kernel are missing. This could happen if a flash procedure was interrupted. Flash the mGuard with the current firmware version. This should solve the problem.

1.1.6 Is it possible to change the MTU size?

It is possible to change the MTU sizes through the menu *Network* -> *Interfaces*, tab *Ethernet*.

1.1.7 Do I need to use a cross link cable?

Not necessarily. The mGuard detects automatically the type of the connected cable and the transfer rate.

1.1.8 May I connect ISDN directly to the mGuard?

NO! The connectors of the mGuard are for Ethernet connections only. You may use an ISDN router, which provides an Ethernet interface. Connecting the mGuard to another device than an Ethernet connection may cause serious damage to the mGuard.

1.1.9 Is it possible to specify a NBNS (WINS) server apart of the DNS server?

A WINS server can be specified through the menu *Network* -> *DHCP*, tabs *Internal/External DHCP*.

1.1.10 What is Network Address Translation (NAT)?

NAT (Network Address Translation or Network Address Translator) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

1.1.11 What is Network Address Translation Traversal (NAT-T)?

The problem with NAT and IPSec

Why doesn't NAT work with IPSec? Remember that the point of IPSec is not just to protect the confidentiality of the data, but also to assure the authenticity of the sender and the integrity of the data (that it hasn't been changed in transit). The problem with NAT is obvious: NAT must change information in the packet headers in order to do its job.

The first problem is that NAT changes the IP address of the internal computer to that of the NAT device. The Internet Key Exchange (IKE) protocol used by IPSec embeds the sending computer's IP address in its payload, and this embedded address doesn't match the source address of the IKE packet (which is that of the NAT device). When these addresses don't match, the receiving computer will drop the packet.

Another problem is that TCP checksums (and optionally, UDP checksums) are used to verify the packets. The checksum is in the TCP header and it contains the IP addresses of the sending and receiving computers and the port numbers used for the communications. With normal NAT communications, this isn't a problem because the NAT device updates the headers to show its own IP address and port in place of the sending computers. However, IPSec encrypts the headers with the Encapsulating Security Payload (ESP) protocol. Since the header is encrypted, NAT can't change it. This means the checksum is invalid, so the receiving computer rejects the packet.

In addition, NAT isn't able to use the port numbers in TCP and UDP headers to multiplex packets to multiple internal computers when those headers have been encrypted by ESP.

NAT-T: How it works

The IPSec working group of the IEEE has created standards for NAT-T that are defined in RFCs 3947 and 3948. NAT-T is designed to solve the problems inherent in using IPSec with NAT.

NAT-T adds a UDP header that encapsulates the ESP header (it sits between the ESP header and the outer IP header). This gives the NAT device a UDP header containing UDP ports that can be used for multiplexing IPSec data streams. NAT-T also puts the sending computer's original IP address into a NAT-OA (Original Address) payload. This gives the receiving computer access to that information so that the source and destination IP addresses and ports can be checked and the checksum validated. This also solves the problem of the embedded source IP address not matching the source address on the packet.

1.1.12 I have enabled remote access for HTTPS/SSH but it still doesn't work

Verify that you also have specified firewall rules for the remote access (HTTPS: menu *Management* -> *Web Settings*, tab *Access*, SSH: menu: *Management* -> *System Settings*, tab *Shell Access*).

1.1.13 Do I need to enable remote access for configuring the mGuard from the client?

No, usually the clients connected to the internal interface of the mGuard have access to the device through SSH/HTTPS.

It is possible to block SSH and/or HTTPS access from the internal network (HTTPS: menu *Management* -> *Web Settings*, tab *Access*, SSH: menu: *Management* -> *System Settings*, tab *Shell Access*). If you disable SSH and/or HTTPS access from the internal network, ensure that you have enabled it for the external network. Otherwise you won't have the possibility to gain access to the mGuard, neither through SSH nor through HTTPS, neither from the internal nor from the external network. In such a case you need to execute the *Recovery* procedure (refer to the *User's Manual*). The *Recovery* procedure will remove defined SSH access rules and allow HTTPS access from the internal network.

1.2 Stealth mode

1.2.1 What does Stealth mode mean?

If the mGuard is operated in *Stealth* mode you don't need to reconfigure the clients which are connected to the internal interface of the mGuard. You simply need to interconnect the mGuard between the clients which need to be protected and the network. The IP addresses of the clients do not change. All processes, which are listening on a port, are hidden to the network and won't be detected by a port scanner. The mGuard works completely transparent. You can't use the *Stealth* mode if the mGuard is connected to a DSL line. In this case you need to use the *PPPoE* or *PPTP* mode respectively combined with *Network Address Translation* (NAT).

1.2.2 Why must a desktop firewall on the client allow ICMP echo requests

The mGuard can't initiate ARP requests if it is operated in *Stealth* mode. For sending data to an external network (as it is the case e.g. for the AVP database update, for establishing a VPN connection or for the online update) the mGuard needs to know the MAC address of the default gateway. For obtaining it, the Guard sends an ICMP echo request to the client first by using the IP address of the destination as source IP address. When receiving the reply from the client, the mGuard filters out the MAC address of the default gateway and removes the ICMP request.

1.2.3 What is the difference between the Stealth modes autodetect, static and multiple clients?

If the mGuard is operated in *Stealth* mode you don't need to reconfigure the clients which are connected to the internal interface of the mGuard. You simply need to interconnect the mGuard between the clients which need to be protected and the network. The IP addresses of the clients do not change. All processes, which are listening on a port, are hidden to the network and won't be detected by a port scanner. The mGuard works completely transparent.

