Check Point R81.10 for Gateway and Maestro Configurations

Common Criteria EAL4+ALC_FLR.1

Security Target

Revision 021
20 October 2022

CHECK POINT
YOU DESERVE THE BEST SECURITY

Document History

Revision	Date	Description
001	27 June 2020	Initial draft of ST introduction and TSS created from CheckPoint R80.30 EAL4+SecurityTarget v020
002	12 August 2020	Initial draft of full ST for release to lab for quotation
003	20 November 2020	Update of Maestro appliance and orchestrator terminology and clarification of these components in SP deployment
005	11 March 2021	Updated to include additional appliances.
006	18 May 2021	Updated in response to evaluator comments, to refresh the list of hardware models and confirm the firmware version as R81 (removing ".xx").
007	25 August 2021	Updated to include Orchestrator in the TOE boundary, reflect use of VLAN and SIC for protection of management traffic and confirm TOE version as R81.10.
008	26 August 2021	Updated TOE name to be more concise.
009	27 October 2021	Clarification of VLAN support
010	12 January 2022	Added firmware build and hotfix details
011	14 January 2022	Include Smart-1 625 appliance and update name of CC administration guide
012	01 February 2022	Updated in response to evaluator comments (FMT_SMF application note added)
013	18 May 2022	Updated to reflect used of TLS v1.3
014	30 May 2022	Updated to clarify administrator communication channels with the TOE.
015	14 June 2022	Updated with details of EAL4 HF in section 1.4.3
016	23 June 2022	Updated to reflect Take 4 of the JHF in section 1.4.3
017	08 August 2022	Migrated to new Check Point template
018	24 August 2022	Reintroduction of A./OE.Local_Network
019	10 October 2022	Correction to FMT_SMR.1
020	17 October 2022	Clarification of Security Management Server administrator and Orchestrator administrator roles and link for AGD
021	20 October 2022	Minor correction

CHECK POINT
YOU DESERVE THE BEST SECURITY

Contents

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims and the ST organization. The TOE is the R81.10 firmware providing Firewall, IPS Blade Pattern Matcher, and Security Management Server functionality for Check Point Software Technologies Ltd Security Gateway Appliances. The TOE is being evaluated as a network infrastructure device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- Extended Components Definition (Section 5)
- Security Requirements (Section 6)
- TOE Summary Specification (Section 7)

Conventions

The conventions used in descriptions of the SFRs are as follows:

- Assignment: Indicated with [italicized] text surrounded by square brackets;
- Selection: Indicated with [underlined] text surrounded by square brackets;
- Refinement: Indicated with bold text and strikethroughs, if necessary;
- Assignment within a Selection: Indicated with [italicized and underlined] text surrounded by square brackets;
- Iteration: Indicated by addition of a string starting with “/”.

1.1 Security Target Reference

ST Title:	Check Point R81.10 for Gateway and Maestro Configurations EAL4+ALC_FLR.1 Security Target
ST Revision:	021
ST Publication Date:	20 October 2022

1.2 TOE Reference

TOE Identification:	Check Point R81.10 for Gateway and Maestro Configurations
TOE Developer:	Check Point Software Technologies Ltd.
TOE Type:	Network and Network-Related Devices and Systems – Firmware-only TOE Stateful Traffic Filter Firewall, IPS Blade Pattern Matcher

1.3 TOE Overview

The Target of Evaluation (TOE) is Check Point R81.10 for Gateway and Maestro Configurations.

The TOE is a combination of the firmware for Security Gateway Module(s), a Security Management Server and (when deployed in Scalable Platform configuration) the firmware for the Maestro Orchestrator appliance(s):

- The Security Gateway Module (SGM) is a managed packet filtering firewall application, with IPS pattern matching (software) blade. The TOE provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls. The SGM can either be deployed using instances of a single Security Gateway appliance, which incorporates the SGM or a combination of Security Gateway Modules (SGM) operating in a cluster as part of a Scalable Platform (SP).
- The Security Management Server is used to manage and deploy the security policies and rules to SGM.
- When operating as part of a Scalable Platform (SP), the Orchestrator appliance provides load balancing services for the SGMs.

The Security Management Server is located on a logically protected LAN behind the firewall in single deployment mode, and behind the load-balancing Orchestrator in Scalable deployment mode. All management traffic is communicated between TOE components over secured channels provided by the TOE.

