Document Title	Requirements on Firewall
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	1062

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R23-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2023-11-23	R23-11	AUTOSAR Release Management	• Added requirement for support for hardware-accelerated filtering
2022-11-24	R22-11	AUTOSAR Release Management	• Initial release

Disclaimer

Contents

1 Scope of Document

This document specifies requirements on Automotive Ethernet **Firewall** that can integrated in Adaptive Autosar and Classic Autosar. The following chapter gives a basic overview of **Firewall**.

1.1 Overview of Automotive Ethernet Firewall

An automotive Ethernet firewall is a network security device that monitors incoming and outgoing network traffic and grants or rejects network access between two or more Electronic Control Units (ECU) or between network zones (e.g. vehicle domain (ADAS, infotainment, diagnostics etc), trusted/non-trusted zones). All the network traffic between two network zones can only flow through a firewall. A control model is used to define the access control mechanism which states that only the traffic defined in the security policy of the firewall is allowed onto the network and all other traffic must be silently dropped. These security policies or firewall rules are called Access Control List (ACL). These ACLs define essential rules that determine whether network access should be granted or rejected for network traffic.

The automotive network firewalls are categorized into three major types:

1.1.1 Stateless packet inspection firewall

This type of network firewall is called a packet filter. It acts by inspecting packets transferred between two network zones. When a packet does not match a set of filtering rules in the packet filters, the packet filter either drops (silently discards) the packet, or rejects the packet (discards it and generates a notification for the sender) else it is allowed to pass. Packets may be filtered based on Ethernet header, IPv4/v6 header, TCP/UDP source/destination ports, and ICMP v4/v6 Type/Code, etc.

1.1.2 Stateful packet inspection firewall

A stateful firewall can grant or reject access to packets not only based on port and protocol, but also based on multiple packet attributes (also known as the state of connection) which are stored in memory as a state table. These state tables may include details like IP addresses, protocol ports, sequence numbers of the packets traversing the connection, and TCP Flags like SYN, ACK and FIN, etc. This cumulative data is evaluated so that filtering decisions would not only be based on access control list rules but also on context that has been built by previous connections as well as previous packets belonging to the same connection.

1.1.3 Deep Packet Inspection firewall

This kind of firewall evolves beyond simple stateless packet filtering and stateful inspection. It involves deep inspection of packets at the very application layer and is specifically designed for different protocols like Diagnostic Over IP (DoIP), Data Distribution Service (DDS) and Scalable Service-Oriented MiddlewarE over IP (SOME/IP) etc. to prevent advanced attacks.

1.2 Deployment of Firewall

Cross-domain centralized E/E architectures, unlike domain-specific E/E architectures, use only a few very powerful vehicle computers instead of many individual control units. The reduced number of control units leads to reduction in cost and system complexity. It also means that an ECU could participate in more than one domain or cater to more than one functionality. These vehicle computers will be connected to the remaining embedded control units as well as the sensors and actuators via zone ECUs. The zone ECUs send the data via high-speed Ethernet to the connected vehicle computers.

From a network security perspective, having a firewall centrally in a central gateway is not enough and more instances of firewall would be required that are distributed around small ECUs, vehicle computers and Ethernet switches to strengthen the security of the EE-architecture. Depending on the use-case and EE-architecture, few or all of the below mentioned deployment scenarios can be utilized to fulfill firewall requirements.

Figure 1.1 shows an example of a zonal architecture including firewall deployment scenarios.

