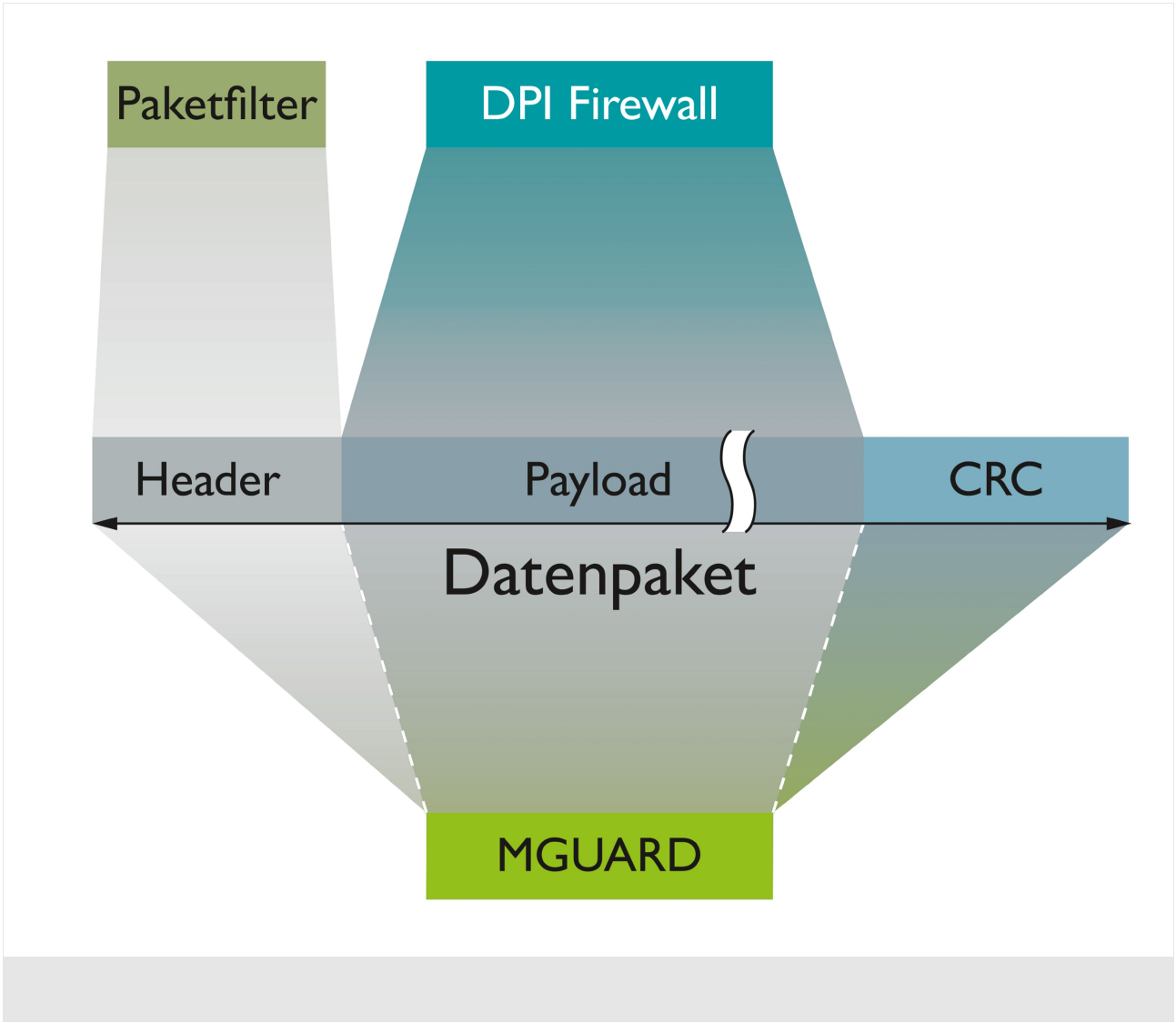

FL MGUARD 2000/4000 Logging / Firewall logging mGuard 10.5.0

Application note

Application note

FL MGUARD 2000/4000 - Logging / Firewall logging mGuard 10.5.0

AH EN MGUARD LOGGING, Revision 00 2025-06-17

This Application note is valid for the following mGuard devices:

Device	Item No.
FL MGUARD 4302 (KX)	1357840 (1696708)
FL MGUARD 4305 (KX)	1357875 (1696779)
FL MGUARD 2102	1357828
FL MGUARD 2105	1357850
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842
Firmware version: mGuard 10.5.0	

The applicable documentation is available for download at phoenixcontact.net/product/<item number>:

112008_en_00

1 Logging / Firewall-Logging

Document-ID: 112008_en_00
Document-Description: AH EN MGUARD LOGGING
© PHOENIX CONTACT 2025-06-17

Make sure you always use the latest documentation.
It can be downloaded using the following link pphoenixcontact.net/products.

Contents of this document

This document describes which events are logged in the log entries of mGuard devices and which abbreviations and log prefixes are used.

1.1 Introduction

The mGuard device logs general system statuses, configuration changes and actions performed on or by the device.

This includes actions performed by the mGuard firewall, user logins and logouts and changes to the device configuration.

The log entries are identified by specific designations and log prefixes. This document briefly describes the log entries and the log prefixes. The aim is to facilitate the interpretation of log entries.

1.2 Classification into log categories

The log entries used on mGuard devices can be divided into categories to simplify matters. The following table provides an overview of important log categories and describes which events are logged in each case.

