Innominate mGuard Version 5

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
www.innominate.com

Table of Contents

1 Disclaimer

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 *Type*
PREC	Type of service, field *Precedence*
TTL	Remaining *Time to Live* in hops
ID	Unique ID of the IP datagram, shared by all fragments if fragmented
DF	Flag *Don't fragment* is active
PROTO	Protocol name or number
SPT	Source port (TCP and UDP)
DPT	Destination port (TCP and UDP)
WINDOW	The *TCP Receive Window* 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 *Urgent Pointer* allows for urgent, "out of band" data transfer

Example:

```
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).

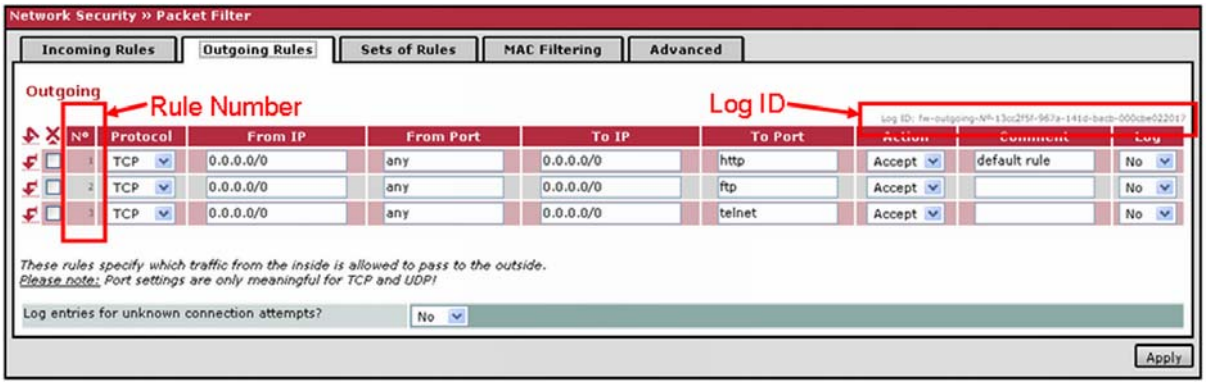
The log identifier has the following format:

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

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

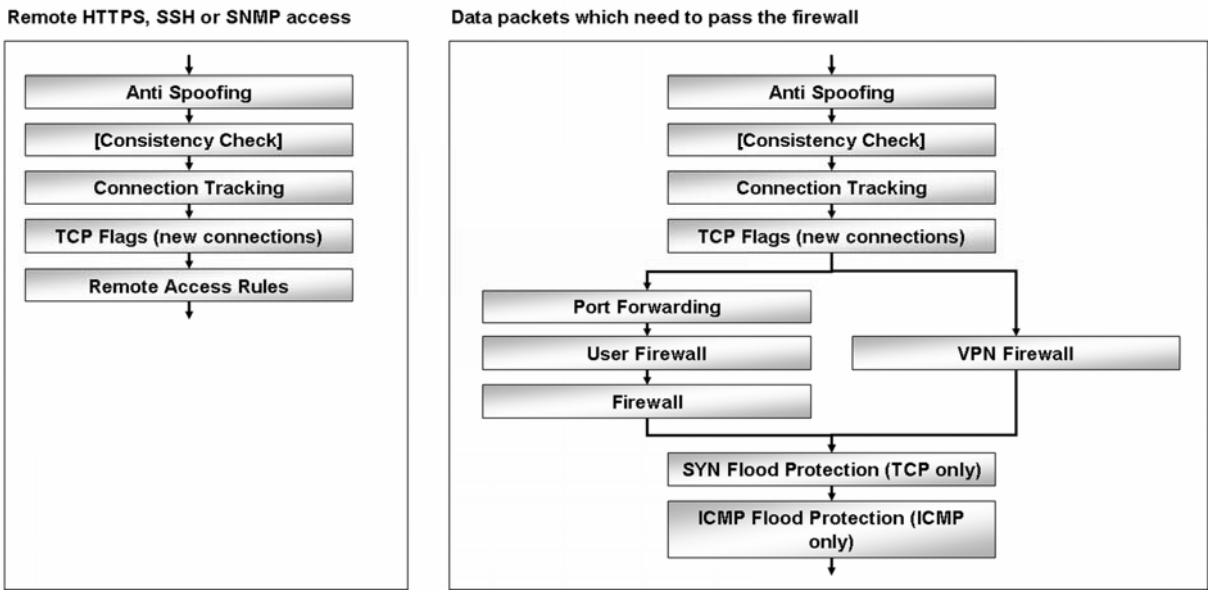
Rule Number
The rule number displays the information which configured firewall rule caused the log entry. <Rule Number> = 0 indicates that the log entry is caused by a default firewall rule.

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 for locating the firewall rule which caused the log entry (*Lookup* function) in the menu *Logging -> Browse local logs*.



Note: If you have activated the NTP service (menu: *Management -> System Settings*, tab *Time and Date*) for synchronizing the system time with an NTP server, 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.

3 Firewall Traversal



Anti spoofing
This 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 if the source IP address belongs to the internal network.

Consistency check
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) and drops invalid packets.

Connection tracking
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.

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:

Checked flags	*Drop condition*	*Description*
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.

SYN flood protection
The limits for new incoming and outgoing TCP connections per second can be configured through the menu *Network Security -> DoS Protection*. If one limit (incoming and/or outgoing) is exceeded, the firewall drops the packets.

ICMP flood protection
The maximum number of incoming and outgoing ICMP echo requests per second can be configured through the menu *Network Security -> DoS Protection*. If one limit (incoming and/or outgoing) is exceeded, the firewall drops the packets.

4 Log Prefixes

4.1 Consistancy Check and TCP Flags (fw-invalid-input-…, fw-invalid-forward-…, fw-invalid-output-…)

Log entries with the prefixes **fw-invalid-input**, **fw-invalid-forward** or **fw-invalid-output** may be caused either by invalid TCP flags or by a failed consistency check (e.g. wrong checksum).

Log-Prefix	*Description*
fw-input-unclean	Packet which was sent directly to the external or internal interface 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.

Example (invalid TCP flags):

2007-10-10_16:07:36.93741 kernel: **fw-invalid-forward**-0- **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 FIN** URGP=0

4.2 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:

2007-10-10_16:03:23.44406 kernel: **fw-ssh-access**-1-1018e08e-f179-1cb3-bbf3-000cbe022aad **act=ACCEPT** fw-0-0-1 act=ACCEPT IN=eth0 OUT= MAC=00:0c:be:02:2a:ad:00:0c:f1:e4:78:54:08:00 SRC=10.1.0.54 DST=10.1.80.100 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=63731 DF PROTO=TCP SPT=4346 DPT=22 SEQ=363370156 ACK=0 WINDOW=65535 RES=0x00 SYN URGP=0 OPT (020404EC0103030001010402)

2007-10-10_16:03:34.62712 kernel: **fw-https-access**-1-1018e08f-f179-1cb3-bbf3-000cbe022aad **act=ACCEPT** fw-0-1-1 act=ACCEPT IN=eth0 OUT= MAC=00:0c:be:02:2a:ad:00:0c:f1:e4:78:54:08:00 SRC=10.1.0.54 DST=10.1.80.100 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=63767 DF PROTO=TCP SPT=4347 DPT=443 SEQ=2097405829 ACK=0 WINDOW=65535 RES=0x00 SYN URGP=0 OPT (020404EC0103030001010402)