Autodetect and static mode:

The *Stealth* modes *autodetect* or *static* can be used if the mGuard should protect one single entity (e.g. server) and if the NIC of the client has only one IP address. Otherwise the *multiple clients* mode needs to be used.

When using *autodetect Stealth* mode, the mGuard detects its IP address automatically by analyzing the traffic which comes from the internal network and adopts the IP address of the client.

Some entities do not generate traffic by itself (e.g. server, webcam) so the mGuard will never get its IP address. In this case you need to use *static Stealth* mode and specify the clients IP and MAC address in the menu *Network -> Interfaces*, tab *General*.

The WebUI of the mGuard can be accessed from the internal network through the URL <https://1.1.1.1> and from the external network by using <https://<IP address of the client>>, assuming that HTTPS remote access is enabled (menu *Management -> Web Settings*, tab *Access*).

Multiple clients mode:

This mode is used if the mGuard should protect multiple clients or if the NIC of the client has more than one IP address.

The WebUI of the mGuard can be accessed from the internal network by using the URL <https://1.1.1.1> as long as no *Management IP* was specified.

If the WebUI should be accessible from the external network, enable HTTPS remote access (menu *Management -> Web Settings*, tab *Access*) and specify a *Management IP* in the menu *Network -> Interfaces*, tab *General*. Now you can access the mGuard through the URL <https://<Management IP>> from the internal and external network. Access through <https://1.1.1.1> from the internal network isn't possible when using a *Management IP*.

 **Note:** VPN is not supported in *Multiple Clients Stealth* mode.

1.2.4 It is not possible to “ping” the client behind the mGuard

- Verify that you have specified incoming firewall rules (menu *Network Security* -> *Packet Filter*, tab *Incoming Rules*) with Protocol=All or Protocol=ICMP. If this isn't the case the firewall will block the ICMP requests.
- Check if there is a desktop firewall (e.g. WinXP SP2 firewall) running on the client, which blocks the ICMP requests.
- Check if there is a VPN Client running on the client. Some VPN clients come with an integrated firewall (e.g. Cisco VPN Client, Checkpoint VPN Client) which blocks the ICMP requests.

1.2.5 I can't access the mGuard through <https://1.1.1.1>

- At first verify that the web browser does not use a proxy (Internet Explorer: *Tools* -> *Internet Options*, tab *Connections*, button *<LAN Settings>*, section *Proxy server*). In this case the web browser would send the requests directly to the proxy.
- Check if a desktop firewall is running on the client which prevents the access to the mGuard. If this is the case, disable the firewall and restart the computer.
- Check with the command `ipconfig /all` if the Ethernet card has more than one IP address. We encountered this problem with an USB software (IP=192.168.100.100) which had sent the data through the wrong interface. In this case the mGuard would reconfigure itself every second for using the other IP address. You need to disable the software which assigned the second IP address to the computer in such a case.
- A default gateway must be defined on the client. The mGuard captures all data traffic directed to the address 1.1.1.1 and uses it internally. If no default gateway is defined, the client will send data only to IP addresses, which belong to his own network (e.g. 192.168.1.0/24). In this case data directed to 1.1.1.1 will never reach the mGuard.

You need to consider the following points if the external interface of the mGuard is not connected to the network:

- Assign static IP settings to the client if the client is configured to receive the setting from a DHCP server (e.g. IP address = 192.168.1.100, Subnet mask = 255.255.255.0, Default gateway = 192.168.1.1). You need to define a default gateway even if the external interface of the mGuard is not connected to a network.
- Assign a static MAC address to the IP address of the default gateway. The computer would try to retrieve the MAC address of the default gateway by sending an ARP request first. This of course will fail because the default gateway doesn't really exist. For avoiding this, you need to assign any static MAC address you like to the default gateway with the ARP command (e.g. `arp -s <IP of the default gateway> aa-aa-aa-aa-aa-aa`). This way the data will be sent through the mGuard and the mGuard will capture all data directed to the address 1.1.1.1.

1.2.6 Does my computer need to belong to the same net as the mGuard (IP=1.1.1.1)?

No, definitely not. The address 1.1.1.1 is a pseudo address. All data traffic directed to this address will be captured by the mGuard and used internally. If you'd select an IP address and a netmask which belongs to the same net as the IP 1.1.1.1 (e.g. 1.1.1.2/255.255.255.0) then the IP 1.1.1.1 must be reachable directly by the computer. Your computer will send an ARP request to verify this. You won't get a connection to the mGuard because the mGuard in *Stealth* mode doesn't reply to ARP requests.

1.2.7 Why do I need to specify a default gateway?

The mGuard captures all data traffic directed to the address 1.1.1.1 and uses it internally. Therefore the data must reach the mGuard. If you don't specify a default gateway then the client will send data only to IP addresses which belong to his own network (e.g. 192.168.1.0/24). If the external interface of the mGuard is not connected to the network, then you need to assign a static MAC address to the IP address of the default gateway. The computer would try to retrieve the MAC address of the default gateway by sending an ARP request first. This of course will fail because the default gateway doesn't really exist. For avoiding this, you need to assign any static MAC address you like to the default gateway with the ARP command (e.g. `arp -s <IP of the default gateway> aa-aa-aa-aa-aa-aa`). This way the data will be sent through the mGuard and the mGuard will capture all data directed to the address 1.1.1.1.

1.2.8 Web browser error message "Unknown host 1.1.1.1"

This error message appears when the web browser uses a proxy. In this case the data packages will be sent directly to the proxy and not to the IP address 1.1.1.1. Configure the web browser not to use a proxy.