Table 1-1 Categories of log entries (examples)

Category	Detail
Common	

User (Login/Logout)	– Login/logout (HTTPS / SSH / SNMP):
	  – Login of users
	  – Login of firewall users
	  – Login error
	  – Manual logout / logout via timeout

User administration	– Change password – Configure, change or delete user firewall template – Create, change or delete firewall user
Change configuration / Configuration profiles	– Change configuration (including parameters) – Create or delete configuration profile – Upload or download configuration profile – Apply configuration profile – Save configuration to SD card or load/apply from SD card.
Certificates	– Upload or delete certificates
Hardware changes	– Insert or remove SD card – Connect or disconnect network cable
Connectivity	– Network configuration received via DHCP – Network cable removed / connected
Update	– Perform firmware update – Add, change or delete update server
Remote logging (syslog)	– Configure, activate or deactivate remote syslog server connection
Redundancy	– Operate two mGuard devices in firewall redundancy mode

Table 1-1 [...]Categories of log entries (examples)

Category	Detail
Network Security	
Firewall	– Firewall rule applies and is applied (logging must be activated) – Firewall rule set is applied (logging must be activated) – Unknown connection attempt (logging must be activated) – Create, change or delete firewall rule – Configure, change or delete user firewall template – Anti-spoofing measures – DoS protection measures – Measures in the course of consistency checks
IPsec VPN	
IPsec VPN	– IPsec VPN connection is established or terminated – Connection (setup) error
OpenVPN Client	
OpenVPN	– OpenVPN connection is being established or terminated – Connection (setup) error
DHCP Server/Relay	
DHCP	– Network configuration assigned to a network client via DHCP
SNMP/LLDP	
SNMP	– Monitor or manage SNMP device via SNMP – Determine or send information about the network infrastructure via LLDP
LDAP	
Dynamic Routing	
OSPF	– Distribute OSPF routing information via OSPF protocol

1.3 Log entry (General)

1.3.1 User login/logout

Web based management (web interface)

Log entry	Description
Webinterface action	A user is logged on or off via the WBM. Authentication takes place on the mGuard device directly or via a RADIUS server. Unsuccessful login attempts and automatic logouts are also logged. If the user is logged in and authenticated using the RADIUS server, the user name configured on the RADIUS server appears as the user name. Unsuccessful login attempts and manual logout or logout after a session timeout are also logged. The logon and logoff of firewall users is also logged.

Example:

2025-03-06_13:05:32.24439 **Webinterface**: Accepted login for 'user-bob' role 'admin' from 192.168.1.55 by Web
2025-03-06_13:06:32.24439 **Webinterface:** Logout for 'user-bob' role 'admin' from 192.168.1.55 by timeout
2025-03-06_13:07:32.24439 **Webinterface**: Failed login for '*******' role '*******' from 192.168.1.55 by Web
2025-05-05_10:23:19.72490 **action**: user-fred:admin performed the action 'userfw/login' via Webinterface 2025-05-05_10:23:19.72586 **Webinterface**: Accepted login for firewall user user-fred' from 192.168.1.55
2025-05-05_10:23:44.91426 **action**: Technician_Bob:admin performed the action 'userfw/logout' via Webinterface 2025-05-05_10:23:44.91568 **Webinterface**: Logout for firewall user 'user-fred' from 192.168.1.55

Shell access (sshd)

Log entry	Description
sshd	A user is logged on or off via the shell access of the mGuard device.
inno-sshlimitd	Unsuccessful login attempts and manual logouts or logouts after a session timeout are also logged.

Example:

2025-03-06_13:21:03.24439 **sshd[28654]**: Accepted password for admin from 192.168.1.55 port 53721 ssh2
2025-03-06_13:21:04.00270 **inno-sshlimitd**: accepting new connection at fd 6
2025-03-06_13:21:05.00315 **inno-sshlimitd**: allow session 1 of maximum 4 for role admin (class 1) at fd 6
2025-03-06_13:21:09.00896 **sshd[28659]**: session start for user 'admin'
2025-03-06_13:24:10.00896 **sshd[28666]**: Closing connection for admin from 192.168.1.55 port 53716
2025-03-06_13:24:10.00896 **sshd[28766]** Failed password for admin from 192.168.1.55 port 53933 ssh2

1.3.2 Change user password

Log entry	Description
maid usermod	A user password is changed.

Example:

2025-05-05_10:03:40.39609 **maid**[12436]: User 'admin' performed a configuration change with role 'admin':

2025-05-05_10:03:40.39628 **maid**[12436]: WWW_PASSWORD_RAW set to '******'

2025-05-05_10:03:40.42302 **usermod**[23853]: change user 'admin' password

1.3.3 Change configuration

Log entry	Description
maid	A user makes a configuration change. The changed parameters are logged. If the user is logged in and authenticated using the RADIUS server, the user name configured on the RADIUS server appears as the user name.

Example:

2025-03-06_13:41:43.27927 **maid**[12341]: User 'admin' performed a configuration change with role 'admin':

2025-03-06_13:41:43.27947 **maid**[12341]: NTP_SERVERS new row 0

2025-03-06_13:41:43.27984 **maid**[12341]: NTP_SERVERS:0.NTP_SERVER set to 'pool.ntp.org'

2025-03-06_13:41:43.27998 **maid**[12341]: NTP_SERVERS:0.PREFER_VPN set to 'no'

2025-03-06_13:41:43.28073 **maid**[12341]: NTP_SERVERS new row 1

2025-03-06_13:41:43.28087 **maid**[12341]: NTP_SERVERS:1.NTP_SERVER set to 'pool.ntp.net'

2025-03-06_13:41:43.28116 **maid**[12341]: NTP_SERVERS:1.PREFER_VPN set to 'no'

1.3.4 Use configuration profiles (ATV / ECS)

Log entry	Description
action service-ihald ECS-save	A configuration profile is created, uploaded, downloaded or applied.

Example:

As ATV profile

2025-05-05_09:47:08.18954 **action**: admin:admin performed the action 'profile/save' via Webinterface

2025-05-05_09:47:44.33517 **action**: admin:admin performed the action 'profile/download' via Webinterface

2025-05-05_09:49:50.58022 **action**: admin:admin performed the action 'profile/upload' via Webinterface

2025-05-05_09:50:18.32148 **action**: admin:admin performed the action 'profile/restore' via Webinterface

On ECS/SD card

Create / Save

2025-05-05_12:38:43.92085 **service-ihald**: INFO: Writing the configuration to the external config storage.

2025-05-05_12:38:47.00398 **syslog**: Generic SD card found.

2025-05-05_12:38:47.03468 **ECS-save**: saved configuration

2025-05-05_12:38:47.03918 **service-ihald**: INFO: Finished writing the configuration to the external config storage.

2025-05-05_12:38:47.06146 **action**: admin:admin performed the action 'ecs/save' via Webinterface

Hochladen / Anwenden

2025-05-05_12:42:03.69947 **service-ihald**: INFO: The configuration from the external config storage differs from the device.

2025-05-05_12:42:03.71027 **ECS-load**: Configuration restored from external config storage.

2025-05-05_12:42:03.82098 **action**: admin:admin performed the action 'ecs/load' via Webinterface

1.3.5 Execute action

Log entry	Description
action	An action is executed by a user with a specific user role (user name:role). If the user is logged in and authenticated using the RADIUS server, the user name configured on the RADIUS server appears as the user name.