The purpose of the firewall blade is to protect the assets operating on a customer's network from malicious attempts to control or gain access to those assets. The IPS pattern matching blade provides protection against signatures defining malicious and unwanted network traffic, focusing on application and server vulnerabilities, as well as in-the-wild attacks by exploit kits and malicious attackers. The firewall filtering rules, and IPS rules are defined, managed and deployed by the Security Management Server. When in Scalable Deployment, the Orchestrator appliance(s) provide load-balancing across the gateway resources.

1.4 TOE Description

Check Point Security Gateway Appliances R81.10 firmware provides a broad range of packet filtering services, features and capabilities to be delivered by the SGM. This Security Target (ST) makes a set of claims regarding the product's security functionality, in the context of an evaluated configuration. The claimed security functionality is a subset of the product's full functionality whereas all other functionality must be disabled for certified use. The evaluated configuration is a subset of the possible configurations of the product, as defined in this ST and established according to the evaluated configuration guidance (*CC Installation Configuration and Administration Guide*, see Section 1.4.3 below).

The Check Point Security Management Server software provides management functionality for the administration of the Security Gateway Appliances.

When in Scalable Platform deployment, the Maestro Orchestrator firmware provides load-balancing services for the Security Gateway Appliances performing the traffic inspection. The administration of the Orchestrator appliances is performed directly via the Orchestrator WebUI.

This part of the Security Target describes the physical and logical scope and boundaries of the TOE. This description relates to the claimed security functionality that is evaluated in the context of this ST.

The TOE Description consists of the following subsections:

- TOE Architecture – describes the high level TOE components, their deployment and their relationship to each other.
- Required non-TOE Hardware/Software/Firmware – specifies hardware, software and firmware required for the TOE to operate correctly that is not included within the TOE boundary.
- Physical Boundaries – describes the firmware and software parts that constitute the TOE, and identifies the guidance documentation that is considered to be part of the TOE.
- Logical Boundaries – describes the claimed logical security features offered by the TOE.

1.4.1 TOE Architecture

The TOE is the Security Gateway Appliances R81.10 firmware providing firewall capabilities for filtering traffic based on packet rules. It is a distributed system with support for a security management server deployed on a dedicated management LAN behind the firewall. The TOE includes the software executing on the hardware components:

- Security Gateway – Security Gateway Appliance firmware with Firewall and IPS Blade Pattern Matcher functionality installed on either a single appliance or on Security Gateway Modules configured in a cluster (managed by an Orchestrator appliance).
- Security Management – Security Management Server software.
- (When in Scalable Platform deployment) Maestro Orchestrator – Orchestrator appliance firmware providing load balancing for traffic filtering according to Security Groups.

All management traffic communicated between TOE components is transmitted over secured channels provided by the TOE and must be established from internal networks.

Check Point Security Gateway R81.10 Security Gateway firmware is installed on a hardware platform (appliance or Security Gateway Module). The firmware includes the Check Point GAiA operating system (OS), which is an integral part of the Security Gateway firmware and as such is included within the TOE boundary. The OS is responsible for

providing storage for audit trail, an IP stack for in-TOE routing, NIC drivers and an execution environment for daemons and security servers. The same GAiA OS (R81.10) is also deployed on the Security Management server and the Orchestrator appliances.

1.4.1.1 Single Security Gateway configuration

Check Point Security Gateway Appliances mediate information flows between clients and servers located on internal and external networks governed by the firewall, as shown in Figure 1 below. The TOE imposes traffic-filtering controls on mediated information flows between clients and servers according to the site's security policy rules. By default, these security policy rules deny all inbound and outbound information flows through the TOE. Only a Security Management Server administrator has the authority to change the security policy rules.

