SPARTA

D5.4 Appendix G

Impact Analysis - Vertical 1 - Scenario 2

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D5.4 / V1.0 / Appendix G
Work package contributing to the deliverable	WP5
Due date	Jan 2022 – M36
Actual submission date	2nd February, 2022

Responsible organisation	CETIC
Editor	Sébastien Dupont
Dissemination level	PU
Revision	V1.0

Abstract	Proposal of impact analysis for incremental certification in the automotive firewall update scenario
Keywords	Impact Analysis report, Firewall, Automotive, Certification

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Sébastien Dupont (CETIC)

Contributors (ordered according to beneficiary numbers)

Guillaume Ginis, Philippe Massonet (CETIC)

Mirko Malacario, Claudio Porretti (LEO)

Reviewers (ordered according to beneficiary numbers)

Maximilian Tschirschnitz (TUM)

Rimantas Zylius (L3CE)

Disclaimer

Executive Summary

This document provides a sample impact analysis report for CAPE connected cars “Firewall update” demonstration scenario (Vertical 1 - Scenario 2). In this scenario, a new version of the firewall is available and needs to be deployed on platoon vehicles. From the certification point of view, if some certified requirements are impacted then the new firewall version must be re-certified on vehicles.

The document describes the change (firewall update), and the modifications to the affected developer evidences.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

In the SPARTA CAPE Vehicle to Infrastructure (V2I) firewall update scenario, a new version of the firewall is available and needs to be deployed on platoon vehicles. The update is performed when vehicles are not being driven. From the certification point of view, if some certified requirements are impacted then the new firewall version must be re-certified on vehicles. This requires following the certification process for the impacted parts.

For the purpose of this demonstration, the assumption is that we base this impact analysis on preexisting accepted impact analysis reports and associated certification.

The TOE is composed of the platooning software (SafSecPMM) and the firewall that are installed in platoon members as described in Figure 1 below.

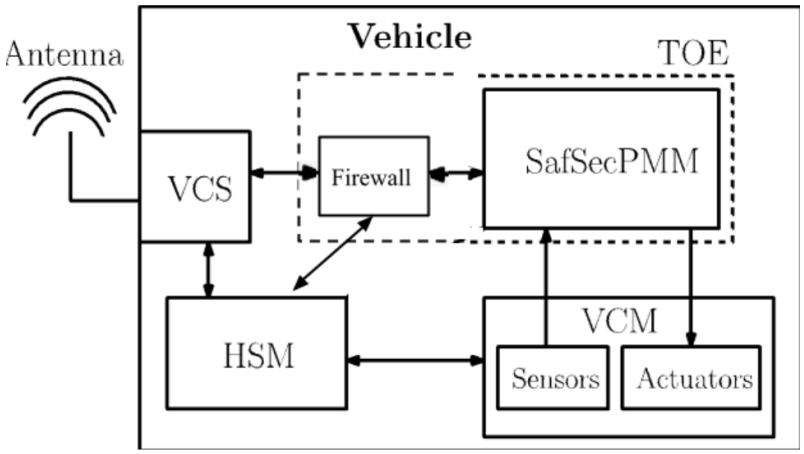

Figure 1: Target of evaluation

The firewall TSF (TOE Security Function) is composed of the green modules in Figure 2.

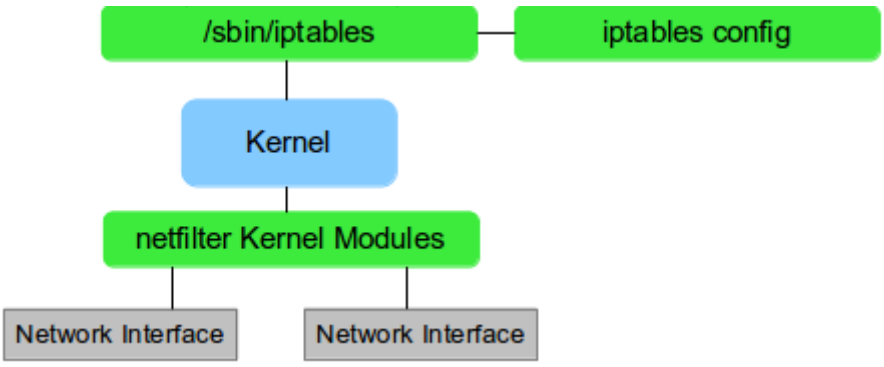

Figure 2: details of the firewall component of the TOE[1]

[1] reference image: https://xerocrypt.wordpress.com/2013/08/26/what-exactly-are-netfilter-and-iptables/

The configuration controls identifiers of the TOE are shown in the following Table 1.

Evaluated Configuration (current)	Updated TOE Version (changes)
iptables - version 1.8.6 - 2020-10-31	iptables - version 1.8.7 - 2021-01-15
SafSecPMM - version x.y.z	SafSecPMM - version x.y.z (no changes)

Table 1: Main TOE Changes

Chapter 2 Description of the change(s)

The following changes to the certified product are identified: the version of the Firewall component has been updated[2]. The release notes below describe the changes for the new version of the firewall, with the associated author:

Florian Westphal (4):

xtables-monitor: fix rule printing

xtables-monitor: fix packet family protocol

xtables-monitor: print packet first

xtables-monitor:

Pablo Neira Ayuso (2):

tests: shell: update format of registers in bitwise payloads.

configure: bump version for 1.8.7 release

Phil Sutter (21):

nft: Optimize class-based IP prefix matches

ebtables: Optimize masked MAC address matches

tests/shell: Add test for bitwise avoidance fixes

ebtables: Fix for broken chain renaming

iptables-test.py: Accept multiple test files on commandline

iptables-test.py: Try to unshare netns by default

libxtables: Extend MAC address printing/parsing support

xtables-arp: Don't use ARPT_INV_*

xshared: Merge some command option-related code

tests/shell: Test for fixed extension registration

extensions: dccp: Fix for DCCP type 'INVALID'

nft: Fix selective chain compatibility checks

nft: cache: Introduce nft_cache_add_chain()

nft: Implement nft_chain_foreach()

nft: cache: Move nft_chain_find() over

nft: Introduce struct nft_chain

nft: Introduce a dedicated base chain array

nft: cache: Sort custom chains by name

tests: shell: Drop any dump sorting in place

nft: Avoid pointless table/chain creation

tests/shell: Fix nft-only/0009-needless-bitwise_0

source: IPTables 1.8.7 changelog[3]

[2] Firewall rules are not updated

[3] https://www.netfilter.org/projects/iptables/files/changes-iptables-1.8.7.txt

Four changes in particular will be studied in this Impact Analysis Report (IAR) but the same process should be followed for all the changes.

Here is the description of these changes :

1. xtables-monitor: fix rule printing: trace_print_rule does a rule dump. This prints unrelated rules in the same chain. Instead the function should only request the specific handle. Furthermore, flush output buffer afterwards so this plays nice when output isn't a terminal.
2. xtables-monitor: fix packet family protocol: This prints the family passed on the command line (which might be 0). Print the table family instead.
3. nft: Optimize class-based IP prefix matches: Payload expression works on byte-boundaries, leverage this with suitable prefix lengths. (discussion)
4. nft: Fix selective chain compatibility checks: Since commit 80251bc2a56ed ("nft: remove cache build calls"), 'chain' parameter passed to nft_chain_list_get() is no longer effective. Before, it was used to fetch only that single chain from kernel when populating the cache. So the returned list of chains for which compatibility checks are done would contain only that single chain. Re-establish the single chain compat checking by introducing a dedicated code path to nft_is_chain_compatible() doing so.

No changes to the development environment of the certified ToE have been identified.