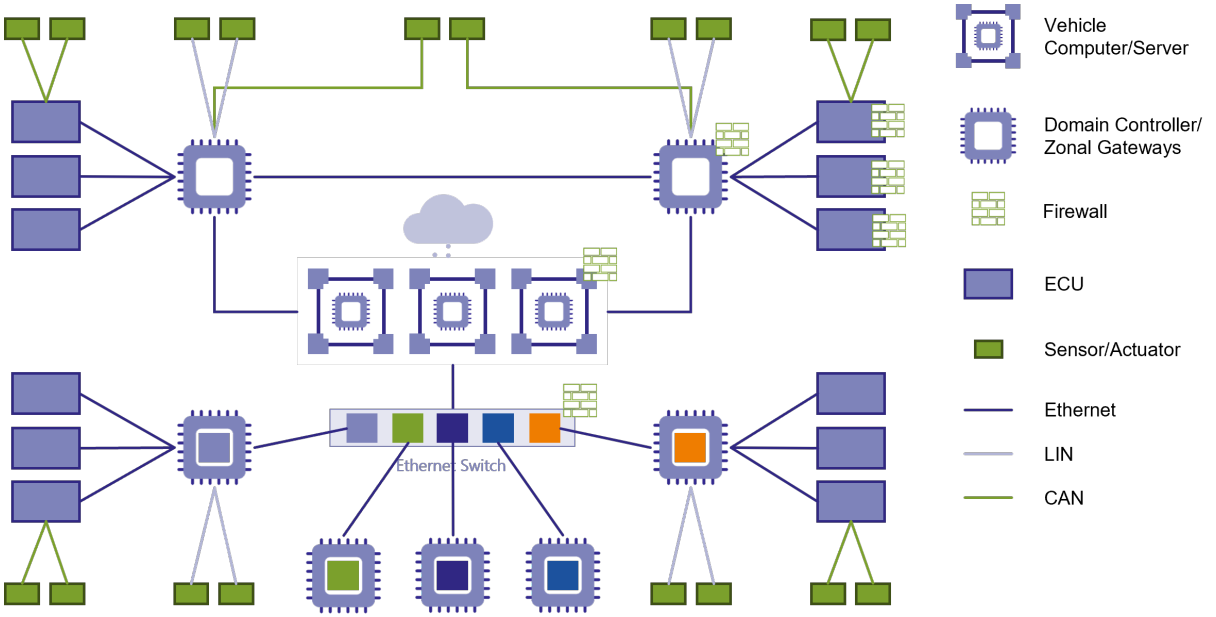

Figure 1.1: Example zonal E/E architecture including firewall

1.2.1 Host-Based Firewall in Classic AUTOSAR ECUs

A firewall on small end ECU would typically cater to very specific use-case like providing access control for selective network traffic e.g. Electric Vehicle Charging ECU.

1.2.2 Host-Based and network Firewall in Adaptive AUTOSAR based Vehicle Computer and Domain Controller ECUs

A firewall here has a multitude of complexity and functions to cater to, like providing network separation, access control, firewalling cross-domain traffic, filtering end-to-end encrypted communication and many others. A high performance ECU can be utilized for multiple applications and can have one or multiple Ethernet ports. If it has just one Ethernet port then the requirements of an end-point firewall would be applicable, but if more than one port is available then the requirements of an end-point firewall as well as a gateway (inter-zone, inter-port communication) can be applicable. Also based on the security threats, a combination of stateless firewall, stateful firewall and deep packet inspection could be applied.

1.2.3 Network-Based Firewall on Ethernet Switches

For smart Ethernet switches, the firewall requirements are complex as well as performance intensive due to the amount of network traffic a switch caters to. Typically, the firewall is paired together with a router in switches and performs network separation, access control for other ECUs and firewalls cross-domain traffic. Also based on security threats, a combination of stateless firewall, stateful firewall and deep packet inspection could be applied.

1.3 Scope of Firewall Requirement Specification

The main focus of this RS document is to describe the requirements for the functionality of a firewall that can be realized within Adaptive and Classic AUTOSAR and the focus is mainly on host-based firewalls.

Firewall functionality can be implemented on Host ECUs and on switches (as network firewalls). Both variants are valid and used in vehicles, and both can be combined to secure the in-vehicle network. Although it is generally possible to run a stripped-down instance of Classic AUTOSAR on a switch, the main purpose of AUTOSAR is to run on ECUs. Hence, this document focuses on host firewall functionality and leaves the network firewall functionality out of scope.

It is however possible to use the AUTOSAR methodology to model a switch in terms of an ECU and configure the firewall on the switch using the filter rules defined within this concept. More details can be found in the respective metamodel specifications.

2 Conventions to be used

2.1 Document Conventions

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template, chapter Support for Traceability ([1]).