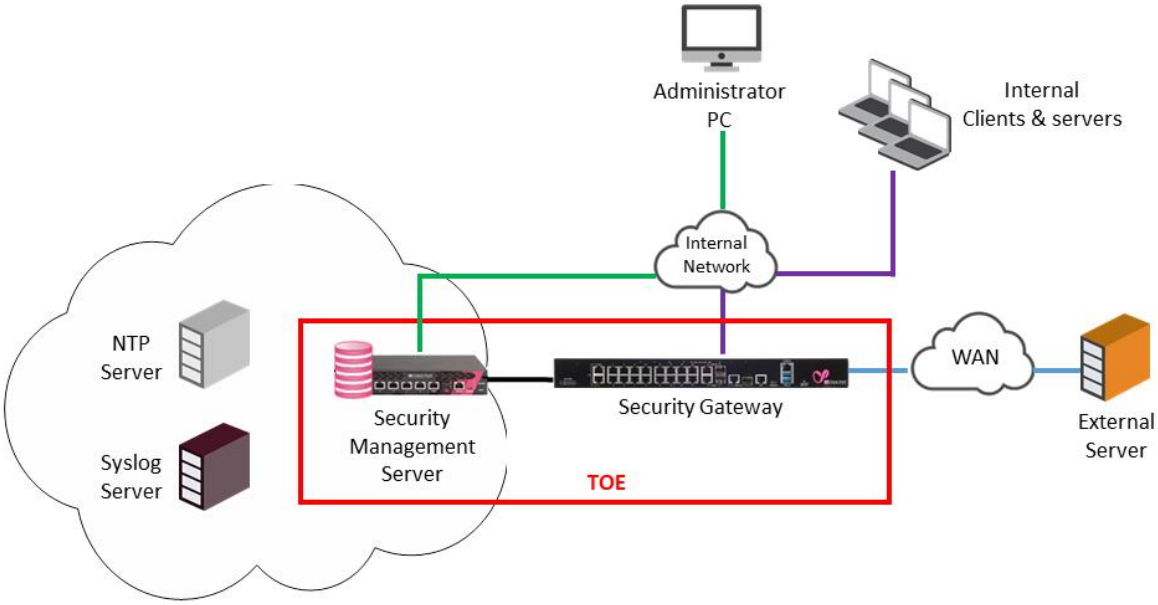


Figure 1 TOE deployment – single appliance

1.4.1.2 Security Gateway Scalable Platform

The traffic-filtering controls on mediated information flows on mediated information flows between clients and servers according to the site's security policy rules are enforced by the gateway in the same manner, whether the TOE is configured as a single appliance or as part of a Scalable Platform deployment with Maestro components. In Scalable Platform deployment traffic is received from untrusted networks by Orchestrator appliances and the Orchestrator appliances distribute the traffic to the SGMs (the SGMs in Scalable Platform deployment are also known as Maestro appliances). The security and threat prevention policies are enforced on the traffic by each SGM, before the SGM forwards the traffic to the trusted networks via the Orchestrator appliance downlink. Every SGM in the cluster has the same security policy.

Figure 2 shows an example Scalable Platform deployment and Figure 3 shows the connection of the Maestro components (Orchestrator appliance and Maestro appliances) within a Scalable Platform deployment. The Orchestrator appliances must be physically located in the same protected environment.