Chapter 3 Affected developer evidence

Regarding the changes to the product, and according to the Common Criteria Assurance Continuity (see [8]), it is necessary to answer the following question to evaluate the affected developer evidence.

- Has it affected the Security Target?

  This part is described in the chapter 3.1.

- Has it affected the reference for the TOE?

  In the Database described below, the components are identified as part of the TOE or not and the issues are associated with the components.

Issues	Impact on TOE
xtables-monitor: fix rule printing	True
xtables-monitor: fix packet family protocol	True
nft: Optimize class-based IP prefix matches	True
nft: Fix selective chain compatibility checks	True

Table 2: Issues impacting the TOE

- Has it affected the list of configuration items for the TOE?

  In the same way, if the components are identified as part of the TOE, they are part of the configuration items.

Issues	Impact on configuration item
xtables-monitor: fix rule printing	True
xtables-monitor: fix packet family protocol	True
nft: Optimize class-based IP prefix matches	True
nft: Fix selective chain compatibility checks	True

Table 3: Issues impacting configuration items

- Has it affected any of the TSF abstraction levels, that is, the functional specification, the TOE design, or the implementation representation?

  During the analysis of the issue, the analyst must define if specifications are impacted.

Issues	Impact on specifications
xtables-monitor: fix rule printing	False
xtables-monitor: fix packet family protocol	False
nft: Optimize class-based IP prefix matches	False
nft: Fix selective chain compatibility checks	False

Table 4: Issues impacting specifications

- Has it affected the architectural description (if the assurance baseline includes a component from the ADV_ARC family)?

  During the analysis of the issue, the analyst must define if the architecture is impacted.

Issues	Impact on Architecture
xtables-monitor: fix rule printing	False
xtables-monitor: fix packet family protocol	False
nft: Optimize class-based IP prefix matches	False
nft: Fix selective chain compatibility checks	False

Table 5: Issues impacting the architecture

- Has it affected the mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design (if the assurance baseline contains a component from the ADV_TDS family), and to the implementation representation (if the assurance baseline contains a component from the ADV_IMP family)?

  During the analysis of the issue, the analyst must define if the interfaces are impacted.

Issues	Impact on Interfaces
xtables-monitor: fix rule printing	False
xtables-monitor: fix packet family protocol	False
nft: Optimize class-based IP prefix matches	False
nft: Fix selective chain compatibility checks	False

Table 6: Interfaces affected

- Has it affected the guidance documentation (if the assurance baseline includes a component from the AGD class)?

  During the analysis of the issue, the analyst must define if the manuals are impacted.

Issues	Impact on Guidances
xtables-monitor: fix rule printing	False
xtables-monitor: fix packet family protocol	False
nft: Optimize class-based IP prefix matches	False
nft: Fix selective chain compatibility checks	False

Table 7: Manuals affected

- Has it affected the testing documentation, that is, the analysis of test coverage, the analysis of the depth of testing or the test documentation (if the assurance baseline includes a component from the ATE class)?

  Yes (Test report is always modified as the tests are automatically performed as part of DevOps. The evidence is automatically provided.)

- Has it affected the vulnerability analysis?

  Yes (The threat model and the risk analysis are automatically updated by the Threagile[4] threat modeling tool. The evidence is automatically provided.)

The model in the next figure is built upon different sources of information and allows to extract information necessary for the Impact Analysis.

[4] https://threagile.io/

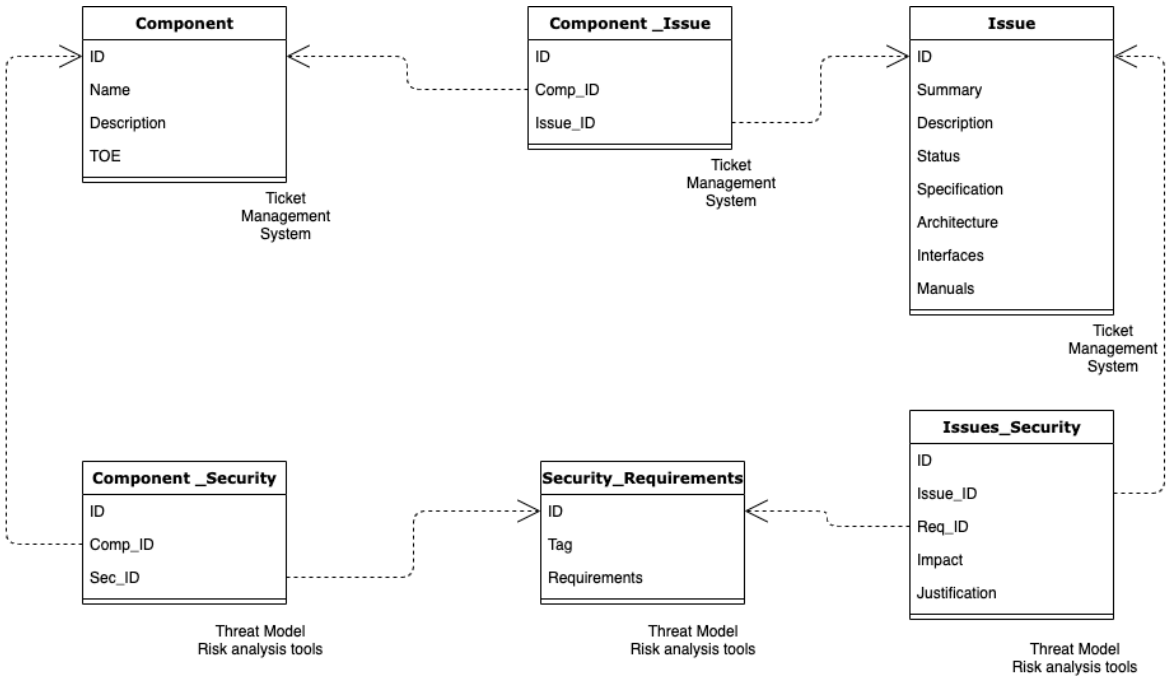

Figure 3: Example database Impact Analysis information

Components are listed in the ticket manager where they are linked to issues corresponding to changes to the software. Issues are in turn linked to security functional requirements in the Threat Model and Risk Analysis tools.

Example for the ticket management service when using GitHub in Figure 4:

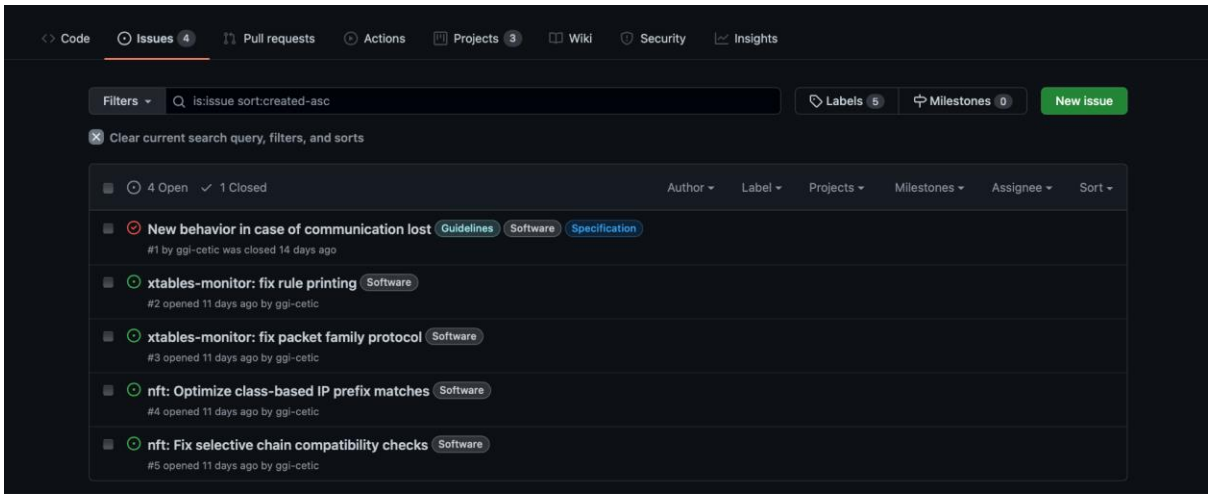

Figure 4: GitHub issues list

If we take as example issue #2 (see Figure 5), the information on the issue allows to make the link between : the issues, the components impacted (iptables project) and the part of the project affected (here only “Software” but labels can be “Guidelines”, “Specification”, …).