1.2.9 Sometimes no access to the mGuard and interrupted connection to the network

Check with the command `ipconfig /all` if the NIC of the client has more than one IP address. If this is the case the mGuard (*Stealth* mode only) will reconfigure itself every second by adopting the senders IP address. This would make it almost impossible to gain access to the mGuard and the connection to the network will be interrupted.

1.2.10 Can I configure the mGuard remotely? Which IP do I have to use?

At first you need to enable remote access for SSH (menu: *Management* -> *System Settings*, tab *Shell Access*) and/or HTTPS (menu *Management* -> *Web Settings*, tab *Access*) and set the according firewall rules. For gaining remote access to the mGuard you need to specify the IP address of the client to which the mGuard is connected.


1.3 Router Modes (Router, PPPoE/PPTP)

1.3.1 It is not possible to “ping” the mGuards external IP address

By default, the mGuard drops ICMP packets from the external network directed to its external interface. You can enable this option through the menu *Network Security -> Packet Filter*, tab *Advanced*, option *ICMP from extern to the mGuard*.

1.3.2 When do I need to configure additional internal/external routes?

You need to define for example an additional internal route if the internal network contains a subnet which can be accessed through another router. In this case you need to specify as *Network* the network IP of the subnet and as *Gateway* the external IP address of the router.

 **Note:** Do never specify an additional internal route for a network/gateway, which belongs to the external network and vice versa. This could cause a strange behaviour of the firewall.

1.3.3 I can't access the mGuard from the web browser

- Verify that the internal IP of the mGuard is defined as default gateway on the client.
- Did you use the correct IP address for accessing the mGuard? If the internal IP address of the mGuard is unknown execute the *Recovery* procedure (please refer to the User's Manual). This procedure will reset the mGuard back to *Stealth* mode so that you can access it through <https://1.1.1.1>.
- Starting with version 3.1.0 it is possible to block SSH and HTTPS access from the internal network (HTTPS: menu *Management -> Web Settings*, tab *Access*, SSH: menu: *Management -> System Settings*, tab *Shell Access*). If you have specified such rules and the IP address for accessing the mGuard from the external network is unknown then you need to execute the *Recovery* procedure. This procedure will remove SSH access rules and enable internal HTTPS access.

1.3.4 PPPoE mode: I can't access the Internet

- Verify that NAT (Network Address Translation) is enabled (menu *Network Security -> NAT*, tab *Masquerading*).
- If you can ping the IP address 212.21.76.70 but if you can't reach the site by its name (www.innominat.com) then you need to specify a name server in the network settings of your computer.

1.4 mGuard PCI

1.4.1 Why is the Rescue Switch not reachable from outside?

A hardware reset is not required because the mGuard PCI has a hardware watchdog. The watchdog tests every second if the Linux kernel is still alive. If the kernel should die for some strange reason then a reset is performed automatically and the kernel is restarted. A *Rescue Switch* located at the outside wouldn't provide more functionality than the watchdog. The advantage is that no one needs to go to the server room if the kernel dies. You can also initiate other additional functions with the *Rescue Switch* like for example the *Recovery-Procedure* which resets the mGuard to *Stealth* mode. This is another reason why the *Rescue Switch* shouldn't be accessible from outside to prevent misuse.

1.4.2 Is the mGuard PCI operable with PCI-x and PCI express slots?

PCI-x: This works if the mGuard PCI is operated in *Power-over-PCI* mode which means, that only the power is taken from the PCI slot. We don't have tested it for the *Driver* mode.

PCI express: No.

2 Software Update, Recovery- and Flash Procedure

2.1 Software Update

2.1.1 Does the mGuard lose its configuration when performing a software update?

The mGuard won't lose its configuration when updating the firmware through the web interface. The configuration will be erased and reset to the default factory settings only when flashing the mGuard.

2.1.2 Offline update error message "tar: Invalid gzip magic"

Verify that the file extension of the update file is *.tar.gz (e.g. update-3.0.x-3.1.1.tar.gz). Sometimes Microsoft Internet Explorer saves the file as *.tar.tar when downloading it from our homepage.

2.1.3 Online update error message "Not a valid hostname or IP address"

This error message usually occurs if the mGuard can't resolve the IP address of the update server *update.innominat.com*. Go to the menu *Network -> DNS*, set *Servers to query* to *User defined* and enter into the field *User defined name servers* the IP address of a valid DNS server.

If the mGuard is operated in *Stealth* mode, check if a desktop firewall is running on the client to which the mGuard is connected. If this is the case, the firewall must allow incoming ICMP requests. The mGuard in *Stealth* mode can't issue ARP requests by itself. Therefore it sends an ICMP echo request to the client and obtains the MAC address of the default gateway from the reply.

2.1.4 Online update error message "server returned error 404: HTTP/1.0 404 Not Found"

Starting with updates to version 3.0.0 the HTTPS protocol needs to be used. Go to the menu *Management -> Update*, tab *Update*, and verify that *Protocol* is set to *https://*.

2.1.5 Online update error message "HTTP/1.0 401 Authorization Required"

Starting with updates to version 3.0.0 you also need to enter your username (Login) and password through the menu *Management -> Update*, tab *Update* for accessing the download area. If one of those parameters is wrong then the error message "HTTP/1.0 401 Authorization Required" is displayed. Note that username and password are case sensitive. You need to enter them as stated in our response mail to your online registration.

2.1.6 Update message "35 packages not installed completely"

The update process checks at first which packages are currently installed on the device and their version. Based on this information the update process determines which and how many packages need to be updated. The total numbers of packages which need to be updated are displayed in the message "xx packages not installed completely".

2.1.7 Update message "1 package not installed completely – Please reboot"

This is not an error message. The installation of the related package will be finished after rebooting the device.