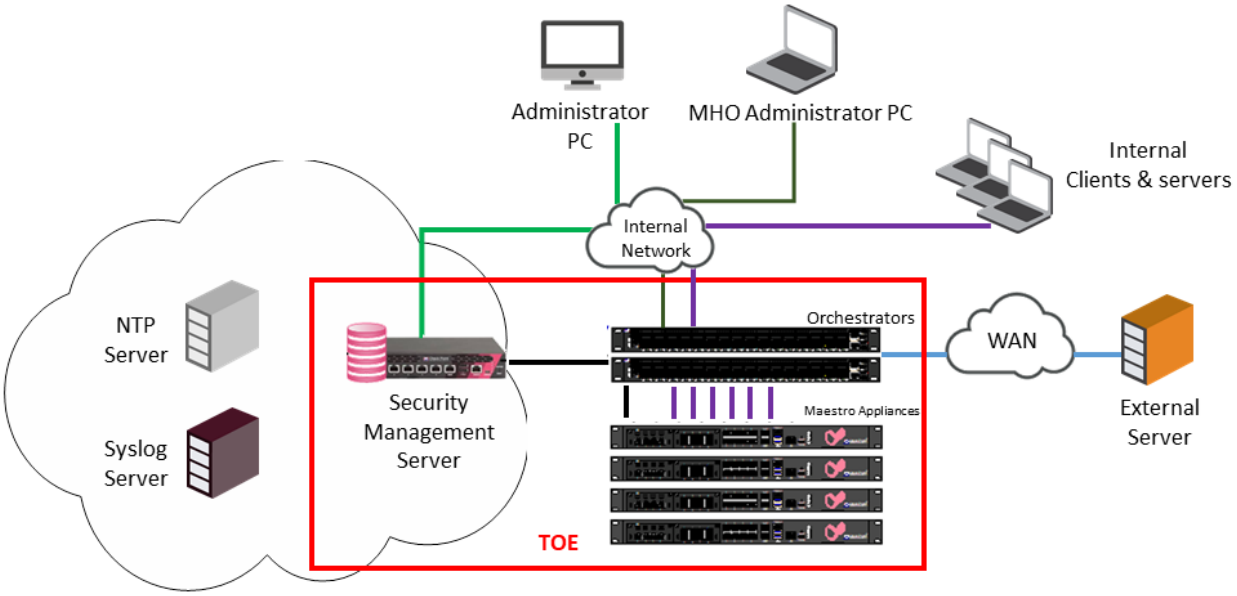


Figure 2 TOE deployment – Scalable Platform

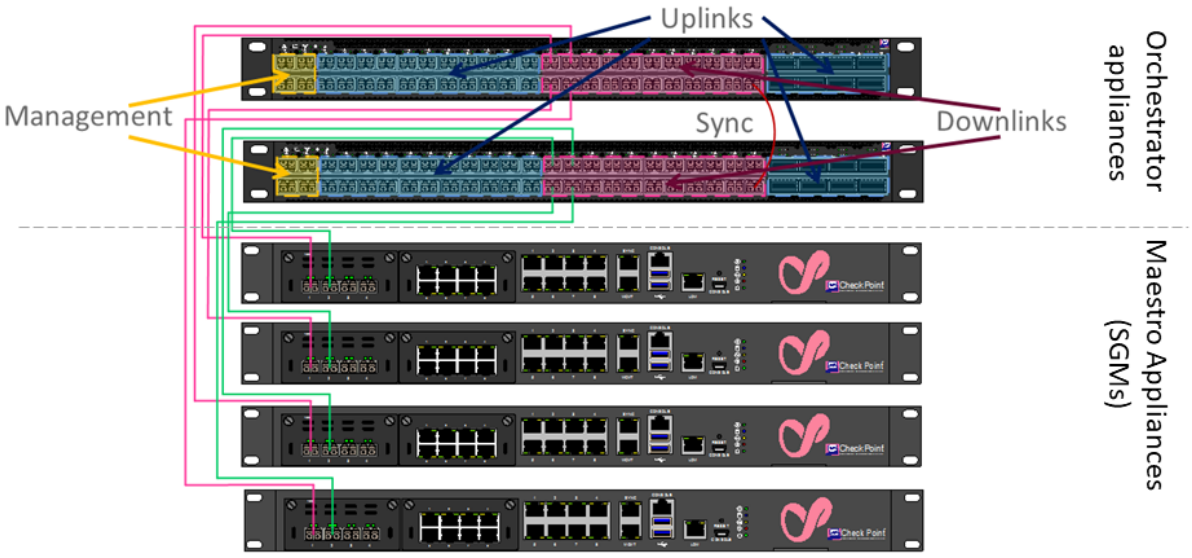


Figure 3 Connection of Maestro components in Scalable Platform deployment

To operate in a Scalable Platform deployment Security Groups are established. A Security Group is a logical group forming an active / active cluster segregated from other Security

Groups. Security groups include network interfaces (uplinks), Management interfaces and Appliances (SGMs). A single IP address is assigned per Security Group for management communications and policy installation. This is concept is known as Single Management Object (SMO).

There is a relationship between a downlink ports and SGM, so in this way an Orchestrator appliance determines which SGM will inspect the traffic.

The Orchestrator appliance provides traffic load-balancing mechanisms across Security Group members, calculating traffic distribution dynamically so that members of the security group can be seamlessly added and removed. HyperSync is used as the Cluster Synchronization mechanism.

Within the same cluster (Security Group) each connection is synchronized to two Security group members (Active and Backup). One of SGMs is Active per given connection (it enforce security policy with all related inspections and protections), another one is Backup (keep connection in its connection table) and will replace Active in case of failure. The SGM receiving the connection will decide which is its backup SGM, and will forward connection information to that backup SGM over the SYNC-VLAN. The REST API is used by the SGM to inform Orchestrator if a SGM is unavailable.