The verbal forms for the expression of obligation specified in [TPS_STDT_00053] shall be used to indicate requirements, see Standardization Template, chapter Support for Traceability ([1]).

3 Acronyms and abbreviations

The glossary below includes acronyms and abbreviations relevant to Autosar RS Firewall that are not included in the AUTOSAR Glossary [2].

Abbreviation / Acronym:	Description:
Firewall	An automotive Ethernet firewall is a network security device that monitors incoming and outgoing network traffic and grants or rejects network access between two or more Electronic Control Units (ECU) or between network zones (e.g. vehicle domain (ADAS, infotainment, diagnostics etc), trusted/non-trusted zones).
SPI	Stateful Packet Inspection
DPI	Deep Packet Inspection
SOC	Security Operations Center or Vehicle Security Operations Center
IDS	Intrusion Detection System. An Intrusion Detection System is a security sensor which detects and generates security events.
IdsM	Intrusion Detection System - Manager. The Intrusion Detection System Manager handles security events generated by security sensors.
IDPS	Intrusion Detection and Prevention System. An Intrusion Detection and Prevention System is a security control which takes predefined preventive measures for the qualified security events detected and reported by IDS sensor.
SEv	Security Events. Security Events & Onboard Security Events are instances of security event types which are reported by BSW or SWC to the AUTOSAR IdsM
QSEv	Qualified Security Events. Security events which pass their filter chain are regarded as Qualified Security Events.

Table 3.1: Acronyms and abbreviations used in the scope of this Document

4 Requirements specification

A firewall operates by inspecting incoming network packets (both ingress and egress traffic) and checking if it matches predefined patterns and then take an action based on the configuration:

- Allow list: Allow only specified communication
- Block list: Block only specified communication

A firewall establishes and preserves communication in all layers of the ISO OSI model. This is achieved via

- Stateless packet filter - layer specific and static:

  A simple stateless packet filter just analyzes the header fields of the protocols on layer 2-4, such as MAC addresses, IP addresses and port numbers. This type of firewall is able to block unauthorized traffic and possible malicious data from reaching its destination. It can also detect attacks obtaining network control (by installing or corrupting a device on the network to control the operation of other devices), denial of service (DoS) attacks against the network and snooping or information theft.

- Stateful packet Inspection (SPI) - multilayer and dynamic:

  A stateless packet filter can only perform network access control based on headers whereas stateful packet filters have the additional capability of tracking a connection state by working with a state table. In the case of TCP, incoming packets would be analyzed for their flags in the TCP header and this information would be used to identify that packet as part of an existing or the beginning of a new connection. This firewall can detect some DoS attacks such as SYN/ACK flooding or ACK storm.

- Deep packet inspection (DPI) - application specific and possibly stateful:

  Deep packet inspection is a stateful application layer firewall and additionally analyzes layers 5-7 in the OSI model whereas the rest just supports up to layer 4. DPI is very effective as not only the packet headers, but the payload is analyzed as well. The more sophisticated a firewall gets, it comes at the expense of performance, leading to the problem of finding a sufficient trade-off between functionality and performance.

In addition to this, the firewall can generate security attack alerts called security events (**SEvs**) and raise them to the **IdsM** module which can forward them for further analysis to the **SOC**. The **SOC** can then adapt the firewall rules based on the (**SEvs**) by deploying a configuration update via a FOTA update of the firewall module and/or even take preventive actions against intruders.

The following use cases drive the requirements for the firewall.

- UC 1: Stateless filtering

- UC 2: Stateful filtering
- UC 3: Deep packet inspection
- UC 4: Standardization of filter rules
- UC 5: Updatable configuration
- UC 6: Reporting of Security Events

4.1 Functional overview

The functional elements of a firewall are described in this chapter in detail.

- Network packet inspection
- Firewall rule enforcement
- Firewall configuration update
- Firewall as sensor for the **IdsM**

4.1.1 Network packet inspection

The design of filter rules is very critical as this is the only input for a firewall to perform network packet inspection. Filters specify the patterns to look for in the network traffic. Firewall filters are protocol specific, and Figure 4.1 represents the different Ethernet relevant protocols in the ISO OSI layers that are existing in the automotive domain.

