

Innominate mGuard Version 6

Application Note: Firewall Logging



mGuard smart



mGuard PCI



mGuard blade



mGuard industrial RS



EAGLE mGuard



mGuard delta

Innominate Security Technologies AG
Albert-Einstein-Str. 14
12489 Berlin, Germany

Phone: +49 (0)30 6392-3300
Fax: +49 (0)30 6392-3307
contact@innominate.com
<http://www.innominate.com>

Table of Contents

1	Disclaimer	3
2	Log Abbreviations	4
3	Log ID	5
4	Firewall Traversal	6
5	Log Prefixes	7
5.1	<i>Anti Spoofing (fw-antispoofing)</i>	7
5.2	<i>Consistency Check (fw-unclean)</i>	7
5.3	<i>Connection Tracking (fw-invalid)</i>	8
5.4	<i>Remote Access Rules (fw-ssh-access, fw-https-access, fw-snmp-access)</i>	8
5.5	<i>Port Forwarding (fw-portforwarding)</i>	8
5.6	<i>User Firewall (ufw)</i>	9
5.7	<i>Firewall (fw-incoming, fw-outgoing)</i>	9
5.8	<i>VPN Firewall (fw-vpn-<name>-in, fw-vpn-<name>-out)</i>	9
5.9	<i>SYN Flood Protection (fw-SYN-flood)</i>	10
5.10	<i>ICMP Flood Protection (fw-ICMP-flood)</i>	10
5.11	<i>Maximum Size of ICMP Echo Request packets exceeded (fw-ICMP-maxlen)</i>	10

1 Disclaimer

© Innominate Security Technologies AG

April 2008

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

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

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

All information contained in this documentation is subject to change without previous notice.

Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes.

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

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

2 Log Abbreviations

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

Abbreviation	Description
act	Performed action on the packet: DROP, REJECT or ACCEPT.
IN (Router Modes) PHYSIN (Stealth Mode)	Incoming interface. eth0: external interface eth1: internal interface eth2: internal interface of the mGuard PCI (driver mode only) ipsec0: external interface of an IPsec connection ppp0: external interface of a PPPoE/PPTP connection
OUT (Router Modes) PHYSOUT (Stealth Mode)	Outgoing interface. eth0: external interface eth1: internal interface eth2: internal interface of the mGuard PCI (driver mode only) ipsec0: external interface of an IPsec connection 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 sent to an external IP address of the mGuard. The format is: <source MAC address, 6 octets>: <destination MAC address, 6 octets>: <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. 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

3 Log ID

Example of a firewall log entry:

```
2007-09-19_17:25:22.07497 kernel: fw-incoming-1-121e0dc4-a774-1f09-9647-000cbe022aad act=ACCEPT
IN=eth0 OUT=eth1 SRC=10.1.0.46 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=126 ID=57945
DF PROTO=TCP SPT=3053 DPT=445 SEQ=2602365526 ACK=0 WINDOW=65535 RES=0x00 SYN URGP=0 OPT
```

Each log entry starts with the time stamp and the log identifier (e.g. fw-incoming-1-121e0dc4-a774-1f09-9647-000cbe022aad). The log identifier can be used in the menu *Logging -> Browse local logs* for locating the firewall rule which caused the log entry (*Lookup* function).

The log identifier has the following format:

<Log Prefix>-<Rule Number>-<Log ID>

Log Prefix

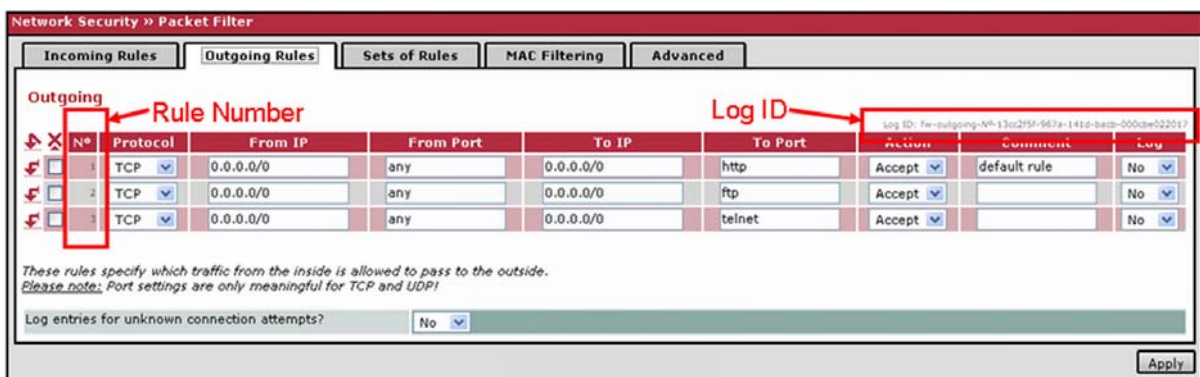
The log prefix indicates at which step of the firewall traversal an action occurred.

Rule Number

The rule number displays the information which configured firewall rule caused the log entry. <Rule Number> = 0 indicates that the log entry is caused by a default firewall rule.

Log ID

Each kind of configured firewall (e.g. incoming rules, outgoing rules, HTTPS remote access) has its own unique log ID. This unique ID is used together with the log prefix and the rule number to locate the firewall rule which caused the log entry (*Lookup* function) in the menu *Logging -> Browse local logs*.

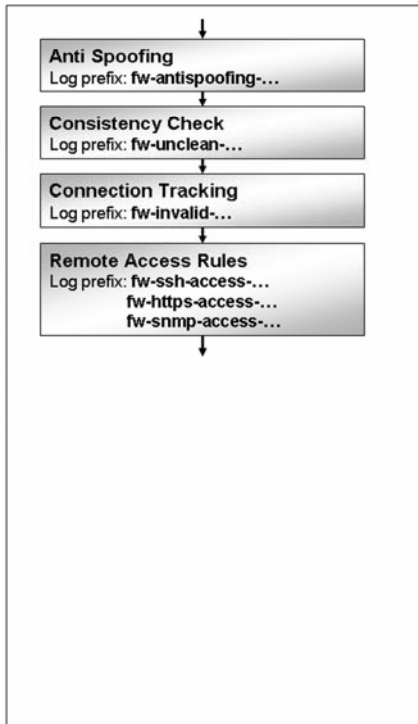


Note: The timezone specified in the menu *Management -> System Settings* (tab *Time and Date*) has an effect on the timestamps displayed in the web interface only. If you use remote logging the timestamp is displayed in UTC. This makes it easier to compare the logs when you use a central syslog server for registering the logs of different devices which are located in different time zones.