The Security Groups are managed from an MHO Administrator PC using the administrative WebUI provided on the Orchestrator appliance. The MHO Administrator PC must be located on the internal network, which is the only network connected to the management port of the Orchestrator appliance. Furthermore, this communication between the MHO Administrator PC and the Orchestrator appliance is protected using TLS v1.3. The browser on the MHO Administrator PC must be configured to only support TLS v1.3 connection requests.

When a new SGM is added to a cluster, Orchestrator uses LLDP (Link Layer Discovery Protocol) to discover it and notify the other SGMs that a new SMG has been added.

In a Single site deployment, all components (SGMs, Orchestrator appliances and, Management Server) are all physically connected using Direct Attached Copper (DAC) or fibre cables, within a single secure location. Use of multiple Orchestrator appliances within a single site deployment is supported in the evaluated configuration. The Orchestrator appliances communicate between each other using REST API. In a dual site deployment, a direct (tunnelled) connection is required between the two Orchestrator appliances, which again is communication in the environment of the TOE. However, this dual site deployment is outside the TOE configuration.

1.4.1.3 Security Management Server

Security Management Server Administrators also need to authenticate to the TOE before they can use the Management APIs to access Security Management. This is achieved using a password-based authentication mechanism.

Security Gateway Modules or one or more Security Gateway appliances are managed by a Security Management server installation (includes GAiA operating system and Security Management application). The Security Management server maintains security policy

information for the gateways, and collects audit records from the gateways for review by Security Management Server administrator. The audit records may also be sent to an external log server (which in the evaluated configuration must be hosted on the logically-protected dedicated management LAN hosted behind the firewall).

The Security Management Server administrator (remotely) communicates with the Security Management server via the Check Point REST API over TLS v1.3 or (locally) via a directly connected console to the CLI.

- Local administration is only supported during initial installation or troubleshooting when the TOE is taken out of operation.
- Remote administration using REST API must be performed from an Administrator PC located on the internal network and the browser on the Administrator PC must be configured to only support TLS v1.3 connection requests. Only the internal network can be connected to the management port on the Security Management Server.

Communication between the Security Management server and the SGMs is protected by SIC (a proprietary Secure Internal Communication protocol). Use of the Check Point SmartConsole is not supported in the evaluated configuration.

In Scalable Platform deployment, all traffic for the management of the SGMs is transmitted over the network connection between the Security Management server and the SGM, via a separate VLAN provided by the Orchestrator appliance.

1.4.2 Required non-TOE Hardware/Software/Firmware

The TOE requires hardware platforms for it to operate, but these are not part of the TOE; they exist within the TOE environment. These hardware platforms are Check Point Security Gateway Appliances/Security Gateway Modules and Security Management Appliances, which execute firmware installed from the applicable R81.10 firmware image, and the Orchestrator appliances if the TOE is deployed as a Scalable Platform. There are separate firmware images for:

- Security Gateway appliances[1]
- Scalable Platform (Maestro) Gateway appliances
- Security Management Server appliances
- (when in SP deployment) Maestro Hyperscale Orchestrator appliances.

The differences between the appliances are mainly in hardware makeup and physical ports. All platforms are x86 based hardware.

The hardware platforms are as follows:

- Maestro appliances running **R81.10** firmware (Scalable Platform image):

[1] Although a Virtual Machine image is provided for the CloudGuard) virtual appliance, the virtual appliance is executing the same firmware as the Security Gateway appliances.

    - Maestro Hyperscale Gateway
        - 6200, 6600, 6700, 7000, 16600, 28600
- Security Gateway appliances running **R81.10** firmware (Security Gateway appliance image):
    - High End Enterprise Data Center:
        - 16000, 16200, 26000, 28000, 28600, 16600
    - Enterprise:
        - 6200, 6400, 6500, 6600, 6700, 6900, 7000
    - Small Business and Branch Offices:
        - 3600, 3800
- Virtual appliances running **R81.10** firmware (VM image including the Security Gateway appliance firmware image):
    - CloudGuard for ESXi running on a HPE D360 G10
- Smart-1 Security Management Server appliances running the **GAiA R81.10** firmware(Security Management Server image):
    - High End Enterprise:
        - 625, 600-M, 600-S, 6000-L, 6000-XL
- Orchestrator appliances
    - Maestro Hyperscale Orchestrator 140
    - Maestro Hyperscale Orchestrator 170
    - Maestro Hyperscale Orchestrator 175

The following additional IT environment components required to support the secure operation of the TOE. All of these components have to be hosted in the secure Management LAN:

- Administration PC – This PC is the machine used by the Security Management Server administrator to issue the management commands to the SGMs over REST API.
- MHO Administrator PC – This PC is the machine used by the Orchestrator administrator to manage the Orchestrator appliances via the Orchestrator WebUI.
- NTP Server – This server provides NTP time services to the TOE (Security Management Server and Orchestrator appliances).
- Syslog Server – This server provides storage for audit logs exported by the TOE.

