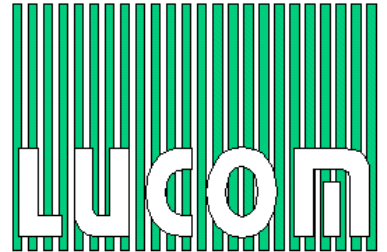


# Innominate **mGuard**

## Industrial Network Security



Innominate  
**certified**  
partner



Innominate  
**mGuard**

**[WWW.LUCOM.DE](http://WWW.LUCOM.DE)**

**LUCOM** GmbH

Komponenten & Systeme  
Ansbacher Str. 2a

**D 90513 Zirndorf**

Tel. +49 (0) 9127 / 59 460-10

Fax. +49 (0) 9127 / 59 460-20

E-Mail: [info@lucom.de](mailto:info@lucom.de)

# Application Note

## mGuard Firewall Logging



***mGuard  
smart***



***mGuard  
PCI***



***mGuard  
blade***



***mGuard  
industrial***

## Table of Contents

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Log Abbreviations</b>   | <b>3</b> |
| <b>2</b> | <b>Firewall Traversal</b>  | <b>4</b> |
| 2.1      | Remote access (HTTPS, SSH, SNMP) to the mGuard   | 4        |
| 2.2      | Traversal  | 4        |
| <b>3</b> | <b>Log Prefix</b>  | <b>5</b> |
| 3.1      | Anti spoofing (fw-in-default-DROP)   | 5        |
| 3.2      | Consistency Check (fw-input-unclean, fw-output-unclean, fw-forward-unclean)                  | 5        |
| 3.3      | Connection Tracking (fw-input-invalid-drop, fw-output-invalid-drop, fw-forward-invalid-drop) | 5        |
| 3.4      | Invalid TCP Flag (fw-invalid-tcp-flags)  | 6        |
| 3.5      | Remote Access (fw-in-[https/ssh/snmp]-admin-<action>)  | 6        |
| 3.6      | Port Forwarding (fw-in-portfw, fw-out-portfw)  | 6        |
| 3.7      | User Firewall (fw-in-<action>, fw-out-<action>, fw-in-default-DROP, fw-out-default-DROP)     | 7        |
| 3.8      | VPN Firewall (fw-vpn-in-<action>-<name>, fw-vpn-out-<action>-<name>)                         | 8        |
| 3.9      | SYN Flood Protection (fw-SYN-flood-protection)   | 8        |
| 3.10     | ICMP Flood Protection (fw-ICMP-flood-protection)   | 8        |

## 1 Log Abbreviations


The following table explains the abbreviations used in the firewall log and their meaning:

| <b>Abbreviation</b>                          | <b>Description</b>   |
|--|--|
| IN (Router Modes)<br>PHYSIN (Stealth Mode)   | Incoming interface.<br>eth0: external interface<br>eth1: internal interface<br>eth2: internal interface of the mGuard PCI (driver mode only)<br>ipsec0: external interface of an IPsec connection<br>ppp0: external interface of a PPPoE/PPTP connection                             |
| OUT (Router Modes)<br>PHYSOUT (Stealth Mode) | Outgoing interface.<br>eth0: external interface<br>eth1: internal interface<br>eth2: internal interface of the mGuard PCI (driver mode only)<br>ipsec0: external interface of an IPsec connection<br>ppp0: external interface of a PPPoE/PPTP connection                             |
| MAC  | This information is displayed only if the protocol is unknown (neither TCP, nor UDP, nor ICMP) and if the packet is send to an external IP address of the mGuard. The format is:<br><source MAC address, 6 octets>:<destination MAC address, 6 octets>:<br><protocol type, 2 octets> |
| SRC  | Source IP address  |
| DST  | Destination IP address   |
| LEN  | Total length of the IP packet in bytes   |
| TOS  | Type of service, field <i>Type</i>   |
| PREC   | Type of service, field <i>Precedence</i>   |
| TTL  | Remaining <i>Time to Live</i> in hops  |
| ID   | Unique ID of the IP datagram, shared by all fragments if fragmented  |
| DF   | Flag <i>Don't fragment</i> is active   |
| PROTO  | Protocol name or number  |
| SPT  | Source port (TCP and UDP)  |
| DPT  | Destination port (TCP and UDP)   |
| WINDOW                                       | The <i>TCP Receive Window</i> size   |
| RES  | Reserved bits  |
| [FLAGS]                                      | When the TCP protocol is used also the TCP flags (e.g. SYN) are displayed.<br>URG=Urgent flag, ACK=Acknowledgement flag, PSH=Push flag, RST=Reset flag, SYN=SYN flag (only exchanged at TCP connection establishment), FIN=FIN flag (only exchanged at TCP disconnection)            |
| URGP   | The <i>Urgent Pointer</i> allows for urgent, "out of band" data transfer   |