Example:

2025-03-06_13:44:29.56656 **action**: admin:admin performed the action 'tools/snapshot' via Webinterface
2025-03-06_13:45:09.97690 **action**: admin:admin performed the action 'tools/tcpdump-start' via Webinterface
2025-05-05_10:26:34.81534 **action**: admin:admin performed the action 'update/patches' via Webinterface

1.3.6 Create firewall user

Log entry	Description
maid	A firewall user is configured or an already configured firewall user is changed or adapted.

Example:

2025-05-05_10:14:55.23385 **maid**[12435]: User 'admin' performed a configuration change with role 'admin':

2025-05-05_10:14:55.23403 **maid**[12435]: USERFW_TEMPLATE new row 0

2025-05-05_10:14:55.23420 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_COMMENT set to ''

2025-05-05_10:14:55.23436 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_ENABLED set to 'yes'

2025-05-05_10:14:55.23453 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_NAME set to 'Firewall-User-01'

2025-05-05_10:14:55.23467 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_RULE:0.COMMENT set to ''

2025-05-05_10:14:55.23483 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_RULE:0.DST_IP set to '0.0.0.0/0'

2025-05-05_10:14:55.23496 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_RULE:0.DST_PORT set to 'any'

2025-05-05_10:14:55.23512 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_RULE:0.LOG set to 'no'

2025-05-05_10:14:55.23526 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_RULE:0.PROTO set to 'all'

2025-05-05_10:14:55.23539 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_RULE:0.SRC_PORT set to 'any'

2025-05-05_10:14:55.23556 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_SRC_IP set to '%authorized_ip'

2025-05-05_10:14:55.23570 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_TIMEOUT set to '28800'

2025-05-05_10:14:55.23651 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_TOUT_TYPE set to 'static'

2025-05-05_10:14:55.23667 **maid**[12435]: USERFW_TEMPLATE:0.TEMPLATE_USERS:0.USERNAME set to 'Technician_01'

2025-05-05_10:14:55.23686 **maid**[12435]: USERFW_TEMPLATE:0.VPN_CONN_REF set to ''

1.3.7 Insert or remove ECS/SD card

Log entry	Description
kernel service-ihald	An SD card is inserted or removed from the device.

Example:

2025-05-05_09:45:59.26220 **kernel**: [245.191375] mmc0: new high speed SDHC card at address 59b4 2025-05-05_09:45:59.26578 **kernel**: [245.193484] mmcblk0: mmc0:59b4 SDC 7.51 GiB 2025-05-05_09:45:59.26631 **kernel**: [245.195280] mmcblk0: p1 2025-05-05_09:46:00.71116 **service-ihald**: INFO: An external config storage medium was inserted.
2025-05-05_09:43:51.42165 **kernel**: [117.347900] mmc0: card 59b4 removed

1.3.8 Perform an update

Log entry	Description
action psm-sanitize	An update or attempt to update the firmware is carried out. Any errors that occur are also logged.

Example:

2025-05-14_07:09:14.96415 **action**: admin:admin performed the action 'update/major' via Webinterface

2025-05-14_07:09:15.03413 **psm-sanitize**: psm-sanitize: info: all packages installed completely.

2025-05-14_07:09:15.04755 **psm-sanitize**: psm-sanitize: info: installing new package set "10.6.0-pre19-beta06.default"...

2025-05-14_07:09:15.63286 **psm-sanitize**: psm-wget: download failed for URL https://***@update.innominate.com//aarch64/major/10.6.0.default: HTTP/1.1 404 Not Found

2025-05-14_07:09:15.64362 psm-sanitize: psm-install: fatal: download of package set "10.6.0.default" failed (107)

2025-05-14_07:09:15.65645 **psm-sanitize**: psm-sanitize: info: psm-install 10.6.0.default failed: 107

2025-05-14_07:09:15.66465 **psm-sanitize**: psm-sanitize: info: done.

2025-05-14_07:09:15.66947 **psm-sanitize**: psm-sanitize: info: running psm-clean...

2025-05-14_07:09:17.98191 **psm-sanitize**: psm-clean: info: done.

1.3.9 Firewall redundancy

Log entry	Description
ham-ssv / ham-vic ham-av-... conntrackd pluto	An event occurs when two mGuard devices are used as a redundancy pair - with firewall redundancy activated (e.g. switching from one device of the redundancy pair to the other if the previously active device lacks connectivity).

Example:

[...]

2025-05-14_08:03:49.48428 **ham-ssv**: INFO transitioned from outdated to on_standby because availability is failed totally, connectivity is successful, replication is not unknown (outdated)

2025-05-14_08:03:49.48871 **ham-ssv**: INFO transitioned from on_standby to becomes_active because availability is failed totally, connectivity is not unknown (successful), replication is not unknown (outdated)

2025-05-14_08:03:49.49177 **ham-vic**: INFO enabled IP forwarding and other conditions

2025-05-14_08:03:49.49193 ham-ac-int: AC INFO ham-ac(5703,eth1) sending CARP messages and listening to them

2025-05-14_08:03:49.49207 **ham-ac-ext1**: AC INFO ham-ac(5723,eth0) sending CARP messages and listening to them

2025-05-14_08:03:49.50734 **conntrackd**: [Wed May 14 08:03:49 2025] (pid=32161) [notice] committing all external caches

2025-05-14_08:03:49.51356 **conntrackd**: [Wed May 14 08:03:49 2025] (pid=32161) [notice] Committed 115 new entries

2025-05-14_08:03:49.51376 **conntrackd**: [Wed May 14 08:03:49 2025] (pid=32161) [notice] commit has taken 0.006242 seconds

2025-05-14_08:03:49.52332 **conntrackd**: [Wed May 14 08:03:49 2025] (pid=32161) [notice] flushing caches

2025-05-14_08:03:49.53259 **conntrackd**: [Wed May 14 08:03:49 2025] (pid=32161) [notice] resync with master conntrack table

2025-05-14_08:03:49.54625 **conntrackd**: [Wed May 14 08:03:49 2025] (pid=32161) [notice] sending bulk update

2025-05-14_08:03:49.84886 **ham-ssv**: INFO sigalrm (timeout)

2025-05-14_08:03:49.84905 **ham-ssv**: INFO transitioned from becomes_active to active because replication is not 'received final' (outdated), timeout

2025-05-14_08:03:49.85119 **ham-vic**: INFO enabled virtual interface eth1.vif

2025-05-14_08:03:49.85238 **pluto**: pluto[21806]: HA: switching to 'active'

2025-05-14_08:03:49.85242 **pluto**: pluto[21806]: HA: I am active now

2025-05-14_08:03:49.87510 **ham-vic**: INFO Kernel Proxy ARP enabled

[...]