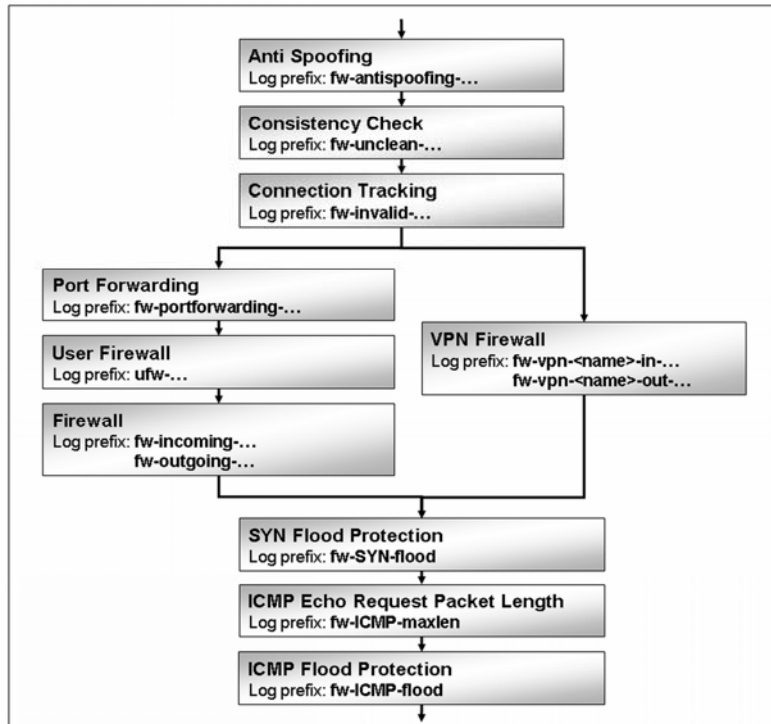
4 Firewall Traversal

Packets which are directed to the mGuard or which need to pass the firewall are checked in the following order:

Remote HTTPS, SSH or SNMP access



Data packets which need to pass the firewall



The purposes of the single checks are explained in the next chapters.

5 Log Prefixes

5.1 Anti Spoofing (fw-antispoofing)

This check is performed on all packets received via an external interface. The firewall drops the packet if the source IP address belongs to the internal network. The log prefix *fw-antispoofing* is followed either by the extension *ext1* or *ext2*, depending on whether the packet was received through the WAN interface (*ext1*) or through the secondary external interface (*ext2*).

Example:

2008-03-28_14:34:19.02184 kernel: **fw-antispoofing-ext1-0- act=DROP** IN=eth0 OUT=eth1 SRC=192.168.80.1 DST=192.168.80.100 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1400 PROTO=TCP SPT=1234 DPT=5678 SEQ=0 ACK=0 WINDOW=1500 RES=0x00 SYN URGP=0

5.2 Consistency Check (fw-unclean)

The firewall performs this check if the option *Enable TCP/UDP/ICMP consistency checks* is enabled in the menu *Network Security -> Packet Filter*, tab *Advanced*. 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. invalid checksum, ports or TCP flags) and drops invalid packets.

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

Examples:

2008-03-31_09:01:18.80548 kernel: **fw-unclean-input-0- act=DROP** IN=eth0 OUT= MAC=00:0c:be:02:20:27:00:13:20:48:d4:e6:08:00 SRC=10.1.0.64 DST=10.1.80.100 LEN=40 TOS=0x00 PREC=0x00 TTL=128 ID=1364 PROTO=TCP SPT=1234 DPT=0 SEQ=0 ACK=0 WINDOW=1500 RES=0x00 SYN URGP=0

2008-03-31_09:01:31.08663 kernel: **fw-unclean-forward-0- act=DROP** IN=eth0 OUT=eth1 SRC=10.1.0.64 DST=192.168.80.100 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1364 PROTO=TCP SPT=1234 DPT=0 SEQ=0 ACK=0 WINDOW=1500 RES=0x00 SYN URGP=0

5.3 Connection Tracking (fw-invalid)

Connection tracking is performed on all packets which do not belong to an established connection. The firewall drops the packet if it does not match an existing connection or if it is out of the current accepted window of sequence numbers.

If the packet belongs to an existing connection, in case of a TCP packet also the validity of the specified TCP flags is verified.

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

Examples:

```
2008-03-31_08:58:20.80170 kernel: fw-invalid-forward-0- act=DROP IN=eth0 OUT=eth1 SRC=10.1.0.64
DST=192.168.80.100 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1364 PROTO=TCP SPT=1234 DPT=5678
SEQ=0 ACK=0 WINDOW=1500 RES=0x00 SYN FIN URGP=0
```

```
2008-03-31_08:58:38.49324 kernel: fw-invalid-input-0- act=DROP IN=eth0 OUT=
MAC=00:0c:be:02:20:27:00:13:20:48:d4:e6:08:00 SRC=10.1.0.64 DST=10.1.80.100 LEN=40 TOS=0x00
PREC=0x00 TTL=128 ID=1364 PROTO=TCP SPT=1234 DPT=5678 SEQ=0 ACK=0 WINDOW=1500 RES=0x00
RST SYN URGP=0
```

5.4 Remote Access Rules (fw-ssh-access, fw-https-access, fw-snmp-access)

Log entries with the prefixes **fw-ssh-access**, **fw-https-access** or **fw-snmp-access** are caused by remote access rules for SSH, HTTPS and SNMP access from the external network with activated logging.