### Example:

```
2005-10-26_10:08:00.57668 kernel: fw-in-ACCEPT IN=eth0 OUT=eth1 SRC=10.10.0.2
DST=10.1.0.246 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=47780 DF PROTO=TCP SPT=2670
DPT=80 WINDOW=5840 RES=0x00 SYN URGP=0
```

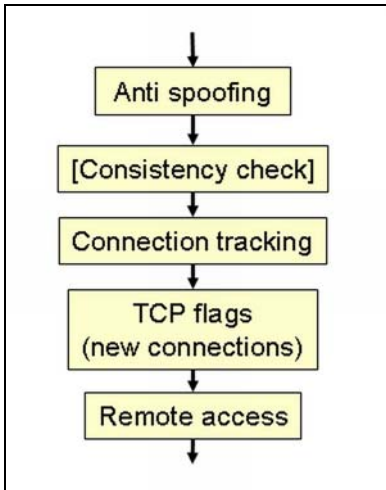
Each log entry starts with the time stamp and a log prefix (e.g. fw-in-ACCEPT). All log prefixes start with **fw-**. The log prefixes are explained below.

 **Note:** If you have activated the NTP service (menu: *Services* -> *NTP*) for synchronizing the time of the device to the local time this has an effect on the timestamps displayed in the web interface only. If you use remote logging the timestamp is displayed in UTC. This makes it easier to compare the logs when you use a central syslog server for registering the logs of different devices which are located in different time zones.

## 2 Firewall Traversal

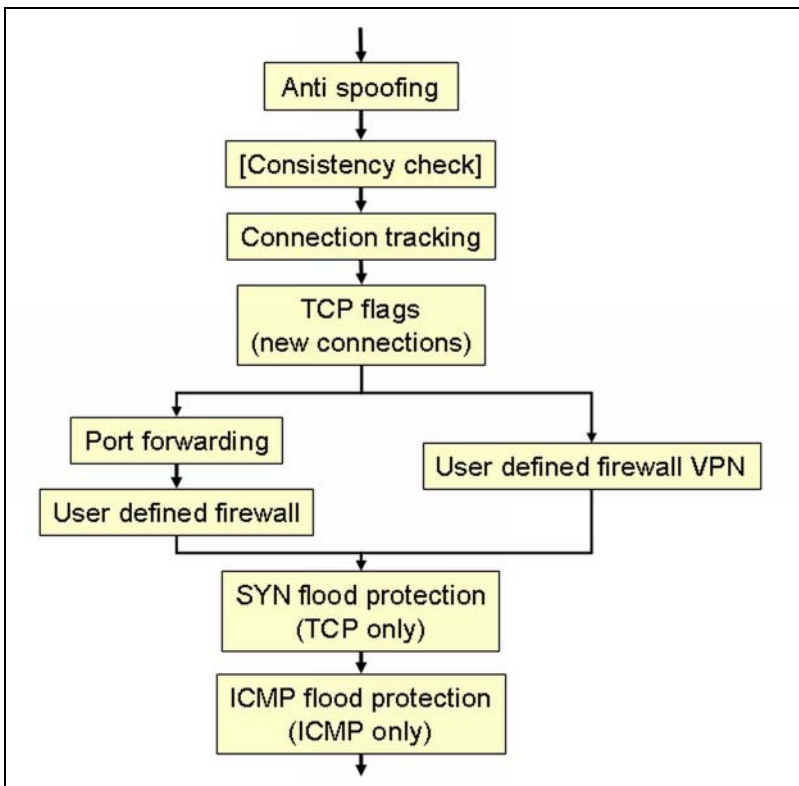
### 2.1 Remote access (HTTPS, SSH, SNMP) to the mGuard

Remote access (HTTPS, SSH, SNMP) data packets are checked by the firewall in the following order:



### 2.2 Traversal

Data packets which should pass the firewall are checked in the following order:



### 3 Log Prefix

#### 3.1 Anti spoofing (fw-in-default-DROP)

The *Anti spoofing* check is performed on all packets which try to establish a new connection from the external to the internal network. The firewall drops the packet with the log prefix **fw-in-default-DROP** if the source IP address belongs to the internal network.