1.3.10 Remove / connect network cable

Log entry	Description
kernel service mauman	A network cable is removed from or connected to the device.

Example:

2025-06-10_09:50:19.27287 **kernel**: [5330.215135] mvneta d0030000.ethernet eth0: Link is Down

2025-06-10_09:50:19.37295 **service-mauman**: [011] Running service loop because an interface changed

2025-06-10_09:50:23.36572 **kernel**: [5334.308092] mvneta d0030000.ethernet eth0: Link is Up - 1Gbps/Full - flow control off

2025-06-10_09:50:23.46578 **service-mauman**: [011] Running service loop because an interface changed

1.3.11 DHCP (Server)

Log entry	Description
dhcp-int dhcp-ext	A network configuration is assigned to a network client by the mGuard DHCP server via DHCP.

Example:

2025-06-11_09:19:06.72032 **dhcp-int**: udhcpd: started, v1.36.1

2025-06-11_09:19:14.35471 **dhcp-int**: udhcpd: sending OFFER to 192.168.100.223

2025-06-11_09:19:14.37093 **dhcp-int**: udhcpd: sending ACK to 192.168.100.223

1.3.12 DHCP (Client)

Log entry	Description
dhclient	The network configuration is requested from a DHCP server and received from it.

Example:

2025-06-11_09:00:41.65347 **dhclient**: udhcpc: Recieved a link-up event, exiting

2025-06-11_09:00:41.65351 **dhclient**:

2025-06-11_09:00:41.65953 **dhclient**: udhcpc: started, v1.36.1

2025-06-11_09:00:41.65957 **dhclient**: udhcpc: Will send DHCP requests.

2025-06-11_09:00:41.68587 **dhclient**: trigger: 'ifchange ext1'

2025-06-11_09:00:41.70078 **dhclient**: udhcpc: broadcasting discover

2025-06-11_09:00:41.75383 service-mauman: [011] Running service loop because an interface changed

2025-06-11_09:00:41.81462 **dhclient**: udhcpc: broadcasting select for 192.168.178.38, server 192.168.100.1

2025-06-11_09:00:41.86462 **dhclient**: udhcpc: lease of 192.168.100.38 obtained from 192.168.100.1, lease time 864000

2025-06-11_09:00:41.90523 **dhclient**: trigger: 'ifchange ext1'

1.3.13 Rebooting the device

Log entry	Description
ham-ssv	The device is restarted by a user or due to an error. The complete log entries for this event can only be analyzed on the syslog server, as the events on the device are deleted after a re-start.

Example:

2025-06-11T15:21:52.145364+02:00 192.168.1.1 2025-06-11_15: 21:23.92907 <13>Jun 11 15:21:23 **ham-ssv**: INFO sigterm (request to terminate)

2025-06-11T15:21:52.145364+02:00 192.168.1.1 2025-06-11_15: 21:23.92959 <13>Jun 11 15:21:23 **ham-ssv**: INFO terminating

2025-06-11T15:21:52.146846+02:00 192.168.1.1 2025-06-11_15: 21:23.92997 <13>Jun 11 15:21:23 **ham-ssv**: INFO terminated

[...]

1.3.14 Uptime (time stamp)

To check on an external syslog server, for example, whether the transfer of log entries is taking place as desired and whether log entries are being transferred regularly, a log entry with the prefix "uptime-audit" is created approximately every 30 minutes and sent to the syslog server. The log entry shows the current time that has passed since the system start of the mGuard device (uptime).

Log entry	Description
uptime-audit	Automatic time stamp to check the logging function of the device.

Example:

2025-03-22_06:17:45.26984 **uptime-audit**: -------- UPTIME: 1 day, 23:51 --------

2025-03-22_06:46:45.27963 **uptime-audit**: -------- UPTIME: 2 days, 20 min --------

2025-03-23_09:50:45.81252 **uptime-audit**: -------- UPTIME: 3 days, 3:24 --------

1.4 Log prefix (Firewall)

1.4.1 Device and routing Firewall

Packets that are directed to the mGuard device or must pass through the firewall are checked in the following order:

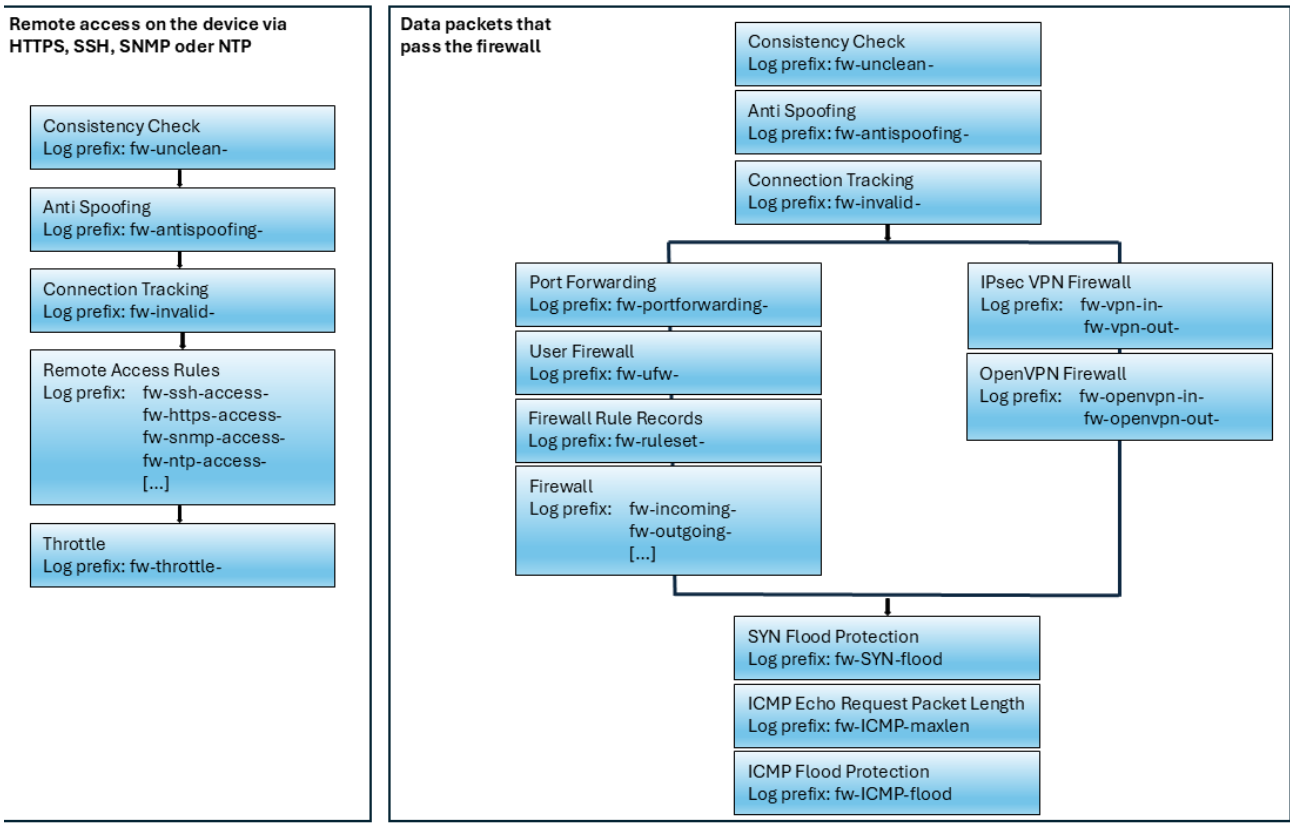

Figure 1-1 Packet inspection of packets that pass through a firewall

Further details on package control are described in the following chapters.

1.4.2 Abbreviations

Table 1-2 Abbreviations used in log entries

Abbreviation	Description
IN (Router mode) PHYSIN (Stealth mode)	Incoming interface eth0: external interface / br0 (Stealth mode) eth1: internal interface / br0 (Stealth mode) tun(x): Interface for each active OpenVPN connection
OUT (Router mode) PHYSOUT (Stealth mode)	Outgoing interface eth0: external interface / br0 (Stealth mode) eth1: internal interface / br0 (Stealth mode) tun(x): Interface for each active OpenVPN connection
MAC	This information is always displayed, regardless of the protocol, if the MAC address of the remote station is known.
act	Action performed for package: DROP, REJECT or ACCEPT
SRC	Source IP address
DST	Destination IP address
LEN	Total length of the IP packet in bytes
TOS	Type of services , Field *Type*
PREC	Type of services , Field *Precedence*
TTL	Remaining lifetime (time to live) in hops
ID	Unique ID of the IP datagram, which is shared by all fragments if they are fragmented.
DF	Flag *"Don't fragment*" is active.
CE	Flag "Reserved fragment"
MF	Flag "More fragments" (reference to further following fragments of the same package)
PROTO	Name or number of the protocol (e.g. ARP or TCP, ICMP)
SPT	Source port (TCP and UDP)
DPT	Destination port (TCP and UDP)
WINDOW	The size of the *TCP Receive Window*. (Only for TCP)
[FLAGS] URG ACK PSH RST SYN FIN CWR ECE	If the TCP protocol is used, the TCP flags (e.g. SYN) are also displayed. URG = Urgent flag ACK = Acknowledgement flag PSH = Push flag RST = Reset flag SYN = SYN flag (wird nur beim Aufbau von TCP-Verbindungen ausgetauscht) FIN = FIN flag (wird nur bei der Trennung von TCP-Verbindungen ausgetauscht) CWR = Peer has reduced "congestion window" (WINDOW) ECE = Peer supports "explicit congestion notification" in the event of overload
SPI	Used SPI (only for ESP protocoll)
URGP	The *Urgent Pointer* enables urgent data transmissions of the "*out of band*" type.
MARK	An internally used marker on the data packet.

Table 1-2 Abbreviations used in log entries

CTMARK	An internally used marker on the connection tracking entry belonging to the data packet.
SEQ	ID of the packet for ICMP Echo and Echo Reply (Ping)
CODE	ICMP code (only ICMP)
TYPE	ICMP type (only ICMP)
ROWID1 / ROWID2	IDs of the associated IPsec connection and the associated IPsec tunnel (if the packet goes into an IPsec tunnel or came out of one).
GATEWAY	Suggested gateway for ICMP "*Redirect*".
MTU	Suggested MTU for ICMP "*Fragmentation Needed*".
REQUEST	Request (ARP only)
REPLY	Response (ARP only)
NAK	*Negative acknowledgement* - The request could not be processed successfully (ARP only).
REPLY_MAC	Resolved MAC address (ARP only)
CODE	Other "*operation code*" for ARP, if it is neither REQUEST, nor REPLY, nor NAK. For example with reverse ARP.

1.4.3 Log-Identifier

Example of a firewall log entry:

2025-03-21_09:02:08.11705 firewall: **fw-incoming-2-3189b8c7-8002-1315-805d-a8741dfd1b11** act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=26695 DF PROTO=TCP SPT=23695 DPT=5201 SEQ=107412944 ACK=0 WINDOW=65535 SYN URGP=0

Each log entry begins with the time stamp and the log identifier.

Time stamp (Example):

2025-03-08_17:25:22.07497

Log Identifier (Example):

The Log Identifier consists of the following elements in the following format:

<Log prefix>-<Rule number>-<Log ID>

Example: fw-incoming-1-3189b8c7-8002-1315-805d-a8741dfd1b11

Log prefix	The log prefix indicates in which area or at which step an action took place during the analysis of the data traffic by the firewall.
Rule number	The rule number indicates which configured firewall rule caused the log entry. <Rule number> = 0 means that the log entry was caused by a standard firewall rule.
Log ID	Each type of configured firewall (e.g. incoming rules, outgoing rules, SSH or HTTPS remote access) has its own unique log ID.

The log identifier can be used in the "Logging>> View logs" menu to find the firewall rule that caused the log entry.

The time zone configured in the "Administration >> System settings >> Time and date" menu only affects the time stamps displayed in the web interface.

If you use remote logging, the time stamp is displayed in UTC format on the remote syslog server. This makes it easier to compare the log entries if you are using a central syslog server to record and analyze the log entries of various devices located in different time zones.

1.4.4 Limitation of access (fw-throttle)

This check is carried out for all packets that are received via the external interface.