4.3 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:

2007-10-10_15:57:14.75422 kernel: **fw-portforwarding**-1-1018e08c-f179-1cb3-bbf3-000cbe022aad **act=ACCEPT** 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

4.4 User Firewall (ufw-…)

Log entries with the prefix **ufw** are caused by an activated used firewall with activated logging.

Example:

2007-10-10_15:34:17.31458 kernel: **ufw-**ufw00000-1-1018e08b-f179-1cb3-bbf3-000cbe022aad **act=ACCEPT** IN=eth0 OUT=eth1 SRC=10.1.0.52 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=2177 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=11008

4.5 Firewall, Anti-Spoofing and Connection Tracking (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:

2007-10-10_15:25:35.15495 kernel: **fw-incoming**-1-1018e085-f179-1cb3-bbf3-000cbe022aad **act=ACCEPT** 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

2007-10-10_15:28:29.68717 kernel: **fw-outgoing**-1-1018e089-f179-1cb3-bbf3-000cbe022aad **act=REJECT** IN=eth1 OUT=eth0 SRC=192.168.1.100 DST=10.1.0.254 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=1073 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=2304

If received data packets do not belong to an existing connection (*Connection Tacking*) the packets are dropped (act=DROP).

If the *Anti spoofing* check succeeded on a packet, the log prefix **fw-incoming** is displayed with **act=DROP**. In this case the displayed SRC IP address belongs to the internal network.

Example:

2007-09-20_10:36:25.06867 kernel: **fw-incoming**-1-121e0dc5-a774-1f09-9647-000cbe022aad **act=DROP** IN=eth0 OUT=eth1 **SRC=192.168.1.1 DST=192.168.1.100** LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1276 PROTO=TCP SPT=1234 DPT=5678 SEQ=0 ACK=0 WINDOW=1500 RES=0x00 SYN URGP=0

4.6 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:

2007-10-10_15:05:43.60093 kernel: **fw-vpn-**v000_000**-in**-1-1018e080-f179-1cb3-bbf3-000cbe022aad **act=ACCEPT** IN=ipsec0 OUT=eth1 SRC=192.168.80.100 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=126 ID=1528 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=1280

2007-10-10_15:08:06.53609 kernel: **fw-vpn-**v000_000**-out**-1-1018e080-f179-1cb3-bbf3-000cbe022aad **act=ACCEPT** IN=eth1 OUT=ipsec0 SRC=192.168.1.100 DST=192.168.80.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=986 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=1024

4.7 SYN Flood Protection (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 **SYN-flood**. Those events are only logged once per second.

Example:

2007-10-10_14:56:56.33045 kernel: **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

4.8 ICMP Flood Protection (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 **ICMP-flood**. Those events are only logged once per second.

Example:

2007-10-10_14:59:31.22647 kernel: **ICMP-flood act=DROP** ICMP-flood act=DROP IN=eth0 OUT=eth1 SRC=10.1.0.52 DST=192.168.1.100 LEN=92 TOS=0x00 PREC=0x00 TTL=254 ID=1432 PROTO=ICMP TYPE=8 CODE=0 ID=40962 SEQ=768

5 Related Documentation

The following documents can be downloaded from our homepage (www.innominate.com -> *Downloads -> Documentation* and *Downloads -> Application Notes*). Please check our homepage periodically for updated or additional documents.

User's Manual
- User Manual mGuard

Application Notes
- Windows 2000/XP TCP Tuning for High Bandwidth Networks
- Innominate mGuard Rollout Support

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

Interoperability Guides
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 1812 (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)
- Microsoft ISA Server 2004 (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)