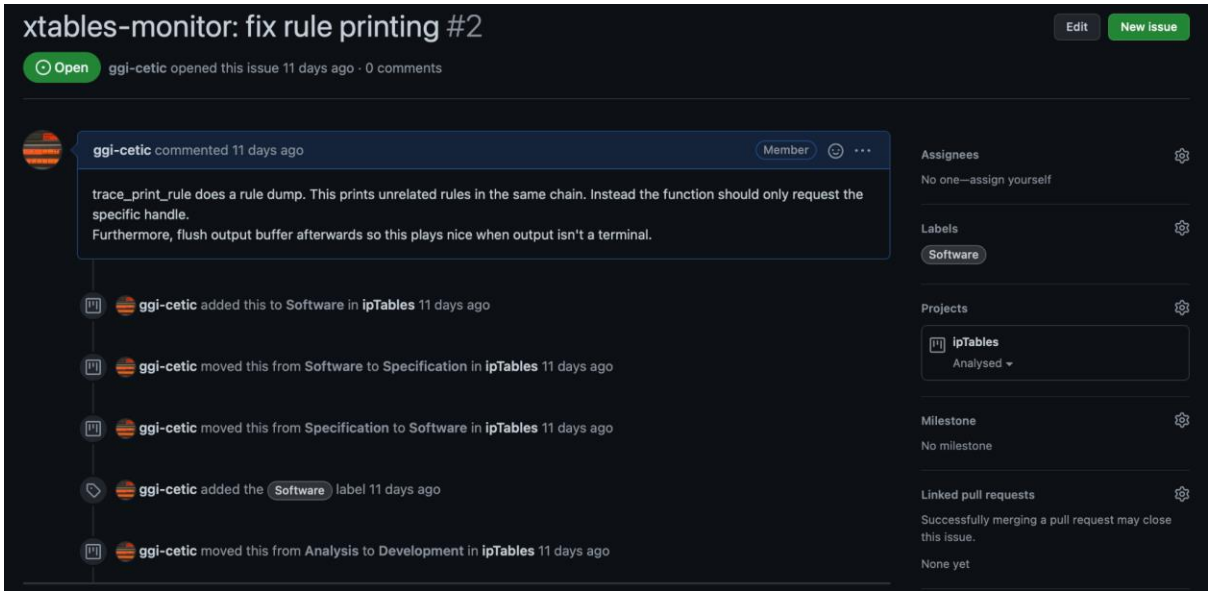

Figure 5: GitHub issue 2 details

3.1 Impact of the changes on the Security Target

To evaluate the impact on the changes of the Security Target, multiple steps were used.

First, here is an extract of some of the Security Functional Requirements (SFR) in the PP [2].

SFR	Requirements
FDP_ACF.1.1	The TSF shall enforce the access control to objects based on security attributes.
FDP_ACF.1.2	The TSF shall enforce rules to determine if an operation among controlled subjects and controlled objects is allowed.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on additional rules.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules.
FDP_IFF.4.1	The TSF shall enforce the information flow control to limit the capacity of illicit information flows to a maximum capacity.
FDP_IFF.4.2	The TSF shall prevent the following types of illicit information flow : tcp shell or http shell.

SFR	Requirements
PMM_IF.1.1	The TOE shall maintain an outgoing heart-beat data flow with other platooning vehicles as specified below: From TOE to VCS (and then to another vehicle TOE). Messages transmitted shall contain the following data computed from the TOE vehicle sensors/algorithms: Vehicle unique identifier - Vehicle speed - Direction - Geo-Position - Timestamp.
PMM_IF.3.1	The TOE shall maintain an incoming flow with other vehicles informing the TOE vehicle about emergency brake maneuvers as specified below: From (another vehicle TOE to vehicle) VCS to TOE. Messages transmitted shall contain the following data: Unique identifier of the vehicle to which the emergency brake has been issued - Emergency brake identifier - Timestamp - Digitally signed certificates.

Table 8: Extract of Security Functional Requirements (SFRs)

In the database described above (see Figure 3), these requirements are associated with components of the solution and an extract allow to visualize information:

Select Components.Name as Name, Security_Requirements.Tag as Tag

From Components, Security_Requirements, Component_Security

Where Component_Security.Comp_ID = Components.ID and Component_Security.Sec_ID = Security_Requirements.ID;

Name	Tag
SafeSecPMM	PMM_IF.1.1
SafeSecPMM	PMM_IF.3.1
iptables	FDP_ACF.1.1
netfilter	FDP_ACF.1.3
netfilter	FDP_ACF.1.4
netfilter	FDP_IFF.4.1
netfilter	FDP_IFF.4.2
iptables	FDP_ACF.1.2

Table 9: Requirements per component of the TOE

Therefore, it is possible to extract only the requirements that are associated with components impacted by the changes described in the chapter Description of the change(s).

Select Components.Name as Name, Security_Requirements.Tag as Tag

From Components, Security_Requirements, Issues_Security, Component_Issue, Issues

Where Component_Issue.Comp_ID = Components.ID and Component_Issue.Issue_ID = Issues.ID and Issues.Status = "Analysed" and Issues.ID = Issues_Security.Issue_ID and Issues_Security.Req_ID = Security_Requirements.ID;

Name	Tag
iptables	FDP_ACF.1.2
netfilter	FDP_ACF.1.3
netfilter	FDP_ACF.1.4
netfilter	FDP_IFF.4.1
netfilter	FDP_IFF.4.2
iptables	FDP_ACF.1.1

Table 10: Filtered requirements per impacted components of the ToE

From these requirements, the Threat Modelling and risk analysis tools5 should be able to define the impact with additional data from the analysis of the issue6.

Select Issues_Security.Issue_ID as Issue, Security_Requirements.Tag as Tag, Security_Requirements.Requirements as Requirements, Issues_Security.Impact as Impact , Issues_Security.Justification as Justification

From Security_Requirements, Issues_Security, Issues

Where Issues.Status = "Analysed" and Issues_Security.Issue_ID = Issues.ID and Security_Requirements.ID = Issues_Security.Req_ID;

Issue	Tag	Requirements	Impact	Justification
2	FDP_ACF.1.2	The TSF shall enforce rules to determine if an operation among controlled subjects and controlled objects is allowed.	False	The changes to the code of ipTables do not affect security requirements as it concerns only display.
3	FDP_ACF.1.2	The TSF shall enforce rules to determine if an operation among controlled subjects and controlled objects is allowed.	False	The changes to the code of ipTables do not affect the security requirement as the requirement is not satisfied by this module.
4	FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on additional rules.	True	The changes impact netfilter in the implementation of the security requirements
4	FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules.	True	The changes impact netfilter in the implementation of the security requirements

[5] e.g. ThreatDragon, Threagile or the SPARTA SATRA risk analysis API
[6] Issues can be found in the GitHub issue tracker: https://github.com/cetic/sparta/issues/