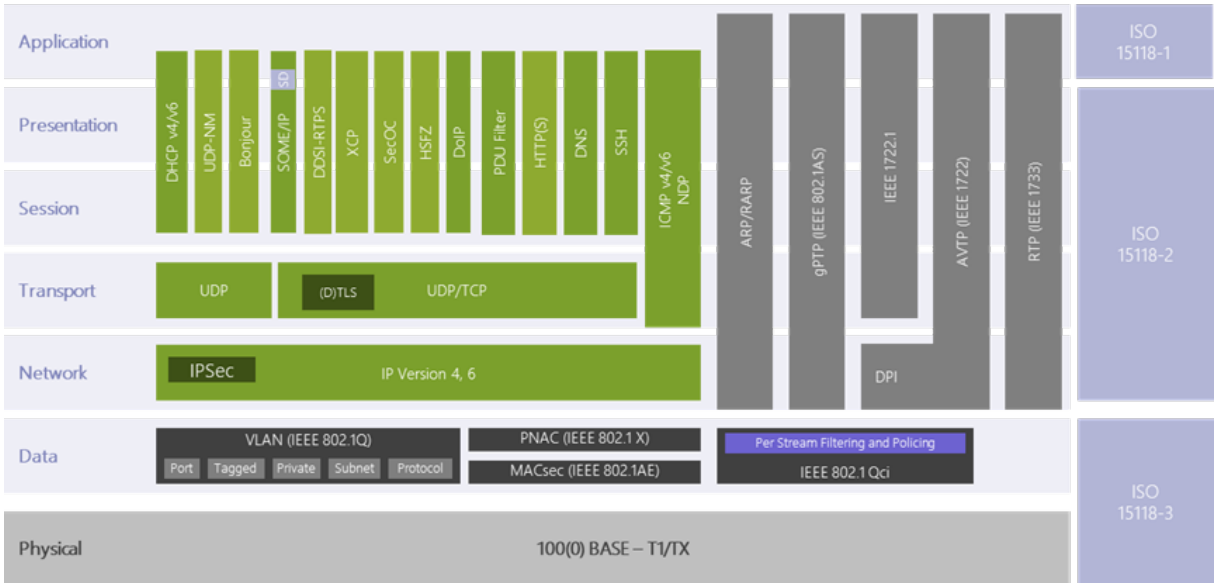

Figure 4.1: Protocols related to Ethernet in ISO/OSI layers

The firewall does not filter on the protocol itself, but on specific information that is defined within the protocol. In most cases, this information can be found in protocol headers, where specific fields are defined that the firewall can use to compare the actual values against expected ones. See Figure 4.2 for examples of filtered fields.

4.1.2 Firewall rule enforcement

For every network packet that passes the communication stack, the firewall performs pattern matching based on the expected values for fields in each filter rule. The firewall checks the ordered list of firewall rules sequentially and the first matching rule is enforced.

A firewall rule can be individually configured with an action to allow or block the network packets. A default action shall be configured for all the remaining network packets that are not part of any of the configured filter rules. In addition to the generic configuration option allow/block, the following options can be configured per rule:

- Security alert: If enabled, the firewall raises an SEv to the IdsM in case of a firewall match. Additionally, the firewall raises an SEv in the case of a no-match
- Reference to vehicle states: The network traffic is depending on the vehicle state and is usually different when the car is in diagnostic mode compared to when it is driving, for instance. Hence, each firewall filter rule can be bound to project-specific vehicle states and is only active when the vehicle is in one of these specific states.
- Rate limiting: The firewall can limit the rate of messages to protect against DoS attacks. To this end, each firewall filter rule can be configured with a rate limit, i.e., after a configured number of matches in a given time interval, matching network packets are dropped.

See Figure 4.2 for firewall filter rule with configuration options included.