#### 3.2 Consistency Check (fw-input-unclean, fw-output-unclean, fw-forward-unclean)

The firewall performs the consistency check if the option *Enable TCP/UDP/ICMP consistency checks* is enabled in the menu **Firewall -> Extended Settings**. The consistency check is performed on all packets. The firewall checks all TCP/UDP/ICMP packets regarding not permitted or wrong header values (e.g. checksum).


| <i>Log-Prefix</i>  | <i>Description</i>  |
|--------------------|---|
| fw-input-unclean   | Packet which was sent directly to an external or internal IP address of the mGuard.   |
| fw-output-unclean  | Packet which was generated by the mGuard. This log prefix should never occur but it was implemented for the sake of completion. |
| fw-forward-unclean | Packet which would pass the firewall.   |

#### 3.3 Connection Tracking (fw-input-invalid-drop, fw-output-invalid-drop, fw-forward-invalid-drop)

Connection tracking is performed on all packets which do not establish a new connection. The firewall drops the packet if it does not belong to an existing connection.

| <i>Log-Prefix</i>       | <i>Description</i>  |
|-------------------------|---|
| fw-input-invalid-drop   | Packet which was sent directly to an external or internal IP address of the mGuard.   |
| fw-output-invalid-drop  | Packet which was generated by the mGuard. This log prefix should never occur but it was implemented for the sake of completion. |
| fw-forward-invalid-drop | Packet which would pass the firewall.   |

---

 **Note:** Data packets which belong to an existing connection do not appear in the log.

---

### 3.4 Invalid TCP Flag (fw-invalid-tcp-flags)

The firewall checks the validity of the specified TCP flags on all packets which would establish a new connection. The combination of the specified TCP flags is checked and the firewall drops the packet if the flags are not conforming to the specification. The following combinations will cause a drop of the packet:

| <i>Checked flags</i> | <i>Drop condition</i> | <i>Description</i>  |
|----------------------|-----------------------|---|
| ALL                  | FIN, URG, PSH         | All flags are checked. The packet will be dropped if the flags FIN, URG and PSH are set.        |
| ALL                  | NONE                  | All flags are checked. The packet will be dropped if no flag is set.                            |
| SYN, RST             | SYN, RST              | The packet will be dropped if the flags SYN and RST are set.                                    |
| SYN, FIN             | SYN, FIN              | The packet will be dropped if the flags SYN and FIN are set.                                    |
| SYN, ACK, FIN, RST   | RST                   | The flags SYN, ACK and FIN are checked. The packet will be dropped if only the flag RST is set. |

### 3.5 Remote Access (fw-in-[https | ssh | snmp]-admin-<action>)

The log prefix **fw-in-[https | ssh | snmp]-admin-<action>** is a result of the specified firewall rules for remote HTTPS, SSH and SNMP access (menu: Access -> HTTPS, Access -> SSH, Access -> SNMP). <action> can be ACCEPT, REJECT or DROP.

### 3.6 Port Forwarding (fw-in-portfw, fw-out-portfw)


If the logging for port forwarding is enabled (menu: Firewall -> Port Forwarding) then the log prefixes **fw-in-portfw** and **fw-out-portfw** respectively are used.

### 3.7 User Firewall (fw-in-<action>, fw-out-<action>, fw-in-default-DROP, fw-in-default-DROP)

Only packets are checked which would pass the firewall for opening a new connection. The log prefixes **fw-in-<action>** and **fw-out-<action>** are a result of the incoming and outgoing firewall rules which are defined in the menu **Firewall -> Incoming** (from the external to the internal interface) and **Firewall -> Outgoing** (from the internal to the external interface). <action> can be ACCEPT, REJECT or DROP.

If the option **Log entries for unknown connection attempts** is enabled then the log prefixes **fw-in-default-DROP** and **fw-out-default-DROP** respectively are used for such attempts. Also unknown connect requests to an external IP address of the mGuard has the log prefix **fw-in-default-DROP**.