Issue	Tag	Requirements	Impact	Justification
4	FDP_IFF.4.1	The TSF shall enforce the information flow control to limit the capacity of illicit information flows to a maximum capacity.	True	The changes impact netfilter in the implementation of the security requirements
4	FDP_IFF.4.2	The TSF shall prevent the following types of illicit information flow : tcp shell or http shell.	True	The changes impact netfilter in the implementation of the security requirements
5	FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on additional rules.	False	The change to the code of netfilter do not affect the security requirement as it is a compatibility change for checks only
5	FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules.	False	The change to the code of netfilter do not affect the security requirement as it is a compatibility change for checks only
5	FDP_IFF.4.1	The TSF shall enforce the information flow control to limit the capacity of illicit information flows to a maximum capacity.	False	The change to the code of netfilter do not affect the security requirement as it is a compatibility change for checks only
5	FDP_IFF.4.2	The TSF shall prevent the following types of illicit information flow : tcp shell or http shell.	False	The change to the code of netfilter do not affect the security requirement as it is a compatibility change for checks only
2	FDP_ACF.1.1	The TSF shall enforce the access control to objects based on security attributes.	False	The changes to the code of ipTables do not affect security requirements as it concerns only display.
3	FDP_ACF.1.1	The TSF shall enforce the access control to objects based on security attributes.	False	The changes to the code of ipTables do not affect the security requirement as the requirement is not satisfied by this module.

Table 11: Impacted requirements

The Table 11 above justifies whether there is a real impact on requirements and provides reference to evidence.

Chapter 4 Description of the developer evidence modifications

ID	Name	Date	Description	Produced by	New impact	Classes
1	Security Profile	2021-02-01	OVAL security policy	CETIC (security officer)	firewall version update	ADV, AVA
2	CI/CD	2020-01-01	Configuration and execution logs	Gitlab-CI, Ansible	firewall version update	ALC
3	Remediation logs	2020-01-01	Remediation logs	Vacinse , Loki	firewall version update	ALC
4	FW Release notes	2020-01-01	Release notes of the firewall	IPTables	firewall version update	ALC
5	Vulnerability scans report	2020-01-01	Results of the vulnerability scans	OpenSCAP	firewall version update	AVA
6	Compliance status	2020-01-02	Dashboard of compliance checks	Foreman	firewall version update	ALC
7	Change request	2020-01-03	Issue describing the change	Gitlab/GitHub	firewall version update	ALC

Table 12: Developer evidences

4.1 Evidence 1 - Security Profile

As a security profile, we use the OpenSCAP policy[7] for CentOS 8, that describes security requirements and associated checks that need to be satisfied on the TOE. The impact is that the firewall integrity is now checked. The policy is composed of 3 elements[8]:

- the **main OpenSCAP policy** - ssg-centos8-ds-1.2.xml
  - This is a datastream file containing multiple security check profile and the associated checks. The profile chosen is “Standard System Security Profile for Red Hat Enterprise Linux 8”. This file is publicly available on OpenSCAP website, and the one used is in the svn repository.
- the **tailoring file** - ssg-centos8-ds-1.2-CETIC-tailoring.xml
  - This is a tailoring file created using the SCAP Workbench and based on ssg-centos8-ds-1.2.xml file to tailor the checks for the vehicles as some of the checks performed may not be relevant in our case
- the **specific firewall rule** - MyTest-ds.xml
  - This is a datastream file developed with the eSCAPe (Enhanced OpenScap Editor) that helps create Security Content Automation Protocol (SCAP) content files and custom rules, in particular OVAL & XCCDF files.
  - it checks the version of the firewall installed by verifying its sha value

4.2 Evidence 2 - Continuous integration and deployment

The TOE source code and target configuration is hosted on a git repository. Continuous integration and deployment of the TOE is orchestrated by the Gitlab-CI CI/CD engine as follows:

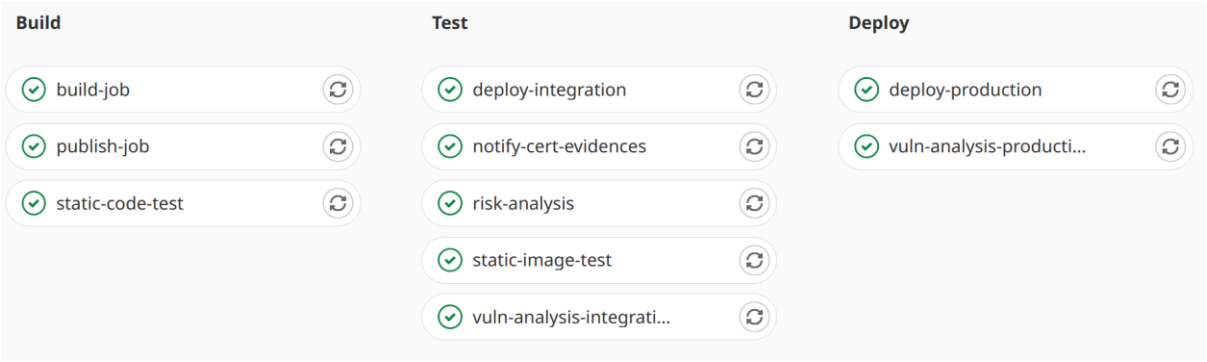

Figure 6: Continuous integration and deployment of the TOE - success run result

This provides an improved DevSecOps pipeline that can integrate with an incremental certification method where the deployment is only allowed to proceed to the Deploy phase when no re-certification is needed [4].

[7] http://www.open-scap.org/security-policies/choosing-policy/

[8] Available in the SPARTA svn repository at https://sparta.technikon.com/03-WPs/WP5-Program-2-CAPE/T54_Demonstration_validation/Vertical1_Evidences/Assurance%20Continuity/1-SP/

The impact is that the CI/CD process vulnerability analysis steps now include checks to verify the firewall integrity.

The CI/CD run results are available in the Gitlab-CI web dashboard and as a pdf format[9].

The pipeline is divided in 3 phases:

- in the build phase, the firewall package is built, published to an artifact repository, and static analysis security tests (SAST) are performed
- in the test phase, the software is deployed in a test environment and dynamic analysis security tests (DAST) are performed, in our case it is a vulnerability analysis scan. At the end of the test phase, risk and threat assessment can take place, and certification evaluator is notified that the evidences are available for evaluation.
- in the deploy phase, the software is deployed in the production environment and additional dynamic analysis security tests (DAST) are performed

Individual CI/CD executions details show the build and deploy steps of the TOE: execution status, date, etc. See Figure 7.

[9] Available in the SPARTA svn repository at https://sparta.technikon.com/03-WPs/WP5-Program-2-CAPE/T54_Demonstration_validation/Vertical1_Evidences/Assurance%20Continuity/2-CICD