2.2 Recovery Procedure

2.2.1 When do I need to execute the Recovery procedure?

You need to execute the *Recovery* procedure if you can't get access to the mGuard for one of the following reasons:

- The mGuard is operated in *Router*, *PPPoE* or *PPTP* mode and its internal IP is unknown. The *Recovery* procedure will reset the **mGuard delta** and **mGuard blade control unit** into *Router* mode and its internal IP to 192.168.1.1 so that the device is accessible again through the URL <https://192.168.1.1>. All other products (**mGuard smart**, **mGuard industrial**, **mGuard blade** and **mGuard PCI**) will be reset into *Stealth* mode so that they are accessible again through the URL <https://1.1.1.1>.
- The mGuard is operated in *Multiple Client Stealth* mode with a configured *Management IP* and this IP is unknown. The *Recovery* procedure will remove the *Management IP* so that the mGuard can be accessed again from the internal network by using the URL <https://1.1.1.1>.
- SSH and HTTPS access have been disabled for the internal network and the remote access wasn't enabled for the external network. This feature is available starting with 3.1.0. The *Recovery* procedure will remove SSH access rules and enable internal HTTPS access.


2.2.2 Does the mGuard lose its configuration when executing the Recovery procedure?

The *Recovery* procedure won't affect current configured VPN connections, firewall settings or passwords, except the SSH and HTTPS access rules.

2.3 Flash Procedure

2.3.1 When do I need to flash the mGuard?

You only need to flash the firmware of the mGuard if the root password is unknown. **Note that this procedure will erase existing configurations on the mGuard.** The mGuard will be restored to the factory (default) settings, also the passwords. You need to reconfigure the mGuard after flashing the firmware.

 **Note:** If you want to update the version of the firmware then the *Update* procedure should be the preferred method.

2.3.2 How do I flash the mGuard?

Please download the document *mGuard Update-/Recovery-/Flash-Procedures* from our homepage (www.innominat.com, *Download Documentation*). It describes in detail the required steps for flashing the mGuard.

2.3.3 Problems with Windows TFTP/DHCP server

The following steps are required if the IP address of the client has been changed regarding the last time you've started the TFTP server:

- Start the TFTP server and ignore appearing error messages.
- Click *<Settings>* and then *<OK>*.
- Restart the TFTP server.

2.3.4 The middle LED flashes red after the DHCP server has sent the IP address

- Verify that the firmware files *image.p7s* and *jffs2.img.p7s* are located in the specified update directory.
- On Linux: Check the access rights of the directory which contains the image files.

2.3.5 Error message "The system cannot find the file specified (rollout.sh)"

The file *rollout.sh* is only required, if the mGuard should be configured through an *atv* file during the flash procedure. Otherwise this error message can be ignored.

2.3.6 How do I configure the script *rollout.sh*?

Please download the application note *mGuard Rollout Support* from our homepage (www.innominat.com, *Download AppNotes & Interops*). This document describes in detail the required steps for configuring the script *rollout.sh*.

3 VPN

3.1 General Questions

3.1.1 License for 10 VPN tunnels: Does it mean a maximum of 10 VPN tunnels or 10 IP connections?

This license limits the maximum number of VPN tunnels that can be configured on the mGuard, not the number of IP connections within a tunnel.

3.1.2 In which cases can I use pre-shared secret keys (PSK) as authentication method?

You can use pre-shared secret keys (PSK), if:

- Both peers have a static IP address. Alternatively a peer with a dynamic public IP address can register its IP under a fixed name in a DynDNS service and the remote peer must refer to it.
- The VPN connection won't be established across one or more gateways that have *Network Address Translation* (NAT) activated.

In any other case certificates need to be used.

3.1.3 How do I obtain X.509 certificates?

The enrolment of certificates requires a certification authority (CA) which issues public key certificates for a specific period of time. A CA can be a private (in-house) CA, run by your own organization, or a public CA. A public CA is operated by a third party that you trust to validate the identity of each client or server to which it issues a certificate.

There are several tools available for creating and managing certificates, as for example Microsoft CA Server, OpenSSL and XCA. If you want to use XCA, you can download this tool from <http://www.hohnstaedt.de/xca.html>. The documentation is located at <http://xca.sourceforge.net/>.

3.1.4 What do I need to consider when creating X.509 certificates?

The certificate shouldn't be valid beyond February 2038 because the mGuard handles the expiry date of the certificate as 32bit unsigned integer. Otherwise the mGuard can't load the certificate when initializing the VPN connection.

3.1.5 The upload of the machine certificate doesn't work

Probably the machine certificate is damaged. Create a new export of the certificate as PKCS#12 and try to upload it again.

3.1.6 How does Dead Peer Detection (DPD) work?

There are three parameters for configuring *Dead Peer Detection*: Delay, Timeout and Action. The default settings are Delay=30, Timeout=120 and Action=Hold. If there is no traffic on the VPN tunnel for 30 seconds the mGuard will send a DPD Keep Alive query (R_U_THERE) over the ISAKMP SA to check the availability of the remote peer. If the remote peer does not answer the Keep Alive query within 120 seconds the mGuard will declare the peer as dead.

Action=Hold: The VPN connection is put into trap and will be re-initiated the next time when traffic needs to be send from the internal network through the tunnel.

Action=Clear: The mGuard will delete the VPN connection.

Action=Restart: The mGuard will try to re-establish the VPN tunnel.

 **Note:** DPD only works if both peers support it!

3.1.7 Does the remote peer support Dead Peer Detection (DPD)?

Please consult the user manual of the device or ask the manufacturer. Apart of this you can get this information also from the VPN logs (menu *Logging* -> *Browse local logs*, option *IPsec VPN* enabled). If you see there the message *Dead Peer Detection (RFC3706) enabled* before the IPsec SA is established, then the remote peer supports DPD.