Tools such Postman can be used to issue the REST API commands from the administration PC to the Security Management server, as described in the *CC Installation Configuration and Administration Guide*.

1.4.3 Physical Boundaries

The physical boundary of the TOE is the Security Gateway Appliances R81.10 firmware and Security Management Server firmware (i.e. it is a software only TOE boundary).

There is a single variant of the R81.10 firmware .iso package depending on which GAiA operating system is supported by the appliance:

Firmware Package	Download file	SHA-256 hash value
Security Gateway or Management Server	Check_Point_R81.10_T335.iso	17817e134c4f0a1c65b59af74baab8939b29a64f653476cad5e4b219f5fd147d
Scalable Platform (Maestro) Gateway and Maestro Hyperscale Orchestrator	Check_Point_R81.10_T338_ScalablePlatform.iso	4215084137b8b66185340f9ec09592ec172b039f4b390547ae31b074b9c5b621
R81.10 EAL4 certification Hotfix	Check_Point_R81_10_JHF_T22_EAL4_HF_MAIN_Bundle_T4_FULL.tar	754e0d0604da6b773dc6d1db6035fd581835976c36c2d32a60d8S20c160b75b

Table 1 TOE firmware packages

The above firmware packages contain the software components listed in **Error! Reference source not found.** and **Error! Reference source not found.** that comprise the TOE. The unique version of the TOE is determined by the execution of two commands on the console during installation:

```
show version all
```

Security Gateway appliance	Maestro appliance
Product version Check Point Gaia R81.10	Product version Check Point Gaia R81.10
OS build 335	OS build 338
OS kernel version 3.10.0-957.21.3cpx86_64	OS kernel version 3.10.0-957.21.3cpx86_64
OS edition 64-bit	OS edition 64-bit

Table 2 TOE Firmware version - Gateway and Maestro appliances

Smart-1 Security Management Server	Orchestrator appliance
Product version Check Point Gaia R81.10	Product version Check Point Gaia R81.10
OS build 335	OS build 338
OS kernel version 3.10.0-957.21.3cpx86_64	OS kernel version 3.10.0-957.21.3cpx86_64

OS edition 64-bit	OS edition 64-bit

Table 3 TOE Firmware version – Management server and Orchestrator appliance

```
cpinfo -y all
```

Security Gateway appliance (the order may be different)
This is Check Point CPinfo Build 914000215 for GAIA
[IDA]
No hotfixes
[MGMT]
HOTFIX_R81_10_JHF_T22_EAL4 _HF_MAIN Take: 4
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 HOTFIX_GOT_TPCONF_AUTOUPDATE
FW1 build number:
Check Point software version R81.10 - Build 883
kernel: R81.10 - Build 002
[SecurePlatform]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[PPACK]
No hotfixes
[AutoUpdater]
No hotfixes
[CPinfo]
No hotfixes
[DIAG]
No hotfixes
[CVPN]
No hotfixes

Security Gateway appliance (the order may be different)
[hcp_wrapper]
HOTFIX_HCP_AUTOUPDATE
[CPUpdates]
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 BUNDLE_GOT_TPCONF_AUTOUPDATE Take: 96 BUNDLE_HCP_AUTOUPDATE Take: 44

Table 4 TOE Component versions – SGM appliances

Maestro Gateway (Scalable Platform Security Gateway) appliance
This is Check Point CPinfo Build 914000215 for GAIA
[IDA]
No hotfixes
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 HOTFIX_GOT_TPCONF_AUTOUPDATE
FW1 build number:
This is Check Point's software version R81.10 - Build 884 kernel: R81.10 - Build 002
[SecurePlatform]
HOTFIX_R81_JHF_T22_EAL4_HF_MAIN Take: 4
[PPACK]
No hotfixes
[AutoUpdater]
No hotfixes
[CPinfo]
No hotfixes
[SMO]