Log prefix	Description
fw-throttle	The firewall limits the permitted connections for remote access to the mGuard device. The permitted number varies for different protocols. If the permitted number of connections is exceeded, new connections are rejected and the packets are discarded.

1.4.5 Anti-Spoofing (fw-antispoofing)

This check is carried out for all packets that are received via the external or DMZ interface.

Packets are rejected and dropped if their sender IP address belongs to the network of an interface other than the one on which they were received.

(For example, if packets are received on the external interface whose sender IP is in the internal network).

The log prefix **fw-antispoofing-** is followed by the extensions *ext1* and *dmz* if the packet was received via the WAN or DMZ interface (*ext1, dmz*).

Log prefix	Description
fw-antispoofing	Packets are rejected and dropped if their sender IP address belongs to the network of an interface other than the one on which they were received. (For example, if packets are received on the external interface whose sender IP is in the internal network).

Example:

2025-03-21_10:13:42.19680 firewall: **fw-antispoofing-ext1**-0- act=DROP IN=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=255.255.255.255 LEN=59 TOS=0x00 PREC=0x00 TTL=128 ID=56636 PROTO=UDP SPT=1004 DPT=1003 LEN=39 CTMARK=100000

1.4.6 Consistency check (fw-unclean)

The firewall performs a consistency check if the "Enable TCP/UDP/ICMP consistency checks" option is activated in the "Network security >> Packet filter>> Advanced" menu.

The consistency check is carried out for the IP headers of all IP packets. For the TCP, UDP and ICMP protocols, the headers of the respective protocol are also checked for invalid values (e.g. invalid checksum, ports or TCP flags).

Log prefix	Description
fw-unclean-input	Packet that was sent directly to an interface of the mGuard.
fw-unclean-output	Packet generated by the mGuard. This log prefix should not actually occur, but is included for the sake of completeness.
fw-unclean-forward	Packet that would pass through the firewall (routing).

Example:

2024-03-31_09:01:18.80548 firewall: **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

2025-03-21_08:41:17.97343 firewall: **fw-unclean-forward**-0- act=DROP IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:6a SRC=192.168.1.100 DST=10.1.80.200 LEN=48 TOS=0x00 PREC=0x00 TTL=63 ID=292 PROTO=TCP SPT=40008 DPT=80 SEQ=811466752 ACK=0 WINDOW=512 SYN URGP=0

1.4.7 Connection tracking (fw-invalid)

Connection tracking is carried out for all packets.

fw-invalid occurs when the firewall discards a network packet for which no suitable connection is entered in the *connection tracking* table of the mGuard device. This means that the packet cannot be related to an existing connection.

In addition, the packet does not create a new entry in the *connection tracking* table, as the connection is blocked or dropped by a firewall rule.

If the packet belongs to an existing connection, TCP packets are also checked to see whether the set TCP flags meet expectations and whether the sequence number is within the currently accepted window. If one of these checks fails, the packet is discarded and an entry with the prefix *fw-invalid* is generated.

Log prefix	Description
fw-invalid-input	Packet that was sent directly to an interface of the mGuard device.
fw-invalid-output	Packet generated by the mGuard device. This log prefix should not actually occur, but is included for the sake of completeness.
fw-invalid-forward	Packet that would pass through the firewall.

Example:

2025-03-21_08:04:40.08134 firewall: **fw-invalid-input**-0- act=DROP IN=eth0 MAC=00:0c:be:04:00:58 SRC=10.1.80.123 DST=10.1.80.100 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=54116 DF PROTO=TCP SPT=37645 DPT=5201 SEQ=3746596578 ACK=16777216 WINDOW=0 ACK RST URGP=0

2025-03-21_08:22:49.49289 firewall: **fw-invalid-output**-0- act=DROP OUT=eth0 MAC= SRC=10.1.80.100 DST=10.1.80.200 LEN=104 TOS=0x08 PREC=0x40 TTL=64 ID=54569 DF PROTO=TCP SPT=22 DPT=22841 SEQ=1343772416 ACK=16777216 WINDOW=501 ACK PSH URGP=0 UID=0 GID=0 MARK=800

2025-03-21_08:06:12.08142 firewall: **fw-invalid-forward**-0- act=DROP IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.123 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=466 DF PROTO=TCP SPT=5201 DPT=37645 SEQ=584616543 ACK=16777216 WINDOW=53217 ACK FIN URGP=0

1.4.8 Remote access (fw-ssh-, fw-https-, fw-snmp-, fw-ntp-access)

Log entries with the prefixes **fw-ssh-, fw-https-, fw-snmp-** and **fw-ntp-access** are caused by remote access rules for SSH, HTTPS, SNMP and NTP access from the external network (if "Logging" has been enabled):

- **SSH remote access**: Menu "Administration>> System Settings>> Shell Access"
- **HTTPS remote access**: Menu "Administration>> Web Settings>> Access"
- S**NMP remote access**: Menu "Administration>> SNMP>> Query"
- **NTP remote access**: Menu "Administration>> System Settings>> Time and Date"

Log prefix	Description
fw-ssh-access	A remote access rule (shell access / SSH) applies to an incoming SSH connection that terminates on the device.
fw-https-access	A remote access rule (web access / HTTPS) applies to an incoming HTTPS connection that terminates on the device.
fw-snmp-access	A remote access rule (SNMP access / SNMP) applies to an incoming SNMP connection that terminates on the device.
fw-ntp-access	A remote access rule (NTP access / NTP) applies to an incoming NTP connection that terminates on the device.

Example:

2025-03-13_11:03:03.62955 firewall: **fw-ssh-access**-1-1dd08637-31d0-1f7f-b283-000cbe000d32 act=REJECT IN=eth0 MAC=d4:d8:53:b2:6d:62 SRC=192.168.178.32 DST=192.168.178.128 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=60064 DF PROTO=TCP SPT=55219 DPT=22 SEQ=1601988361 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=100030

2025-03-13_11:04:38.28569 firewall: **fw-https-access**-1-1dd0864d-31d0-1f7f-b283-000cbe000d32 act=ACCEPT IN=eth0 MAC=d4:d8:53:b2:6d:62 SRC=192.168.178.32 DST=192.168.178.128 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=60722 DF PROTO=TCP SPT=65104 DPT=443 SEQ=2949231819 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=100030

2025-03-13_10:57:21.38954 firewall: **fw-ntp-access**-1-1dd08618-31d0-1f7f-b283-000cbe000d32 act=DROP IN=eth0 MAC=00:0c:be:00:10:fc SRC=192.168.178.40 DST=192.168.178.128 LEN=76 TOS=0x18 PREC=0xA0 TTL=64 ID=20909 DF PROTO=UDP SPT=123 DPT=123 LEN=56 CTMARK=100030

1.4.9 Firewall (fw-incoming, fw-outgoing)

Log entries with the prefixes **fw-incoming** and **fw-outgoing** are caused by configured incoming and outgoing firewall rules (if "Logging" has been enabled).