3.1.8 What do I need to consider if both mGuards are located behind NAT gateways?

- Only one mGuard can initiate the connection. The other mGuard must wait for the connection. Do not configure both mGuards to initiate the connection.
- You must use X.509 certificates as authentication method. Pre shared keys (PSK) can only be used, if both peers have a static public IP address AND if the connection won't be established across one or more gateways that have Network Address Translation (NAT) activated.
- You need to enter %any as *Address of the remote site's VPN gateway* on the mGuard that waits for the connection. On the receiving site you need to define port forwarding on the NAT gateway for UDP port 500 and UDP port 4500 to the external IP address of the mGuard.

3.1.9 When do I need to use VPN 1:1 NAT?

VPN 1-to-1 NAT is used for establishing VPN tunnels to other locations which use the same network IP or to establish a VPN tunnel between two sites which use the same internal network IP. Please refer to the *mGuard Configuration Examples* which can be downloaded from our homepage (www.innominate.com, *Download Documentation*).

3.1.10 The script `nph-vpn.cgi` for activating a VPN tunnel doesn't work with MS Internet Explorer

Using this script requires that the web browser supports URL authentication. By default, URL authentication is disabled when using Microsoft Internet Explorer 6 or 7. To enable this option, create **ieexplore.exe** DWORD value in the following registry key and set its value data to 0:

```
HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Internet Explorer \ Main \ FeatureControl \  
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
```


3.2 VPN tunnel problems

3.2.1 VPN tunnel using DynDNS can't be established or fails after a while

Check if the service DynDNS monitoring (menu *IPsec VPN -> Global*, tab *DynDNS Monitoring*) is enabled. If it isn't enabled, the mGuard won't notice when the IP address of the remote gateway has changed.

3.2.2 VPN tunnel using DynDNS gets interrupted after a couple of hours

If you have specified a DynDNS name for the remote VPN gateway, ensure that DynDNS monitoring (menu *IPsec VPN -> Global*, tab *DynDNS Monitoring*) is enabled. Otherwise the mGuard won't notice when the IP address of the remote VPN gateway has changed.

3.2.3 PPPoE mode: Problems transferring huge data (e.g. database, email) through a VPN tunnel

The packages which reach the mGuard are already fragmented due to the Ethernet adapter to which the mGuard is connected. The Ethernet adapter (MTU=1500) fragments the packages and forwards them to the mGuard. Due to the encoding of the packages their size will increase slightly. This could cause problems at some ISP router if they don't support fragmentation/de-fragmentation. Perform the following steps if you encounter such a problem:

- Establish a ssh connection to the mGuard and login as admin.
- Execute the commands:

```
shell> gaiconfig --set VPN_IPSEC0_MTU 1400
shell> gaiconfig -reboot
```

Now the problem was moved away from the ISP router to the mGuard. If a data package larger than 1400 Bytes reaches the mGuard the package will be fragmented first and then encoded. Therefore its size will be less than 1500 Bytes and won't cause any problem at the ISP router.

Another possibility is to reduce the MTU size of the Ethernet adapter on the initiating site.

3.2.4 VPN tunnel works in one direction only

Ensure that the internal IP address of the mGuard is specified as default gateway on the clients of the internal network.

3.2.5 A VPN tunnel can't be established. What could be the reason?

A VPN tunnel is established in two phases: Phase 1 (ISAKMP) and Phase 2 (IPsec).

Phase 1 (ISAKMP) couldn't be established:

- Mismatched Pre-shared secret keys (PSK) or certificates.
- Mismatched ISAKMP policy parameters. Compare the *ISAKMP SA (Key exchange)* settings with the settings on the remote gateway.

Phase 1 (ISAKMP) could be established but not phase 2 (IPsec):

- Mismatched IPsec policy parameters. Compare the *IPsec SA (Data exchange)* settings with the settings on the remote gateway.
- Mismatched tunnel settings:
 - The local and the remote network of the tunnel setting may not be within the same network IP. The following settings won't work: local network=192.168.1.0/16, remote network= 192.168.2.0/16. In this case the netmask must be changed to a C-Class netmask.
 - The local network of the mGuard must be specified as *remote network* on the remote gateway. The local network of the remote gateway must be specified as *remote network* on the mGuard.

3.2.6 VPN connection can't be established, the ipsec daemon isn't started

Is the option *Disable VPN until the user is authenticated via HTTP* (menu *User Authentication -> Local Users*, tab *Passwords*) enabled? This option especially protects mGuards used by *Road Warrior* against unauthorized usage. The VPN connection won't be established as long as you did not enter the user password. The login screen appears as soon as you try to access any web page.

3.2.7 IPsec status: The displayed lifetimes differ from the settings

This is caused by the settings of *Rekeymargin* and *Rekeyfuzz*. If you set both to 0 then the displayed lifetimes would correspond to the settings of the ISAKMP SA and IPsec SA lifetimes. *Rekeymargin* specifies how long before SA (and key) expiry the mGuard should attempt to negotiate replacements begin. *Rekeyfuzz* specifies the maximum percentage by which *Rekeymargin* should be randomly increased to randomize rekeying intervals (important for hosts with many connections). Both values are taken into account when the lifetimes are calculated which are displayed in the menu *IPsec VPN -> IPsec status*.