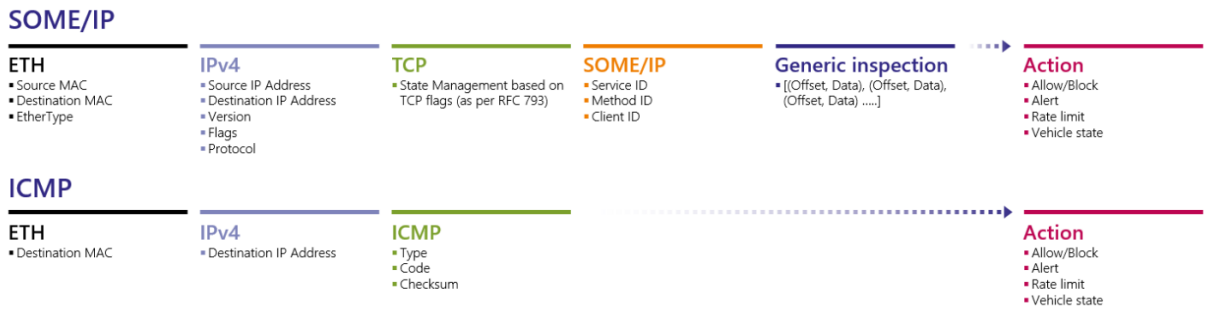

Figure 4.2: Firewall Filter Rules including configuration options

4.1.3 Firewall configuration update

Cyber security attacks are getting stronger day by day. Since a firewall is a rule-based security system, a means to update the configuration needs to be established in order to stay secured during the entire lifetime of the ECU/vehicle. The firewall supports two mechanisms of updating the firewall filter rules by means of

- Manifest deployment
- Runtime control by a dedicated API

4.1.3.1 Manifest deployment

The firewall filter rules will be modeled in the AUTOSAR meta-model, which means that the firewall filter configuration can be included in the respective manifests and ARXMLs. This also means, that the firewall configuration can also be updated by updating the respective manifests, for instance by an OTA update.

4.1.3.2 Runtime control by a dedicated API

The firewall also provides an interface to update firewall rules during runtime. The interface offers only the functionality to activate/deactivate pre-defined firewall filter rules during runtime. Generation of completely new firewall filter rules is not possible via this interface. Completely new rules can only be added using manifest deployment.

This interface can be used by an Intrusion Prevention System, for instance to deactivate filter rules in an allow-list firewall to block malicious traffic or to switch to a more restrictive set of filter rules. Furthermore, this interface can also be used to allow service-communication only after successful service discovery.

4.1.4 Firewall as sensor for IDS

The firewall can act as an IDS sensor to generate Security Events (**SEv**) using the interfaces provided by IdsM. The IdsM module receives these SEvs and further processes them to generate Qualified Security Events (**QSEv**), if the SEv meets the configured criteria. The firewall can raise SEvs when

- The firewall identifies a match for a firewall filter rule and security alert is configured for this rule
- The firewall identifies a no-match and the network packet is dropped due to the default action.

Figure 4.3 shows a sample implementation of firewall as an IDS Sensor.

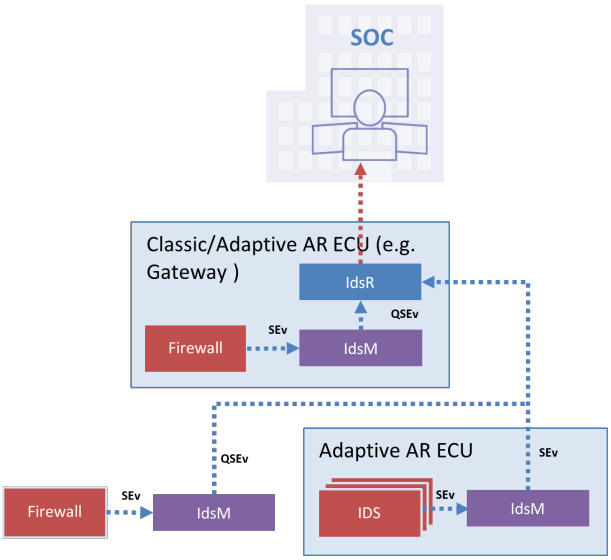

Figure 4.3: Sample Implementation of Firewall as IDS Sensor

It can be deployed in both Adaptive and Classic AUTOSAR by using the interfaces provided by IdsM module. Depending on the security model requirements, it can be decided whether the generated QSEv shall be

- sent to the backend Security Operation Centre SOC via an IDS Reporter (IdsR) for further processing (e.g. performing an application update or deploy preventive actions

and/or

- stored in the memory for later use such as providing raw data for analysis on request (e.g. for forensic analysis).