- **Incoming rules: Menu "Network Security>> Packet Filter>> Inbound Rules"**
- **Outgoing rules: Menu "Network Security>> Packet Filter>> Outgoing Rules"**

Log prefix	Description
fw-incoming	An incoming rule applies to a connection that is established from external to internal (WAN --> LAN).
fw-outgoing	An outgoing rule applies to a connection that is established from internal to external (LAN --> WAN).

Example:

2025-03-21_09:01:46.32490 firewall: **fw-incoming**-1-3189b8c7-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=26694 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=390

2025-03-21_09:02:08.11705 firewall: **fw-incoming**-2-3189b8c7-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=26695 DF PROTO=TCP SPT=23695 DPT=5201 SEQ=107412944 ACK=0 WINDOW=65535 SYN URGP=0

2025-03-21_08:59:32.91681 firewall: **fw-outgoing**-1-3189b8c8-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=29288 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=39

2025-03-21_09:00:04.37373 firewall: **fw-outgoing**-2-3189b8c8-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=29291 DF PROTO=TCP SPT=51582 DPT=5201 SEQ=1243586400 ACK=0 WINDOW=65535 SYN URGP=0

1.4.10 DMZ firewall (fw-dmz-incoming, fw-dmz-outgoing)

Log entries with the prefixes **fw-dmz-incoming-lan** and **fw-dmz-outgoing-lan a**s well as **fw-dmzincoming-wan** and **fw-dmz-outgoing-wan** are caused by configured incoming and outgoing DMZ firewall rules (if "Logging" has been enabled)).

– **DMZ rules:** Menu "Network Security >> Packet Filter>> DMZ"

Log prefix	Description
fw-dmz-incoming-wan	A firewall rule applies to a connection (WAN --> DMZ).
fw-dmz-outgoing-wan	A firewall rule applies to a connection (DMZ --> WAN).
fw-dmz-incoming-lan	A firewall rule applies to a connection (LAN --> DMZ).
fw-dmz-outgoing-lan	A firewall rule applies to a connection (DMZ --> LAN).

Example:

2025-03-25_13:24:35.44775 firewall: **fw-dmz-incoming-wan**-1-38db7ed8-85b6-1760-a630-000cbe00105c act=ACCEPT IN=eth0 OUT=dmz0 MAC=d4:d8:53:b2:6d:62 SRC=192.168.100.32 DST=192.168.3.128 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=29021 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=15028

2025-03-25_13:27:08.21530 firewall: **fw-dmz-outgoing-wan**-1-38db7eda-85b6-1760-a630-000cbe00105c act=ACCEPT IN=dmz0 OUT=eth0 MAC=00:0c:be:00:0d:32 SRC=192.168.3.128 DST=192.168.100.1 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=27183 DF PROTO=ICMP TYPE=8 CODE=0 ID=17879 SEQ=4

2025-03-25_13:45:16.95125 firewall: **fw-dmz-outgoing-lan**-1-38db7edb-85b6-1760-a630-000cbe00105c act=ACCEPT IN=eth1 OUT=dmz0 PHYSIN=swp0 MAC=d4:d8:53:b2:6d:62 SRC=192.168.100.32 DST=192.168.3.128 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=30850 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=16278

2025-03-25_13:46:39.31935 firewall: **fw-dmz-outgoing-lan**-1-38db7edb-85b6-1760-a630-000cbe00105c act=ACCEPT IN=eth1 OUT=dmz0 PHYSIN=swp0 MAC=d4:d8:53:b2:6d:62 SRC=192.168.100.32 DST=192.168.3.128 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=30980 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=16366

1.4.11 Firewall rule records (fw-ruleset)

Log entries with the prefixes **fw-ruleset** are caused by configured firewall rules that have been defined in firewall rule records (if logging has been enabled in the corresponding incoming/outgoing firewall rule).

– **Rule records**: Menu "Network Security>> Packet Filter>> Rule Records"

Log prefix	Description
fw-ruleset	A rule that is defined in an active and corresponding firewall rule record applies to a connection.

Example:

2025-03-25_10:50:50.60941 firewall: **fw-ruleset**_MAIv167032083-1-108ee44b-c0c7-19cd-8938-000cbe00105c act=DROP IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=swp0 MAC=d4:d8:53:b2:6d:62 SRC=192.168.1.32 DST=192.168.1.128 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=9188 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=10364 MARK=c

2025-05-09_10:55:53.90349 firewall: **fw-ruleset**_MAIv226940804-1-1c55a7b6-c861-1037-a74f-000cbe00105c act=ACCEPT IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=swp0 MAC=bc:e9:2f:c3:60:06 SRC=192.168.1.37 DST=192.168.1.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=25467 DF PROTO=UDP SPT=138 DPT=138 LEN=221 MARK=10000 CTMARK=100000

1.4.12 User firewall (ufw)

Log entries with the prefix **ufw** are caused by a configured user firewall (if "Logging" has been enabled).

Log prefix	Description
ufw	A user firewall rule applies to a connection.

Example:

2025-03-21_09:41:59.15695 firewall: **fw-ufw_**MAIv390774000-1-3189b901-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=63856 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=398 MARK=10000

2025-03-21_09:42:36.18082 firewall: **fw-ufw_**MAIv390774000-1-3189b901-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=63857 DF PROTO=TCP SPT=24482 DPT=5201 SEQ=1915233667 ACK=0 WINDOW=65535 SYN URGP=0 MARK=10000

1.4.13 IP- and Portforwarding (fw-portforwarding)

Log entries with the prefix **fw-portforwarding** are caused by configured IP and port forwarding rules (menu "Network >> NAT >> IP and Port Forwarding") (if "Logging" has been enabled).

Log prefix	Description
fw-portforwarding	An IP and port forwarding rule applies to a connection.