Maestro Gateway (Scalable Platform Security Gateway) appliance
No hotfixes
[DIAG]
No hotfixes
[CVPN]
No hotfixes
[hcp_wrapper]
HOTFIX_HCP_AUTOUPDATE
[CPUpdates]
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 BUNDLE_GOT_TPCONF_AUTOUPDATE Take: 96 BUNDLE_HCP_AUTOUPDATE Take: 44

Table 5 TOE Component versions –Maestro appliances

Smart-1
Check Point CPinfo Build 914000215 for GAIA
Local host is not a Gateway
[IDA]
No hotfixes
[MGMT]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 HOTFIX_GOT_MGMT_AUTOUPDATE HOTFIX_WEBCONSOLE_AUTOUPDATE HOTFIX_GOT_TPCONF_MGMT_AUTOUPDATE
FW1 build number:
This is Check Point Security Management Server R81.10 - Build 220 This is Check Point's software version R81.10 - Build 883
[SecurePlatform]

Smart-1
HOTFIX_ R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[AutoUpdater]
No hotfixes..
[CPinfo]
No hotfixes..
[DIAG]
No hotfixes..
[Reporting Module]
No hotfixes..
[CPuepm]
No hotfixes..
[VSEC]
No hotfixes..
[SmartLog]
No hotfixes..
[SFWR77CMP]
No hotfixes..
[SFWR80CMP]
No hotfixes..
[R77CMP]
No hotfixes..
[R8040CMP]
No hotfixes..
[MGMTAPI]
No hotfixes..
[CPUpdates]
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4 BUNDLE_DC_CONTENT_AUTOUPDATE Take: 12 BUNDLE_GOT_MGMT_AUTOUPDATE Take: 91 BUNDLE_DC_INFRA_AUTOUPDATE Take: 26 BUNDLE_WEBCONSOLE_AUTOUPDATE Take: 43

Smart-1
BUNDLE_HCP_AUTOUPDATE Take: 44 BUNDLE_GOT_TPCONF_MGMT_AUTOUPDATE Take: 32
[hcp_wrapper]
HOTFIX_HCP_AUTOUPDATE
[itp_wrapper]
HOTFIX_GOT_MGMT_AUTOUPDATE

Table 6 TOE Component versions – Smart-1 Security Management Server

Orchestrator appliance
Check Point CPinfo Build 914000215 for GAIA
[IDA]
No hotfixes
[CPFC]
No hotfixes
[FW1]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
FW1 build number:
This is Check Point's software version R81.10 - Build 884
[SecurePlatform]
HOTFIX_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4
[PPACK]
No hotfixes
[AutoUpdater]
No hotfixes.
[CPinfo]
No hotfixes.
[SMO]
No hotfixes
[CPUpdates]
BUNDLE_R81_10_JHF_T22_EAL4_HF_MAIN Take: 4

Table 7 TOE Component versions – Maestro Orchestrator appliances

All firmware is delivered from the Check Point User Center (https://usercenter.checkpoint.com) by user initiated download over an HTTPS protected connection with a 2048-bit RSA certificate.

For verification of integrity of the delivered image hash values are available separately and a software tool is supplied to allow a customer to check the hash values against the supplied image. The hash values are also reflected in Table 1 above.

The TOE includes the guidance:

- R81.10 CC Firmware for Gateway and Maestro Configurations, Installation and Configuration, Administration Guide, Rev 002, 20 October 2022

This guidance documentation (available in PDF format) is available for download from the Check Point User Center (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk173465).

1.4.4 Logical Boundaries

This section summarizes the security functions provided by R81.10:

- Security audit
- Stateful Traffic Filtering Firewall
- Packet Filtering
- Intrusion Prevention Systems
- Identification and authentication
- Security management
- TOE access
- Protection of TSF

The following table shows which TOE component is responsible for the implementation of each of the SFRs:

Requirement Class	Security Gateway Appliance/Maestro Gateway			Management Server		Orchestrator Appliance
	Firewall blade	IPS blade	GAiA	Management Server application	GAiA	GAiA
FAU: Security audit	X	X	X	X		X
FFW: Stateful Traffic	X	X				

Filtering Firewall						
IPS: Intrusion Prevention Systems		X				
FIA: Identification and authentication			X	X	X	X
FMT: Security management				X		X
FTA: TOE access				X		X
FPT: Protection of the TSF			X		X	X

Figure 4 Security Functionality provided TOE components

1.4.4.1 Security audit

The Security Management server generates audit records for all changes to configuration of the TOE relating to filtering policies. In addition, audit records are generated for changes to authentication credentials and all administrative login/logout activities at the Security Management server.