3.2.8 Stealth mode: Pluto restarts continuously (displayed in the VPN log)

VPN Log entries:
adding interface ipsec0/br0 10.196.148.183
adding interface ipsec0/br0 10.196.148.183:4500
...
shutting down interface ipsec0/br0 10.196.148.183
shutting down interface ipsec0/br0 10.196.148.183
...
listening for IKE messages
adding interface ipsec0/br0 192.168.110.1
adding interface ipsec0/br0 192.168.110.1:4500

Take a look at the VPN Log and check if always the same IP address is displayed for the ipsec0/br0 interfaces. If this is not the case, as shown in the example above, the problem can be caused by one of the following reasons:

- The mGuard is connected the wrong way round (LAN to WAN and WAN to LAN).
- The mGuard is operated in *Stealth* mode but multiple clients are connected to the internal interface. The *Stealth* mode is used to protect one system only.
- The NIC of the system, which is connected to the internal interface of the mGuard, has more than one IP address. This is for example the case when using VMWARE.

Explanation: The mGuard (*Stealth autodetect* mode) gets its IP address by analyzing the traffic which comes from the internal interface. When the IP address of the client has changed then the dependent services (e.g. pluto) will be restarted. During the restart of the services you will lose the connection to the external network and you also won't have access to the WebUI.

3.2.9 Error message "cannot initiate connection without knowing peer IP address"

This error message appears when *Pre-Shared Secret Keys* (PSK) are used as authentication method and if *%any* is specified as *Address of the remote site's VPN gateway*. When using PSKs you need to enter either the IP address of the remote VPN gateway or its DynDNS name. *%any* won't work because this would require the *Aggressive Mode* which is not supported by the mGuard in the current version.

3.2.10 Poor VPN throughput in a Windows environment

Please read the application note “Windows 2000/XP TCP Tuning for High Bandwidth Networks” which can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*).

Microsoft has really done a remarkable job. The TCP implementation includes virtually all of the recent extensions to improve performance but the default values of some parameters are too conservative and need to be adjusted for getting the optimum of performance. Usually you won't notice the reduced performance during your normal work but it gets visible when making performance measurement.

Tuning the Windows TCP settings according to this document will not only increase the VPN throughput. It will also increase the overall performance of your network. For low delay networks we could increase the overall performance by a factor of **1.8** and the VPN throughput by a factor of **1.5**. For high delay networks with an RTT of 40ms we could increase the overall performance by a factor of **11.7** and the VPN throughput by a factor of **3.4**. This is a remarkable result, which makes it worth to tune the Windows TCP settings.

3.3 L2TP

3.3.1 L2TP connection doesn't work anymore after applying a Windows update/SP

Previous releases of Windows were strict in the used ports for the L2TP connection. They used the ports *from port = 1701 and to port = 1701*. This is supported on the mGuard with the setting *Connection Type = Transport (L2TP Microsoft)*. This was changed by Microsoft starting with Windows XP, Service Pack 2. Therefore you need to set *Connection Type = Transport (L2TP SSH Sentinel)* which supports *from port = any and to port = 1701*.

3.3.2 How do I setup an L2TP connection between a Windows client and the mGuard?

Please download the document *mGuard Configuration examples* from our homepage (www.innominat.com, *Download Documentation*). It describes in detail the required steps for setting up an L2TP connection between a Windows client and the mGuard.

3.3.3 Windows client error #789

Verify that the Windows service *IPsec Policy Agent* is up and running. If you have installed a VPN client previously (e.g. SSH Sentinel) it is possible that this VPN client turned off this service.

3.3.4 Windows client error #792

- mGuard Log: initial Main Mode message received on xxx.xxx.xxx.xxx:500 but no connection has been authorized with policy=RSASIG
 - Check which Windows Service Pack is installed and the selected encryption algorithm for the ISAKMP SA. W2k without SP supports only DES, starting with SP2 3DES is also supported.
- mGuard Log: cannot respond to IPsec SA request because no connection is known for xxx.xxx.xxx.xxx[CN=mGuard, C=de, L=Berlin, ST=Germany, O=Innominat, OU=Support, E=support@innominat.com]:17/1701...yyy.yyy.yyy.yyy[CN=Windows, C=de, L=Berlin, ST=Germany, O=Innominat, OU=Support, E=support@innominat.com]:17/1701
 - Switch *Connection Type* from *Transport (L2TP Microsoft)* to *Transport (L2TP SSH Sentinel)* or vice versa. Previous releases of Windows were strict in the used ports for the L2TP connection. They used the ports *from port = 1701 and to port = 1701*. This is supported on the mGuard with the setting *Transport (L2TP Microsoft)*. This was changed by Microsoft starting with Windows XP, Service Pack 2. Therefore you need to set *Connection Type = Transport (L2TP SSH Sentinel)* which supports *from port = any and to port = 1701*.

3.4 Interoperability

3.4.1 Astaro 5/6

An interoperability guide for setting up a VPN tunnel between mGuard and Astaro can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.2 Astaro Security Gateway 220?

An interoperability guide for setting up a VPN tunnel between mGuard and Astaro Security Gateway 220 can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.3 Bintec VPN Access 25?

An interoperability guide for setting up a VPN tunnel between mGuard and Bintec VPN Access 25 can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.4 Check Point NGX (R60)

An interoperability guide for setting up a VPN tunnel between mGuard and Check Point NGX (R60) can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.5 Cisco PIX

An interoperability guide for setting up a VPN tunnel between mGuard and Cisco PIX can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.6 Cisco VPN3000 Concentrator Series

An interoperability guide for setting up a VPN tunnel between mGuard and Cisco VPN3000 Concentrator can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.7 Fortigate-60

An interoperability guide for setting up a VPN tunnel between mGuard and Fortigate can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up a VPN tunnel between the mGuard and the Fortigate, using PSK or PKI with X.509 certificates.