Example:

2025-03-21_08:00:29.71358 firewall: **fw-portforwarding**-1-3189b80a-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:0c:be:04:00:58 SRC=10.1.80.123 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=126 ID=2146 DF PROTO=TCP SPT=37646 DPT=5201 SEQ=1731043981 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=1010

1.4.14 IPsec VPN firewall (fw-vpn-in, fw-vpn-out)

Log entries with the prefixes **fw-vpn-in** and **fw-vpn-out** are caused by configured incoming and/or outgoing VPN firewall rules (if "Logging" has been enabled).

Log prefix	Description
fw-vpn-in	An incoming rule applies to a connection established by the remote peer through the IPsec VPN tunnel.
fw-vpn-out	An outgoing rule applies to a locally established connection to the remote peer through the IPsec VPN tunnel.

Example:

2025-03-21_07:21:31.98537 firewall: **fw-vpn-in**_MAIv711498711-1-3189b7d8-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:0c:be:04:00:58 SRC=192.168.27.100 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=126 ID=239 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=376 CTMARK=800 ROWID1=MAIv711498711 ROWID2=MAIv144871511

2025-03-21_07:24:22.48150 firewall: **fw-vpn-in**_MAIv711498711-1-3189b7d8-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:0c:be:04:00:58 SRC=192.168.27.100 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=126 ID=248 DF PROTO=TCP SPT=20703 DPT=5201 SEQ=1396473492 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=800 ROWID1=MAIv711498711 ROWID2=MAIv144871511

2025-03-21_07:15:10.03337 firewall: **fw-vpn-out**_MAIv711498711-1-3189b7d9-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=6650 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=12 ROWID1=MAIv711498711 ROWID2=MAIv144871511

2025-03-21_07:15:49.55344 firewall: **fw-vpn-out**_MAIv711498711-1-3189b7d9-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=6654 DF PROTO=TCP SPT=51029 DPT=5201 SEQ=1008731145 ACK=0 WINDOW=65535 SYN URGP=0 ROWID1=MAIv711498711 ROWID2=MAIv144871511

1.4.15 OpenVPN firewall, -forwarding (fw-openvpn-in, -out, -openvpn-portfw)

Log entries with the prefixes **fw-openvpn-in** and **fw-openvpn-out** are caused by configured incoming and/or outgoing OpenVPN firewall rules (menu "OpenVPN Client >> Connections ((EDIT)) >> Firewall) (if "Logging" has been enabled).

Log entries with the prefixes **fw-openvpn-portfw** are caused by configured OpenVPN NAT rules (menu "IPsec VPN >> Connections ((EDIT)) >> NAT) (if "Logging" has been enabled).

Log prefix	Description
fw-openvpn-in	An incoming rule for the OpenVPN connection applies to an inbound connection.
fw-openvpn-out	An outgoing rule for the OpenVPN connection applies to an outgoing connection.
fw-openvpn-portfw	A port forwarding rule applies to a connection through the OpenVPN tunnel.

Example:

2025-03-21_07:02:39.24936 firewall: **fw-openvpn-in**_MAIv231480925-1-3189b7a5-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=tun0 OUT=eth1 MAC= SRC=11.8.0.1 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=6909 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=361

2025-03-21_07:03:23.40939 firewall: **fw-openvpn-in**_MAIv231480925-1-3189b7a5-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=tun0 OUT=eth1 MAC= SRC=11.8.0.1 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=6913 DF PROTO=TCP SPT=20025 DPT=5201 SEQ=910850867 ACK=0 WINDOW=65535 SYN URGP=0

2025-03-21_06:22:47.05735 firewall: **fw-openvpn-out**_MAIv231480925-1-3189b7a6-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=tun0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=21771 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=4

2025-03-21_06:23:06.76962 firewall: **fw-openvpn-out**_MAIv231480925-1-3189b7a6-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=tun0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=21775 DF PROTO=TCP SPT=50086 DPT=5201 SEQ=3770954720 ACK=0 WINDOW=65535 SYN URGP=0

2025-03-21_07:09:44.46552 firewall: **fw-openvpn-portfw**_MAIv231480925-1-3189b7b9-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=tun0 OUT=eth1 MAC= SRC=11.8.0.1 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=33661 DF PROTO=TCP SPT=20179 DPT=5201 SEQ=1909642899 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=1010

1.4.16 DoS protection: SYN flood protection (fw-SYN-flood)

The limit/threshold for new incoming and outgoing TCP connections (SYN flood protection) per second can be configured via the "Network Security >> DoS Protection" menu. If one limit is reached, a log entry with the log prefix **fw-SYN-flood** is recorded. These events are logged once per second.

Log prefix	Description
fw-SYN-flood	A limit for an incoming or outgoing TCP connection per second has been reached.

Example:

```
2025-03-21_08:56:51.06084 firewall: fw-SYN-flood act=DROP IN=eth1 OUT=eth0
MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200 LEN=52 TOS=0x00
PREC=0x00 TTL=127 ID=29158 DF PROTO=TCP SPT=51564 DPT=8080
SEQ=408716129 ACK=0 WINDOW=64240 SYN URGP=0
```

1.4.17 DoS protection: ICMP flood protection (fw-ICMP-flood)

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

Log prefix	Description
fw-ICMP-flood	A limit for incoming or outgoing ICMP echo requests per second has been reached.

Example:

```
2025-03-21_08:51:10.64480 firewall: fw-ICMP-flood act=DROP IN=eth1 OUT=eth0
MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200 LEN=60 TOS=0x00
PREC=0x00 TTL=254 ID=28715 PROTO=ICMP TYPE=8 CODE=0 ID=47114 SEQ=4
```

1.4.18 Max. size „ICMP Echo Request packets“ (fw-ICMP-maxlen)

The maximum size of the permitted ICMP echo request packets can be set via the "Network Security >> Packet Filter >> Advanced" menu. If an ICMP echo request packet exceeds this limit, a log entry with the log prefix **fw-ICMP-maxlen** is recorded.

Log prefix	Description
fw-ICMP-maxlen	The limit for the maximum size of an ICMP echo request has been reached.

Example:

```
2025-03-21_09:05:28.59680 firewall: fw-ICMP-maxlen act=DROP IN=eth1
OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200
LEN=2028 TOS=0x00 PREC=0x00 TTL=127 ID=49800 PROTO=ICMP TYPE=8 CODE=0
ID=1 SEQ=43
```

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
Email: info@phoenixcontact.com
phoenixcontact.com

© Phoenix Contact 2025-06-17

112008_en_00
Item No. –00