4.2 Functional Requirements

4.2.1 Initialization of the Firewall

[FO_RS_Fw_00010] Initialization of the Firewall ⌈

Description:	The firewall shall be initialized at start-up
Rationale:	Network packet filtering has to be directly active after start-up to ensure a secure system at all times.
Dependencies:	–
Use Case:	UC1, UC2, UC3
AppliesTo:	CP, AP
Supporting Material:	–

⌋*(RS_Main_00131)*

4.2.2 Stateless filtering of network traffic

[FO_RS_Fw_00001] Stateless filtering of network traffic ⌈

Description:	The firewall shall filter ingress/egress network traffic, based on stateless inspection of network protocol header fields
Rationale:	Network access control
Dependencies:	–
Use Case:	UC1
AppliesTo:	CP, AP
Supporting Material:	–

⌋*(RS_Main_00131)*

4.2.3 Stateful filtering of network traffic

[FO_RS_Fw_00002] Stateful filtering of network traffic ⌈

Description:	The firewall shall filter ingress/egress network traffic, based on the state of the connection.
Rationale:	Protection against attacks targeting stateful protocols (e.g. SYN flood, SYN-ACK flood, Reset attack, ACK storm)
Dependencies:	–
Use Case:	UC2
AppliesTo:	CP, AP
Supporting Material:	

⌋*(RS_Main_00131)*

4.2.4 Deep Packet Inspection of network traffic

[FO_RS_Fw_00003] Deep Packet Inspection of network traffic ⌈

Description:	The firewall shall filter ingress/egress network traffic by inspecting headers and payload of application layer protocols.
Rationale:	Deep packet inspection is specifically designed for different protocols like Diagnostic Over IP (DoIP), Data Distribution Service (DDS) and Scalable Service-Oriented MiddlewarE over IP (SOME/IP) etc. to prevent advanced attacks
Dependencies:	–
Use Case:	UC3
AppliesTo:	CP, AP

▽

△

Supporting Material:	

⌋(*RS_Main_00131*)

4.2.5 Rule-Based filtering of network traffic

[FO_RS_Fw_00005] Rule-Based filtering of network traffic ⌈

Description:	The firewall shall standardize a format for firewall filter rules, which can be used to perform pattern matching of network packets to implement access control
Rationale:	As more OEMs include Firewalls in their EE architecture, there are many customized developments based on the complexity and diversity of ethernet protocols with different firewall rules, configuration, and integration options. There arises the necessity for standardization of format of filter rules.
Dependencies:	–
Use Case:	UC4
AppliesTo:	CP, AP
Supporting Material:	

⌋(*RS_Main_00131*)

4.2.6 Allow list and block list configuration

[FO_RS_Fw_00004] Allow list and block list configuration ⌈

Description:	The firewall shall support the configuration of two filter behaviors: • Allow list: Filter rules that define which network packets are allowed • Block list: Filter rules that define which network packets to block The firewall shall also support a default behavior for messages that are not matching a filter rule (allow/block).
Rationale:	A standard filter generally can allow or block network packets based on predefined configuration.
Dependencies:	–
Use Case:	UC1, UC2, UC3
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_Main_00131*)

4.2.7 Rate Limiting

[FO_RS_Fw_00006] Rate Limiting ⌈

Description:	The firewall shall limit the rate of messages to protect against DoS attacks
Rationale:	The firewall can limit the rate of messages to protect against DoS attacks. To this end, each firewall filter rule can be configured with a rate limit, i.e., after a configured number of matches in a given time interval, matching network packets (in an allow list firewall) are dropped
Dependencies:	–
Use Case:	UC4
AppliesTo:	CP, AP
Supporting Material:	–