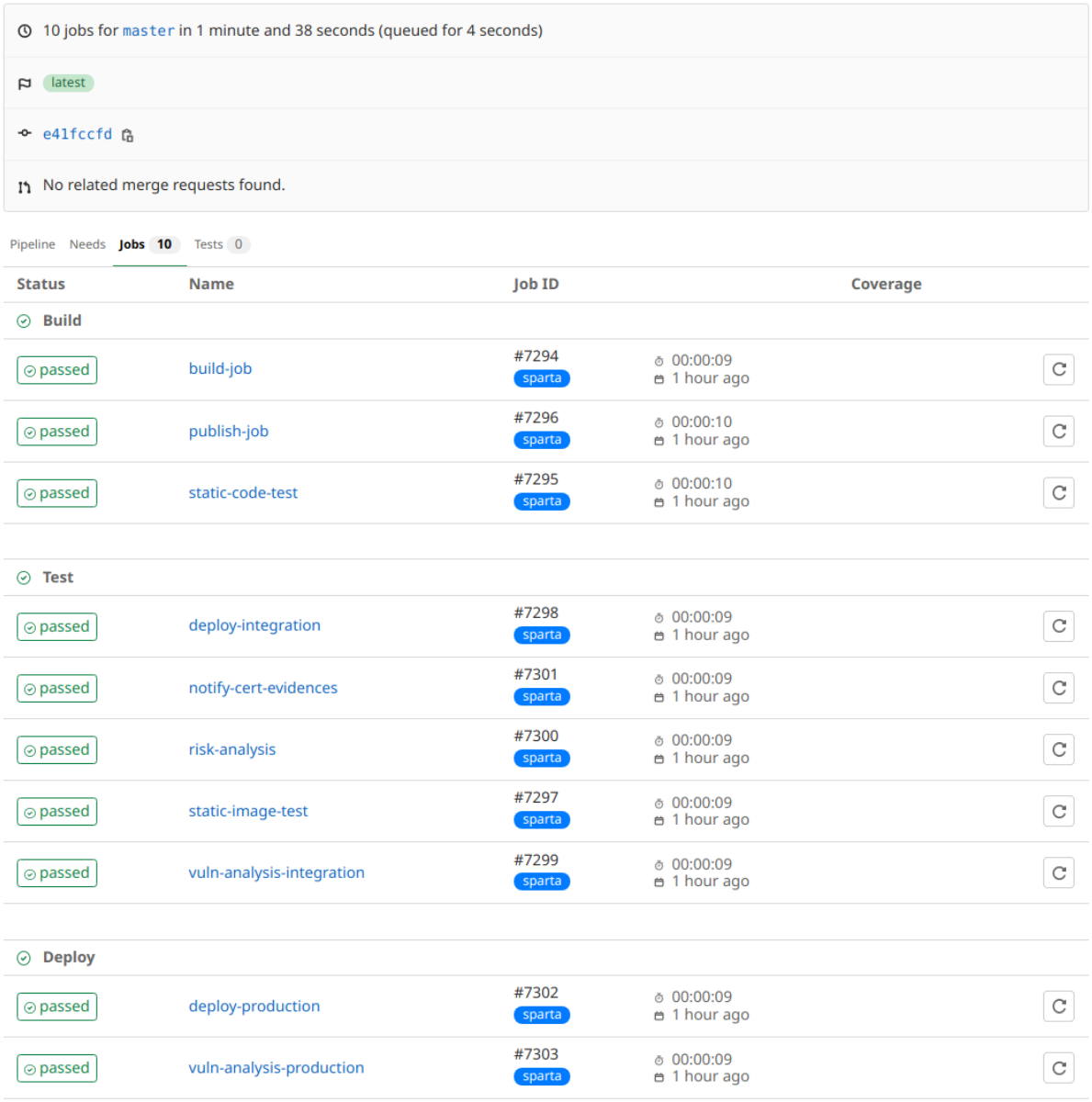

Figure 7: Details of a CI/CD execution

4.3 Evidence 3 - Remediation logs

Remediation logs are collected and available in the SPARTA SVN[10], the remediation logs are impacted because the change in firewall version will trigger a remediation to deploy the new firewall version. The log file is a plain text file where each line corresponds to an event in the remediation process and is structured as follows:

- **timestamp** of the event

[10] https://sparta.technikon.com/03-WPs/WP5-Program-2-CAPE/T54_Demonstration_validation/Vertical1_Evidences/Assurance%20Continuity/3-REMEDIATION

- log **level** corresponding to the severity of the event: DEBUG, INFO, WARNING, ERROR and CRITICAL
- **component** that created the event, this can be a platoon member, vulnerability scanner OpenSCAP or remediation tool Vacsine.
- **information message** provides details on the event

Figure 8 shows a more user-friendly way to view the log file in a web interface using the log aggregation system Grafana Loki[11]. It shows a timeline of the events and provides filtering to explore the logs.

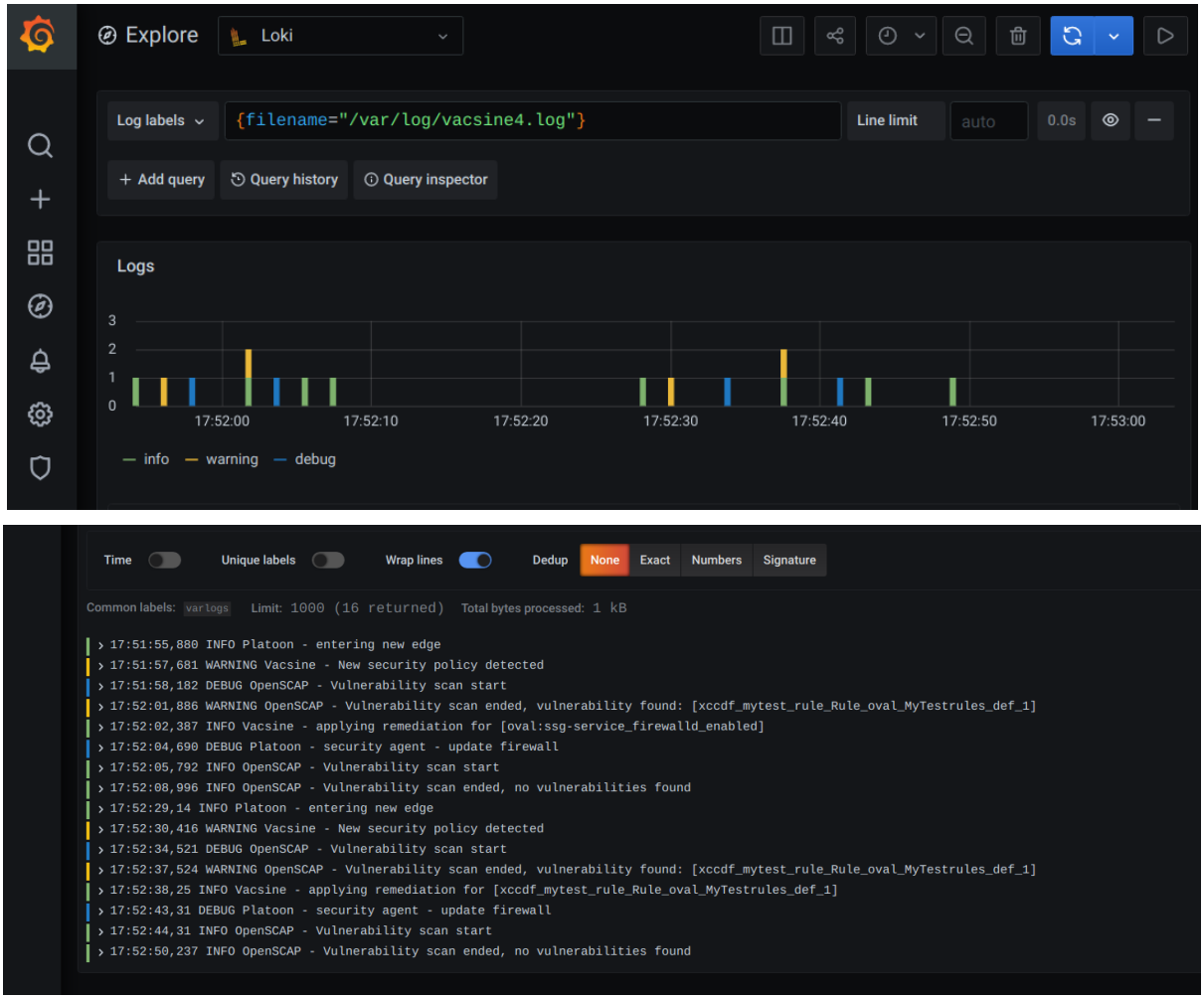

Figure 8: Remediation Logs

4.4 Evidence 4 - Firewall release notes

Firewall release notes describe the changes included in the new version of the firewall. They are available online as a text file, we have added some links[12] to the issue tracker providing more details for relevant changes.