- Remote HTTPS access rules: menu *Management* -> *Web Settings*, tab *Access*.
- Remote SSH access rules: menu *Management* -> *System Settings*, tab *Shell Access*.
- Remote SNMP access rules: menu *Management* -> *SNMP*, tab *Query*.

Examples:

```
2008-03-31_09:37:18.22043 kernel: fw-ssh-access-1-231cca12-63eb-1325-8ec6-000cbe022027
act=ACCEPT IN=eth0 OUT= MAC=00:0c:be:02:20:27:00:0c:be:02:20:17:08:00 SRC=10.1.80.1
DST=10.1.80.100 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=13797 DF PROTO=TCP SPT=1211 DPT=22
SEQ=385453384 ACK=0 WINDOW=65535 RES=0x00 SYN URGP=0 OPT (020405B401010402)
```

```
2008-03-31_09:37:26.58205 kernel: fw-https-access-1-231cca13-63eb-1325-8ec6-000cbe022027
act=ACCEPT IN=eth0 OUT= MAC=00:0c:be:02:20:27:00:0c:be:02:20:17:08:00 SRC=10.1.80.1
DST=10.1.80.100 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=13827 DF PROTO=TCP SPT=1212 DPT=443
SEQ=166932975 ACK=0 WINDOW=65535 RES=0x00 SYN URGP=0 OPT (020405B401010402)
```

5.5 Port Forwarding (fw-portforwarding)

Log entries with the prefix **fw-portforwarding** are caused by configured port forwarding rules (menu *Network Security* -> *NAT*, tab *Port Forwarding*) with activated logging.

Example:

```
2008-03-31_09:42:11.32688 kernel: fw-portforwarding-1-03a047bb-bcd8-1fb7-b972-000cbe022027
act=ACCEPT IN=eth0 OUT=eth1 SRC=10.1.80.1 DST=192.168.80.100 LEN=60 TOS=0x00 PREC=0x00 TTL=63
ID=4788 DF PROTO=TCP SPT=3761 DPT=80 SEQ=1918107032 ACK=0 WINDOW=5840 RES=0x00 SYN
URGP=0 OPT (020405B40402080A0136EF2C0000000001030301)
```

5.6 User Firewall (ufw)

Log entries with the prefix **ufw** are caused by a configured user firewall with activated logging.

Example:

```
2008-03-31_09:45:37.54248 kernel: ufw-ufw00000-1-03a047be-bcd8-1fb7-b972-000cbe022027 act=ACCEPT
IN=eth0 OUT=eth1 SRC=10.1.0.64 DST=192.168.80.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=596
PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=3072
```

5.7 Firewall (fw-incoming, fw-outgoing)

Log entries with the prefixes **fw-incoming** and **fw-outgoing** are caused by configured incoming and/or outgoing firewall rules with activated logging.

- Incoming firewall rules: menu *Network Security -> Packet Filter*, tab *Incoming Rules*.
- Outgoing firewall rules: menu *Network Security -> Packet Filter*, tab *Outgoing Rules*.