3.4.8 Netgear FVS338

An interoperability guide for setting up a VPN tunnel between mGuard and Netgear FVS338 can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up a VPN tunnel between the mGuard and the Netgear FVS338, using PSK or PKI with X.509 certificates.

3.4.9 Netscreen 5GT/204/5400

An interoperability guide for setting up a VPN tunnel between mGuard and Netscreen 5GT/204/5400 can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.10 TrustGate5

An interoperability guide for setting up a VPN tunnel between mGuard and TrustGate can be downloaded from our homepage (www.innominat.com, *Download AppNotes & Interops*). It describes in detail the required steps for setting up the VPN tunnel, using PSK or PKI with X.509 certificates.

3.4.11 VPN problems with Cisco devices

Usually the ISAKMP SA and IPsec SA lifetimes are negotiated when the connection is established, even if different values are specified on the gateways. Cisco devices require that exactly the same values for the ISAKMP SA and IPsec SA lifetimes are defined on both gateways. Verify this when encountering problems with a VPN connection between the mGuard and a Cisco device.

3.4.12 Problems establishing a VPN across a Lancom router (model 1611)

This problem may occur when using an older firmware version (e.g. 3.5x) of the router. Upgrade the router to a current firmware version (e.g. 5.x).

3.4.13 VPN tunnel between mGuard and Astaro doesn't work

- When using X.509 certificates, ensure that *X.509v3 Distinguished Name (DN)* is selected as VPN identifier on the Astaro. Please contact support@innominat.com if you need to use either *Email Address* or *IP Address* as VPN identifier.
- Ensure that *IP Compression* is turned off on the Astaro. The mGuard does not support this feature.

4 Firewall

4.1 Which rules do I need to follow when configuring the firewall?

- The firewall rules will be checked one by one, starting with the first rule. If one rule matches the criteria, independent from the action (Accept, Reject or Drop), then the following rules won't be considered.
- The entries *From Port* and *To Port* are only considered if *Protocol* is set to UDP or TCP. Otherwise those entries won't have any effect. Note that the following rule will reject all data packages because *Protocol=All* and therefore the specified *To Port=80* will be ignored: *Protocol=All, From IP=0.0.0.0/0, From Port=any, To IP=0.0.0.0/0, To Port=80, Action=Reject*

4.2 Do I also need to configure incoming firewall rules?

You only need to do this if you'd like to make services on your computer accessible for other remote users. The mGuard uses *stateful filtering*. If a connection was established by your computer then the firewall will let in all data packets which belong to this connection.

4.3 I'd like to prevent access to the Internet but it doesn't work

Note that you need to specify *Protocol=TCP, From Port=any* and *To Port=80* for preventing access to the internet. If you also have specified *From Port=80* then this rule will not work because HTTP requests from web browser use a port ≥ 1024 .

4.4 What's the meaning of the abbreviations in the firewall log?

Please download the application note *mGuard Firewall Logging* from our homepage (www.innominate.com, *Download AppNotes & Interops*). This document describes in detail the abbreviations used in the firewall log.

4.5 ICMP echo requests from the client to the mGuard do not appear in the FW log

This is correct because those ICMP packets do not need to pass the firewall.

4.6 I can reach the clients of the internal network through port forwarding although the incoming FW should prevent it

This is correct. Port forwarding has a higher priority than the firewall therefore port forwarding overrules the incoming firewall.


4.7 Port scanner reports "Port xxxx CLOSED" though I've allowed this port

Port scanner send their request from any port (>1024) to the specified one. Therefore a rule like e.g. *From Port = xxxx* and *To Port = xxxx* won't match. You need to specify e.g. *From Port = any* and *To Port = xxxx*.

4.8 MAC filter: Restricted IPv4 access doesn't work

The IPv4 access to the internal network of the mGuard should be restricted for a subset of MAC addresses. Nevertheless it is possible to gain access to the internal network from any other machine of the external network. In contrast to the stateful inspection firewall, all ARP and IPv4 frames will pass the MAC filter by default. If the MAC filter should restrict the access for specific MAC addresses then you need to define a final rule for IPv4, which drops everything else.

```
Source MAC = xx:xx:xx:xx:xx:xx
Destination MAC = xx:xx:xx:xx:xx:xx
Ethernet protocol = IPv4
Action = Drop
```

 **Note:** MAC filtering is only supported for the *Stealth* mode.

4.9 When do I need to use 1:1 NAT?

1:1 NAT is used for example for connecting several subnets with the same network IP (e.g. 192.168.0.0/24) to the "main" network. 1:1 NAT mirrors addresses from the internal network to the external network. Depending on the specified netmask the host address field of the IP address will be kept unchanged and the network address is masqueraded. Please refer to the *mGuard Configuration Examples* which can be downloaded from our homepage (www.innominate.com, *Download Documentation*).

4.10 Poor firewall throughput

Go to the menu *Network -> Interfaces*, tab *Hardware* and check the current transfer mode (FDX = Full Duplex, HDX = Half Duplex) of the interfaces. It is possible that one of the interfaces uses HDX even if the network uses FDX. This can be caused by some NICs which are not configured to use auto-negotiation or does not support auto-negotiation correctly. In those cases the mGuard can detect the transfer rate but not the transfer mode and will switch to HDX. This of course will reduce the performance.

If one of the interfaces use HDX and you are sure that the network uses FDX, set *Automatic Configuration = No* and specify the desired transfer rate and transfer mode with the *Manual Configuration* settings.

5 Services

5.1 I have entered a NTP server and enabled this service but it doesn't work

Note that you also need to specify a valid name server (menu *Network* -> *DNS*, tab *DNS Server*). Otherwise the IP address of the NTP server can't be resolved.