[11] https://grafana.com/oss/loki/

[12] The release notes can be found in the SPARTA SVN at https://sparta.technikon.com/03-WPs/WP5-Program-2-

Florian Westphal (4):

xtables-monitor: fix rule printing

xtables-monitor: fix packet family protocol

xtables-monitor: print packet first

xtables-monitor:

Pablo Neira Ayuso (2):

tests: shell: update format of registers in bitwise payloads.

configure: bump version for 1.8.7 release

Phil Sutter (21):

nft: Optimize class-based IP prefix matches

ebtables: Optimize masked MAC address matches

tests/shell: Add test for bitwise avoidance fixes

ebtables: Fix for broken chain renaming

iptables-test.py: Accept multiple test files on commandline

iptables-test.py: Try to unshare netns by default

libxtables: Extend MAC address printing/parsing support

xtables-arp: Don't use ARPT_INV_*

xshared: Merge some command option-related code

tests/shell: Test for fixed extension registration

extensions: dccp: Fix for DCCP type 'INVALID'

nft: Fix selective chain compatibility checks

nft: cache: Introduce nft_cache_add_chain()

nft: Implement nft_chain_foreach()

nft: cache: Move nft_chain_find() over

nft: Introduce struct nft_chain

nft: Introduce a dedicated base chain array

nft: cache: Sort custom chains by name

tests: shell: Drop any dump sorting in place

nft: Avoid pointless table/chain creation

tests/shell: Fix nft-only/0009-needless-bitwise_0

source: IPTables 1.8.7 changelog[13]

CAPE/T54_Demonstration_validation/Vertical1_Evidences/Assurance%20Continuity/IPTables%201.8.7%20changelog%20-%20details.pdf

[13] https://www.netfilter.org/projects/iptables/files/changes-iptables-1.8.7.txt

4.5 Evidence 5 - Vulnerability scans report

Vulnerability scans are defined to check if the firewall is enabled and configured with secure defaults (e.g. no unneeded protocols or open ports allowed) using Mitre OVAL[14] format (XML file) and provided as input to the OpenSCAP vulnerability assessment tool. Reports are presented in Figure 9 (detailed report) and Figure 10 (Failed check on the firewall version).

Title	Severity	Result
Guide to the Secure Configuration of Red Hat Enterprise Linux 8		
System Settings		
Account and Access Control		
Installing and Maintaining Software		
File Permissions and Masks		
Network Configuration and Firewalls		
firewalld		
Inspect and Activate Default firewalld Rules		
Install firewalld Package	medium	pass
Verify firewalld Enabled	medium	pass
Configure Syslog		
Ensure rsyslog is Installed	medium	pass
Enable rsyslog Service	medium	pass

Figure 9: Extract of the OpenSCAP report

Iptables_check

Rule ID	xccdf_mytest_rule_Rule_oval_MyTestrules_def_1
Result	fail
Multi-check rule	no
OVAL Definition ID	oval:MyTestrules:def:1
Time	2021-06-28T01:03:11
Severity	unknown
Identifiers and References	
Description	File content that checks /sbin for file named iptables

OVAL test results details

File hash test of path /sbin for files named iptables | oval:MyTestrules:tst:1 | true

Following items have been found on the system:

Filepath	Path	Filename	Md5	Sha1
/sbin/iptables	/sbin	iptables	d21b039cdc7d33e6fa727de503d9e1ad	91b678e6ccde5846b2a478e7b34c35c66e529519

Figure 10: Firewall check failed because of hash mismatch

Vulnerability scan is based on the OpenSCAP policy for CentOS 8, that describes a series of checks that need to be performed on the TOE. In this analysis, we consider the checks related to the firewall, in particular we will check if it is enabled.

[14] https://oval.mitre.org/

The vulnerability scan report can be found as a html web page at https://sparta.technikon.com/03-WPs/WP5-Program-2-CAPE/T54_Demonstration_validation/Vertical1_Evidences/Assurance%20Continuity/5-VULNSCAN/scap_report.html

4.6 Evidence 6 - Compliance status

A Foreman global dashboard shows the status of the compliance for each host, and the details of security scans executions (see Figure 11 and Figure 12) according to the compliance policies configured in Foreman (see Figure 13).

The compliance status is impacted because the new firewall integrity check of the vulnerability scans impacts the compliance status of the target hosts (rovers).