---

 **Note:** Data packets which belong to an existing connection do not appear in the log.

---

#### Examples:

```
fw-out-DROP IN=eth1 OUT=eth0 SRC=192.168.27.100 DST=10.1.80.201 LEN=64  
TOS=0x00 PREC=0x00 TTL=63 ID=44128 DF PROTO=TCP SPT=3936 DPT=21 WINDOW=65535  
RES=0x00 SYN URGP=0
```

The outgoing firewall drops a FTP connect request (DPT=21).

```
fw-out-ACCEPT IN=eth1 OUT=eth0 SRC=192.168.27.100 DST=10.1.80.201 LEN=64  
TOS=0x00 PREC=0x00 TTL=63 ID=44115 DF PROTO=TCP SPT=3937 DPT=80 WINDOW=65535  
RES=0x00 SYN URGP=0
```

The outgoing firewall accepts a HTTP requests (DPT=80).

```
fw-out-REJECT IN=eth1 OUT=eth0 SRC=192.168.27.100 DST=10.1.80.201 LEN=64  
TOS=0x00 PREC=0x00 TTL=63 ID=44100 DF PROTO=TCP SPT=3934 DPT=23 WINDOW=65535  
RES=0x00 SYN URGP=0
```

The outgoing firewall rejects a telnet connection (DPT=23).

### 3.8 VPN Firewall (fw-**vpn-in-*<action>*-*<name>***, fw-**vpn-out-*<action>*-*<name>***)

The log prefixes **fw-*vpn-in-*<action>*-*<name>**** and **fw-*vpn-out-*<action>*-*<name>**** are a result of the incoming (from the external to the internal interface) and outgoing (from the internal to the external) firewall rules which are defined for a VPN connection in the menu **VPN ->**

**Connections.** *<action>* can be ACCEPT, REJECT or DROP. *<name>* is the name of the VPN connection with a maximum of 11 characters. If the name contains more than 11 characters then *<name>* is assembled by the first 7 characters plus two dots plus the last two characters (e.g. name of the VPN connection = VPN\_to\_mGuard, *<name>* = VPN\_to\_..rd).

If the option **Log entries for unknown connection attempts** is enabled then the log prefixes **fw-*vpn-in-DROP-*<name>**** and **fw-*vpn-out-DROP-*<name>**** respectively are used for such attempts.

#### Examples:

```
fw-out-vpn-ACCEPT-mGuard IN=eth1 OUT=ipsec0 SRC=192.168.27.100  
DST=192.168.1.100 LEN=64 TOS=0x00 PREC=0x00 TTL=63 ID=42498 DF PROTO=TCP  
SPT=3857 DPT=21 WINDOW=65535 RES=0x00 SYN URGP=0
```

The outgoing firewall of the VPN connection with the name *mGuard* allows FTP access (DPT=21) to the remote network.

```
fw-out-vpn-DROP-mGuard IN=eth1 OUT=ipsec0 SRC=192.168.27.100  
DST=192.168.1.100 LEN=64 TOS=0x00 PREC=0x00 TTL=63 ID=42518 DF PROTO=TCP  
SPT=3860 DPT=80 WINDOW=65535 RES=0x00 SYN URGP=0
```

The outgoing firewall of the VPN connection with the name *mGuard* drops HTTP requests (DPT=80) to the remote network.

```
fw-out-vpn-REJECT-mGuard IN=eth1 OUT=ipsec0 SRC=192.168.27.100  
DST=192.168.1.100 LEN=64 TOS=0x00 PREC=0x00 TTL=63 ID=42794 DF PROTO=TCP  
SPT=3874 DPT=23 WINDOW=65535 RES=0x00 SYN URGP=0
```

The outgoing firewall of the VPN connection with the name *mGuard* rejects a telnet connection (DPT=23) to the remote network.

### 3.9 SYN Flood Protection (fw-**SYN-flood-protection**)

The limits for new incoming and outgoing TCP connections (SYN flood protection) can be configured through the menu **Firewall -> Extended Settings**. If one of the limits is exceeded then a log entry is issued with the log prefix **fw-*SYN-flood-protection***. Those events are only logged once per second.

### 3.10 ICMP Flood Protection (fw-**ICMP-flood-protection**)

The maximum number of incoming and outgoing ICMP echo requests (ICMP flood protection) can be configured through the menu **Firewall -> Extended Settings**. If one of the limits is exceeded then a log entry is issued with the log prefix **fw-*ICMP-flood-protection***. Those events are only logged once per second.

#### Example:

```
fw-ICMP-flood-protection IN=eth0 OUT=eth1 SRC=10.1.0.27 DST=192.168.1.100 LEN=60  
TOS=0x00 PREC=0x00 TTL=63 ID=40537 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=9472
```