5.2 Problems with DHCP Relay

Consider the following points when configuring DHCP relay:

- The mGuard must have a static external IP address.
- The DHCP server must know to which gateway the response needs to be sent. On the DHCP server, you must either specify the external IP address of the mGuard as default gateway or add a route to the internal network of the mGuard.

5.3 How do I need to configure the mGuard for using DynDNS.org?

In the following example we want to configure the mGuard to register its public IP address under the name *mguard.dyndns.org*:

Menu: *Network* -> *DNS*, tab *DynDNS*

Registration Register this mGuard at a DynDNS Service? = Yes
Refresh Interval (sec) = 420 (default)
DynDNS Provider = DynDNS.org
DynDNS Server = dyndns
DynDNS Login = <username>
DynDNS Passwort = <password>
DynDNS Hostname = mguard.dyndns.org

6 Anti Virus Protection (AVP)

6.1 I have requested the AVP license but I still don't have received it

Note that a second screen appears for validating the entered data after clicking at <Submit>. The license request will be sent to us after confirming the data in the second screen. If the second screen doesn't appear then some of the entered data (Voucher Serial Number, Voucher Key) were wrong. You'll get an automatic reply once we have received your license request. If you have received a Voucher number xxOxxxxx (e.g. 24O21003) the third character is the character 'O' and not the number zero.

6.2 License request: The screen for confirming the entered data does not appear

Some of the entered data (Voucher Serial Number, Voucher Key) were wrong. If you have received a Voucher number xxOxxxxx (e.g. 24O21003) the third character is the character 'O' and not the number zero.

6.3 Email with attachment can't be scanned and blocks subsequent emails

This problem is caused by the email client, which downloads the mails from the email server sequential. If one email can't be downloaded from the email server then this email will block the download of subsequent emails. Change the setup of your email client to download only the header line of an email if the size exceeds a predefined value.

7 Third Party Products

7.1 Stealth mode: Cisco firmware upgrade through TFTP doesn't work

Even if the TFTP server is started on the client, the upload will be initiated by the Cisco router. Therefore the incoming firewall of the mGuard must allow UDP traffic on port 69.

7.2 Stealth mode: Access to Lotus Notes server with mGuard 10-20 times slower

Go to the menu *Network -> Interfaces*, tab *Hardware*, and check the current transfer mode (FDX = Full Duplex, HDX = Half Duplex) of the interfaces. It is possible that one of the interfaces uses HDX even if the network uses FDX. This can be caused by some NICs which are not configured to use auto-negotiation or does not support auto-negotiation correctly. In those cases the mGuard can detect the transfer rate but not the transfer mode and will switch to HDX. This of course will reduce the performance.

If one of the interfaces use HDX and you are sure that the network uses FDX, set *Automatic Configuration = No* and specify the desired transfer rate and transfer mode with the *Manual Configuration* settings.

7.3 Does the mGuard support Novell IPX?

The mGuard does not support IP/IPX because this is a non routable protocol. The mGuard supports MAC filtering starting with version 3.0.0. With this feature it is possible to allow IPX frames to pass in both directions. If rules are specified for other Ethernet protocols than IPv4 and ARP, no filtering will take place except for the MAC address. Note that MAC filtering is supported for *Stealth* mode only.

7.4 Stealth mode: Problems with Microsoft Server and Network Load Balancing (NLB)

The following needs to be considered if you want to secure Microsoft servers, which form a cluster using *Network Load Balancing* (NLB), with mGuards (Stealth mode):

The Microsoft servers exchange information using a proprietary Ethernet protocol with the hex value 886f. Usually the mGuard will block this protocol. The mGuard supports MAC filtering starting with version 3.0.0. With this feature it is possible to allow this protocol to pass the mGuard in both directions.

Apart of this the mGuard needs to be operated in *multiple client stealth* mode because the NICs of the servers have more than one IP address.

Menu *Network Security-> Packet Filter*, tab *MAC Filtering*: The MAC filter is stateless in contrast to the IPv4 stateful inspection firewall. This means that rules must be defined for both directions. You need to define an incoming and outgoing rule with the following parameters for allowing the NLB protocol to pass:

Source MAC = xx:xx:xx:xx:xx:xx
Destination MAC = xx:xx:xx:xx:xx:xx
Ethernet Protocol = 886f
Action = Accept

Note that no filtering except for the MAC address will take place if other protocols are used than IPv4 and ARP.

8 Related Documentation

The following documents can be downloaded from our homepage (www.innominat.com, *Download Documentation* and *Download AppNotes & Interops*). Please check our homepage periodically for updated or additional documents.

8.1 User's Manual

- User Manual mGuard

8.2 Application Notes

- Windows 2000/XP TCP Tuning for High Bandwidth Networks
- Innominate mGuard Rollout Support
- Innominate mGuard Firewall Logging

8.3 Additional Documentation

- mGuard Configuration Examples
- mGuard Update-/Recovery-/Flash-Procedures

8.4 Interoperability

How to setup a VPN tunnel between the mGuard and one of the following devices:

- Astaro V5/V6 (PSK and X.509 Certificates)
- Astaro Security Gateway 220 (PSK and X.509 Certificates)
- Bintec VPN Access 25 (PSK and X.509 Certificates)
- Check Point NGX (R60) (PSK and X.509 Certificates)
- Cisco PIX (PSK and X.509 Certificates)
- Cisco VPN3000 Concentrator (PSK and X.509 Certificates)
- Fortigate 60 (PSK and X.509 Certificates)
- Netgear FVS338 (PSK and X.509 Certificates)
- Netscreen 5GT/204/5400 (PSK and X.509 Certificates)
- TrustGate5 (PSK and X.509 Certificates)