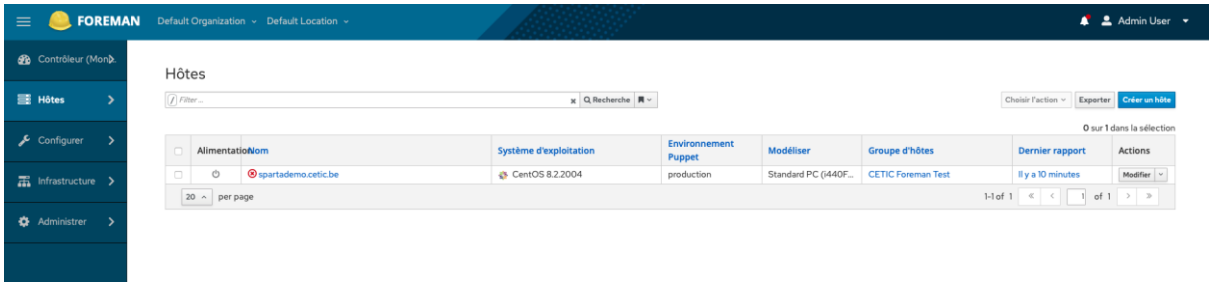

Figure 11: Sample Foreman dashboard showing the details of an host

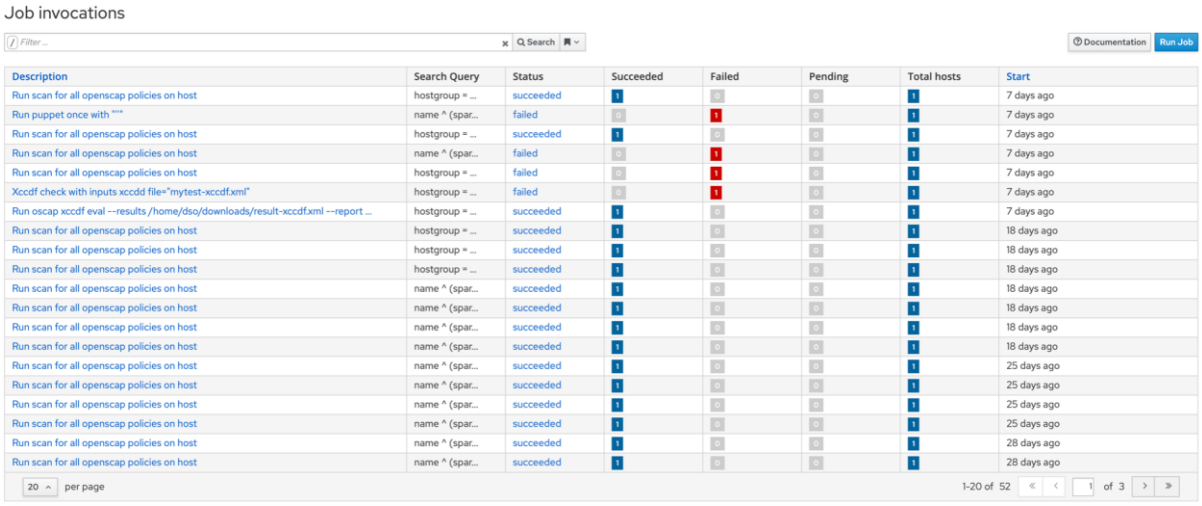

Figure 12: OpenScap security scan logs dashboard in Foreman

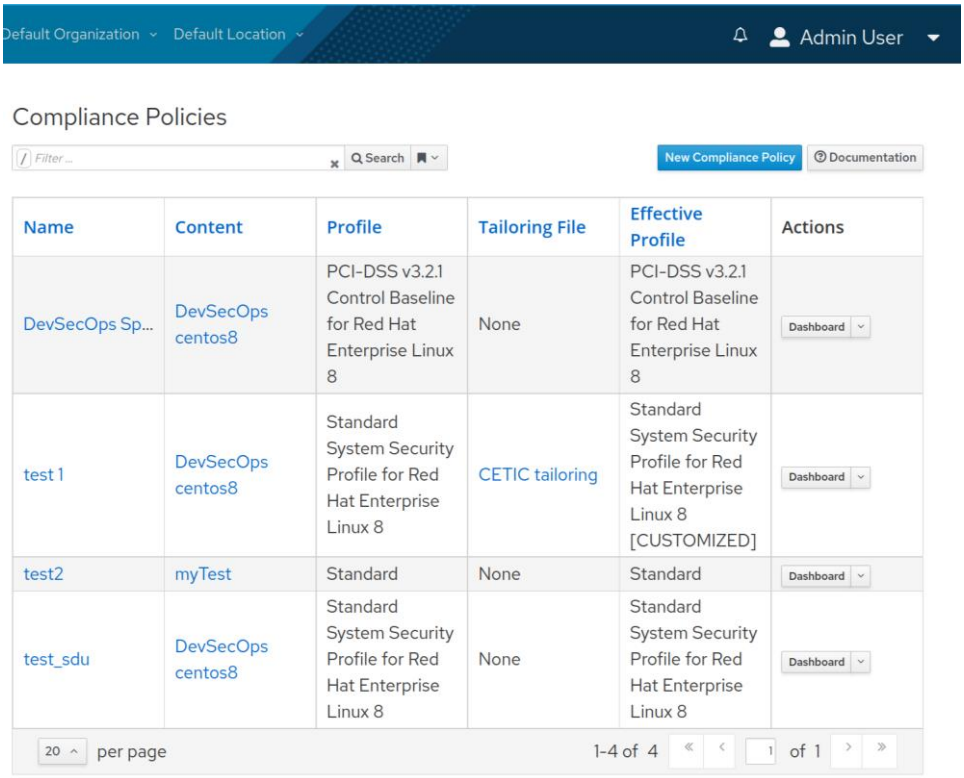

Figure 13 : Compliance policies

The compliance policy presented in Figure 13 and named “test1” is a compliance policy based on a publicly available CentOS policy[15] which was tailored by us to fit our use case. It is based on a Red Hat profile for Standard System.

The compliance policy presented in Figure 13 and named “test2” is a specific compliance policy developed to check that the version of the Firewall installed is the version expected based on the computation of an SHA verification.

Figure 14 presents the compliance policy report for all monitored hosts. Compliance reports for test 1 and test 2 policies on the rover are located in the SPARTA SVN at https://sparta.technikon.com/03-WPs/WP5-Program-2-CAPE/T54_Demonstration_validation/Vertical1_Evidences/Assurance%20Continuity/6-COMPLIANCE/

[15] Public policies can be found at https://www.open-scap.org/security-policies/choosing-policy/

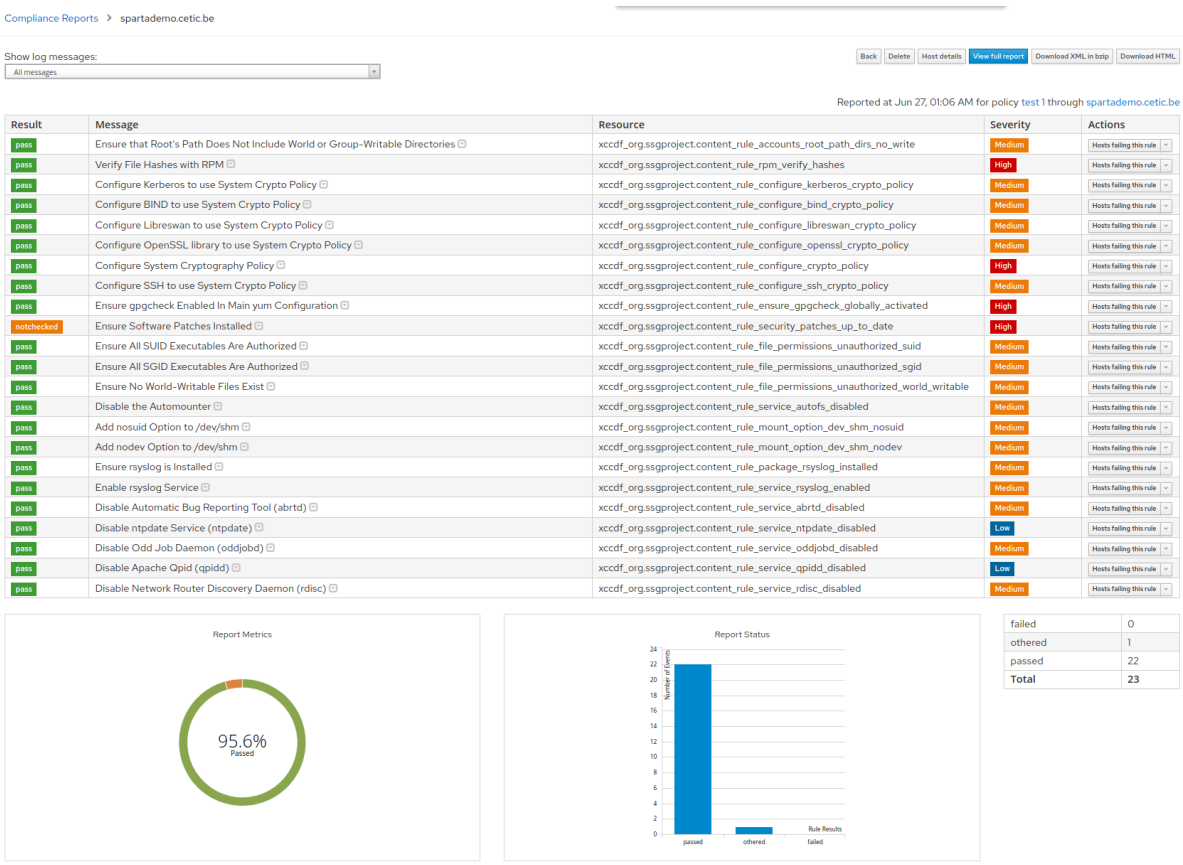

Figure 14: Compliance Policy report - All hosts

4.7 Evidence 7 - Change request

The change request is described in the issue tracker as an issue in the issue tracker[16]. The Figure 15 shows the link between the issue and the associated change in the code (commit).

The impact is that the issue created for the change request will be automatically closed once the system has been updated.