Examples:

```
2008-03-31_09:53:08.36783 kernel: fw-incoming-1-231cca17-63eb-1325-8ec6-000cbe022027 act=ACCEPT
IN=eth0 OUT=eth1 SRC=10.1.0.64 DST=192.168.80.100 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=622 DF
PROTO=TCP SPT=1073 DPT=139 SEQ=2707534842 ACK=0 WINDOW=16384 RES=0x00 SYN URGP=0 OPT
(020405B401010402)
```

```
2008-03-31_09:53:32.24494 kernel: fw-outgoing-1-231cca18-63eb-1325-8ec6-000cbe022027 act=ACCEPT
IN=eth1 OUT=eth0 SRC=192.168.80.100 DST=10.1.0.52 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=1090
DF PROTO=TCP SPT=1043 DPT=445 SEQ=3236760052 ACK=0 WINDOW=65535 RES=0x00 SYN URGP=0 OPT
(0204056401010402)
```

5.8 VPN Firewall (fw-vpn-<name>-in, fw-vpn-<name>-out)

Log entries with the prefixes **fw-vpn-<name>-in** and **fw-vpn-<name>-out** are caused by configured incoming and/or outgoing VPN firewall rules (menu *IPsec VPN -> Connections*, tab *Firewall*) with activated logging.

<name> is the mGuard's internal name for the VPN connection. The relation between name of the VPN connection and its mGuard's internal name is displayed in the menu *IPsec VPN -> IPsec Status*.

Examples:

```
2008-03-31_09:58:22.56457 kernel: fw-vpn-v000_000-in-1-231cca1b-63eb-1325-8ec6-000cbe022027
act=ACCEPT IN=ipsec0 OUT=eth1 SRC=192.168.27.1 DST=192.168.80.100 LEN=48 TOS=0x00 PREC=0x00
TTL=126 ID=21873 DF PROTO=TCP SPT=1273 DPT=139 SEQ=807608871 ACK=0 WINDOW=65535 RES=0x00
SYN URGP=0 OPT (020405B401010402)
```

```
2008-03-31_09:58:38.49604 kernel: fw-vpn-v000_000-out-1-231cca1b-63eb-1325-8ec6-000cbe022027
act=ACCEPT IN=eth1 OUT=ipsec0 SRC=192.168.80.100 DST=192.168.27.1 LEN=48 TOS=0x00 PREC=0x00
TTL=127 ID=1239 DF PROTO=TCP SPT=1048 DPT=445 SEQ=3833457991 ACK=0 WINDOW=65535 RES=0x00
SYN URGP=0 OPT (0204056401010402)
```

5.9 SYN Flood Protection (fw-SYN-flood)

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

Example:

```
2008-03-28_14:06:26.12078 kernel: fw-SYN-flood act=DROP SYN-flood act=DROP IN=eth0 OUT=eth1
SRC=10.1.0.52 DST=192.168.1.100 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=232 PROTO=TCP SPT=1234
DPT=5678 SEQ=0 ACK=0 WINDOW=1500 RES=0x00 SYN URGP=0
```

5.10 ICMP Flood Protection (fw-ICMP-flood)

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

Example:

```
2008-03-28_14:02:26.98026 kernel: fw-ICMP-flood act=DROP IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=10.1.0.58 DST=10.1.0.64 LEN=92 TOS=0x00 PREC=0x00 TTL=255 ID=1427
PROTO=ICMP TYPE=8 CODE=0 ID=41997 SEQ=2304
```

5.11 Maximum Size of ICMP Echo Request packets exceeded (fw-ICMP-maxlen)

The maximum size of allowed ICMP echo request packets can be configured through the menu *Network Security-> Packet Filter*, tab *Advanced* (default value = 65535 bytes). If an ICMP echo request packet exceeds this limit a log entry is issued with the log prefix **fw-ICMP-maxlen**.

Example:

```
2008-03-28_14:11:23.39326 kernel: fw-ICMP-maxlen act=DROP IN=br0 OUT=br0 PHYSIN=eth0
PHYSOUT=eth1 SRC=10.1.0.58 DST=10.1.0.64 LEN=65535 TOS=0x00 PREC=0x00 TTL=255 ID=1589
PROTO=ICMP TYPE=8 CODE=0 ID=10255 SEQ=768
2008-03-28_14:12:00.11160 gai: WWW_LEVEL changed to "10"
```