⌋*(RS_Main_00131)*

4.2.8 State-dependent Filtering

[FO_RS_Fw_00007] State-dependent Filtering ⌈

Description:	The firewall shall include state-dependent activation or deactivation of filter rules
Rationale:	The network traffic is depending on the vehicle state and is usually different when the car is in diagnostic mode compared to when it is driving, for instance. Hence, each firewall filter rule can be bound to project-specific vehicle states and is only active when the vehicle is in one of these specific states
Dependencies:	–
Use Case:	UC4
AppliesTo:	CP, AP
Supporting Material:	–

⌋*(RS_Main_00131)*

4.2.9 Raising of security Alerts

[FO_RS_Fw_00008] Raising of security Alerts ⌈

Description:	The Firewall shall support the overall IDPS strategy by raising SEVs to the IdsM in the case of observed security incidents. It shall be configurable, in which cases a SEv is raised.
Rationale:	It shall be configurable, in which cases a SEv is raised to facilitate the standardization of IDS Security Events that can be raised by a firewall.

▽

△

Dependencies:	Generation of security events for IDS
Use Case:	UC6
AppliesTo:	CP, AP
Supporting Material:	IDSM Concept.

⌋(*RS_Main_00131*)

4.2.10 Firewall filter rule (de-)activation during runtime

[FO_RS_Fw_00009] Firewall filter rule (de-)activation during runtime ⌈

Description:	It shall be possible to activate/deactivate individual firewall filter rules during runtime
Rationale:	Dynamic firewall filter rule (de-)activation is needed by use-cases like intrusion prevention and service communication after service discovery. Adding/Changing/Deleting firewall filter rules can be performed by a software update, i.e. no explicit firewall functionality is required.
Dependencies:	–
Use Case:	UC5
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_Main_00131*)

4.2.11 Support for hardware-accelerated filtering

[FO_RS_Fw_00011] Hardware-Accelerated Filtering Support ⌈

Description:	If hardware accelerated filtering mechanisms are available then the Firewall shall support to use them. Additional Information: e.g. based on (T)CAM rules.
Rationale:	–
Dependencies:	–
Use Case:	–
AppliesTo:	CP, AP
Supporting Material:	–

⌋(*RS_Main_00131*)

5 Requirements Tracing

The following table references the features specified in [3] and links to the fulfillments of these.

Requirement	Description	Satisfied by
[RS_Main_00131]	Communication filtering mechanisms	[FO_RS_Fw_00001] [FO_RS_Fw_00002] [FO_RS_Fw_00003] [FO_RS_Fw_00004] [FO_RS_Fw_00005] [FO_RS_Fw_00006] [FO_RS_Fw_00007] [FO_RS_Fw_00008] [FO_RS_Fw_00009] [FO_RS_Fw_00010] [FO_RS_Fw_00011]

Table 5.1: RequirementsTracing

6 References

[1] Standardization Template
AUTOSAR_FO_TPS_StandardizationTemplate

[2] Glossary
AUTOSAR_FO_TR_Glossary

[3] Requirements on AUTOSAR Features
AUTOSAR_CP_RS_Features

A Change history of AUTOSAR traceable items

Please note that the lists in this chapter also include traceable items that have been removed from the specification in a later version. These items do not appear as hyperlinks in the document.

A.1 Traceable item history of this document according to AUTOSAR Release R23-11

A.1.1 Added Requirements in R23-11

Number	Heading
[FO_RS_Fw_00011]	Hardware-Accelerated Filtering Support

Table A.1: Added Requirements in R23-11

A.1.2 Changed Requirements in R23-11

Number	Heading
[FO_RS_Fw_00001]	Stateless filtering of network traffic
[FO_RS_Fw_00002]	Stateful filtering of network traffic
[FO_RS_Fw_00003]	Deep Packet Inspection of network traffic
[FO_RS_Fw_00004]	Allow list and block list configuration
[FO_RS_Fw_00005]	Rule-Based filtering of network traffic
[FO_RS_Fw_00006]	Rate Limiting
[FO_RS_Fw_00007]	State-dependent Filtering
[FO_RS_Fw_00008]	Raising of security Alerts
[FO_RS_Fw_00009]	Firewall filter rule (de-)activation during runtime
[FO_RS_Fw_00010]	Initialization of the Firewall

Table A.2: Changed Requirements in R23-11

A.1.3 Deleted Requirements in R23-11

none