[16] and is available as pdf in the SPARTA SVN at https://sparta.technikon.com/03-WPs/WP5-Program-2-CAPE/T54_Demonstration_validation/Vertical1_Evidences/Assurance%20Continuity/7-CHANGE/

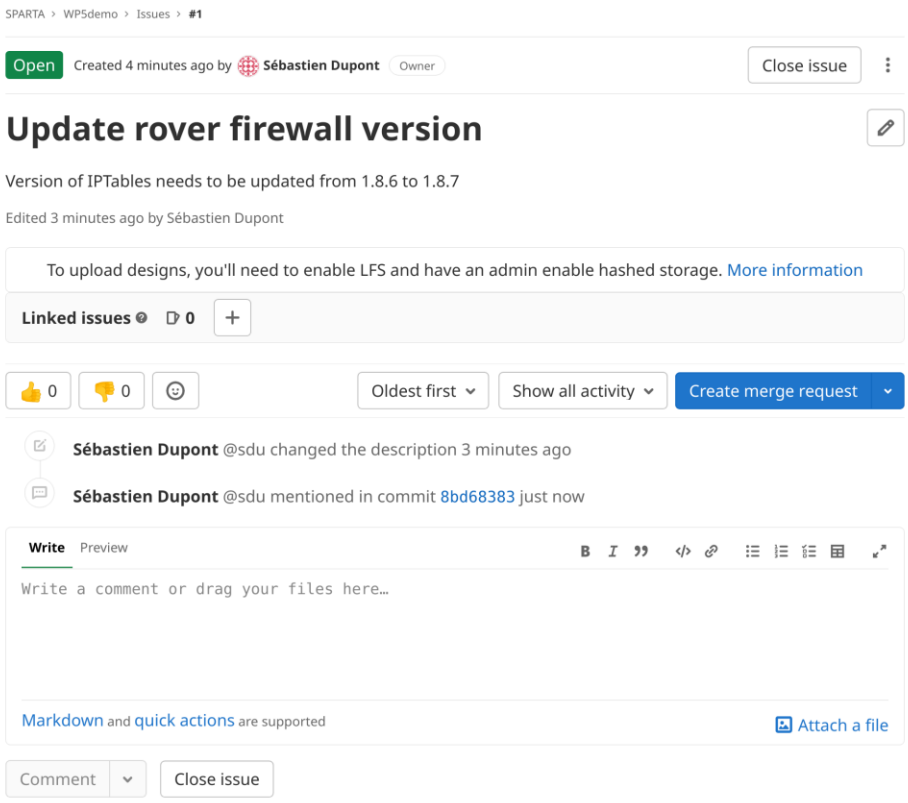

Figure 15: Change request

The version change of the firewall is implemented in the CI/CD automated scripts, and can be observed in the related configuration files and deployment logs. Figure 16 shows the difference in the Ansible configuration file corresponding to the firewall version change in the source code repository, this configuration is used by the Ansible role of Figure 17 to automatically deploy the changes. Logs of the automated deployment of the new version of the Firewall are available in the remediation execution logs.

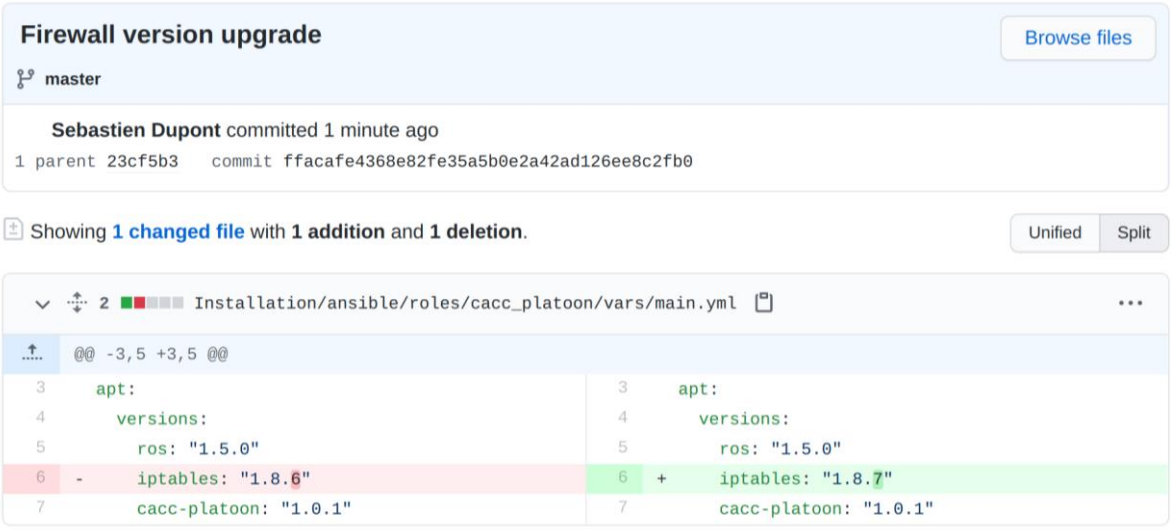

Figure 16: Change of version in the automated deployment configuration

```
---
# tasks/main.yml
# This Ansible role describes the automated steps for
# upgrading software on the vehicles

- name: Stop driving
  description: Leave platoon
  shell: vehicle_shutdown.py

- name: Install software packages in the car
  apt:
    pkg:
    - ros-foxy-ros-base={{ apt.versions.ros }}
    - iptables={{ apt.versions.iptables }}
    - cacc-platoon={{ apt.versions.cacc-platoon }}

- name: Resume driving
  shell: vehicle_resume.py
```

Figure 17: Automated update playbook

4.8 Unchanged or out of CC scope

Some developer evidences are not impacted or not part of CC, we list those here for context.

Name	Date	Description	Produced by	New impact	Classes
ST/PP[17]	2021-02-01	Protection Profile	CETIC (security officer)	firewall version update	ASE
TOE Design	2020-03-01	Architecture document	CETIC (architect)	firewall version update	ADV,
Functional specification	2020-01-01	Software Requirements specification	CETIC (analyst)	firewall version update	ADV,
Risk assessment	2020-01-03	Risk assessment report	SATRA	firewall version update	
Threat analysis	2020-01-03	Threat model and analysis	Threagile	firewall version update	

Table 13: Unchanged or out of scope evidnces

[17] For the purpose of our demonstration, we approximate the security target to the protection profile.

4.8.1 Security Target / Protection profile

See D5.4 Appendix F - Protection Profile for a Safety and Security Platooning Management Module including a firewall – [6].

4.8.2 TOE design

Architecture document - SPARTA D5.2 and D5.3 architecture sections for vertical 1, scenario 2 - [7].

4.8.3 Functional Specification

SRS - SPARTA (D5.1,) D5.2 and D5.3 requirements sections for vertical 1, scenario 2 - [7].

Chapter 5 Conclusion and summary

This document provided a sample impact analysis report for CAPE connected cars “Firewall update” demonstration scenario (Vertical 1 - Scenario 2). In this scenario, a new version of the firewall is available and needs to be deployed on platoon vehicles.

The document describes the change (firewall update), and the modifications to the affected developer evidences:

- the security profile
- the CI/CD pipeline
- the logs for remediation activities
- the firewall release notes
- the vulnerability scan reports
- the compliance status
- the change request

Chapter 6 List of Abbreviations

Abbreviation	Translation
CC	Common Criteria
IAR	Impact Analysis Report
PP	Protection Profile
SFR	Security Functional Requirement
SP	Security Policy
ST	Security target
TOE	Target Of Evaluation
V2I	Vehicle to Infrastructure

Chapter 7 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 1: Introduction and general model

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 2: Functional security components.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 3: Assurance security components.

[4] Dupont, G. Ginis, M. Malacario, C. Porretti, N. Maunero, C. Ponsard and P. Massonet "Incremental Common Criteria Certification Processes using DevSecOps Practices," *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2021, pp. 12-23, doi: 10.1109/EuroSPW54576.2021.00009.

[5] SPARTA CAPE D5.2 “Appendix B Protection Profile for a Safety and Security Platooning Management Module”, January 2021

[6] SPARTA CAPE D5.4 “Appendix F Protection Profile for a Safety and Security Platooning Management Module including a firewall”, version 1.0, January 2022.

[7] D5.3 Demonstrator prototypes, version1.0, January 2020.

[8] Common Criteria Assurance Continuity: CCRA Requirements version 2.1 June 2012