The SGMs generate audit records of the application of rules configured with the 'log' operation. The SGMs can be configured to store these logs locally, forward logs to the Security Management Server, or both. If configured to send logs to the Security Management Server, in the event of a loss of network connectivity to the Security Management Server, then the SGM will store locally until the connection is restored. The Management Server generates audit records for specified events, recording at least date and time of the event, type of event, subject identity, and the outcome. The SGM can be configured to send audit logs to a log server (hosted in the dedicated management LAN) as well. Finally, note that the SGMs can be configured such that if they run out of disk space for local logs, they can block all connections. The audit records include a timestamp of the event using the clock provided by the operating system.

When in SP deployment, the Orchestrator appliance generates audit records for all changes to configuration of the Security Groups. In addition, it generates audit records for changes to authentication credentials and all administrative login/logout activities on the Orchestrator appliance.

1.4.4.2 Packet Filtering and Stateful Traffic Filtering Firewall

The SGMs support many protocols for packet filtering including ICMPv4, IPv4, TCP and UDP. The firewall rules implement the SPD rules (permit, deny, bypass). Each rule can be configured to log status of packets pertaining to the rule. All codes under each protocol are implemented.

Routed packets are forwarded to a TOE interface with the interface's MAC address as the layer-2 destination address. The TOE routes the packets using the presumed destination address in the IP header, in accordance with route tables maintained by the TOE.

IP packets are processed by the Check Point Security Gateway Appliances/Modules software, which associates them with application-level connections, using the IP packet header fields: source and destination IP address and port, as well as IP protocol. Fragmented packets are reassembled before they are processed.

The TOE mediates the information flows according to a Security Management Server administrator-defined policy. Some of the traffic may be either silently dropped or rejected (with notification to the presumed source).

An IPS engine is integrated with the product's traffic-filtering functionality, matching traffic with predefined attack signatures and providing reaction capabilities.

The TOE's firewall capabilities are controlled by defining an ordered set of rules in the Security Rule Base. The Rule Base specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, at what times, whether to log the connection and the logging level.

1.4.4.3 Intrusion Prevent System (IPS)

The SGMs provide a multi-layer IPS engine that is integrated into the product (see Section 1.4.4.2 for a description of the TOE's IPS related packet filtering mechanism). Traffic that has been allowed by the firewall security policies is matched against a combined set of protocol enforcement and pattern matching logic that identifies suspicious network traffic and assigns Confidence Level (that the traffic indeed contains an attack) and Severity (potential impact of the attack on protected resources) security attributes to the traffic. Based on these attributes and on Security Management Server administrator-specified security policy settings, the IPS engine (blade) may take action by generating applicable log records (detect) and optionally blocking the traffic (prevent).

1.4.4.4 Identification and authentication

The Security Management Server and (when in SP deployment) Orchestrator appliances implement a password-based authentication mechanism that identifies Security Management Server and (when in SP deployment) Orchestrator administrators via usernames. Three sequential failed authentication attempts made by an administrator will result in a lockout of the administrator account for 30 minutes.

1.4.4.5 Security management

The Security Management server allows both local and remote administration for management of the TOE's security functions. The single Security Management Server administrator profile "read write all" is supported in the evaluated configuration. A Security Management Server administrator can log in locally to the TOE using a serial connection. The Security Management Server administrator is greeted with a console environment,

where configuration is mainly done through command-line syntax. The local login operates in a Check Point shell (based on top of a Unix shell).

Remote administration of the SGM security policies is available via the Security Management server using the Check Point REST API (as defined at https://sc1.checkpoint.com/documents/latest/APIs/#web). Again, the Security Management Server administrator has to authenticate to the Security Management server before being able to successfully initiate any management functionality. This management functionality includes configuration of network objects (hosts, NAT, etc), firewall policies, IPS policies, Security Management Server administrator accounts, auditing functionality.

In the evaluated configuration the management workstation must be connected to the same dedicated management LAN as the Management Server.

When in SP deployment, administration of the Orchestrator appliances is performed using the WebUI provided by the Orchestrator appliance[2]. This WebUI provides functionality to manage the Security Groups, as well as the Orchestrator administrator accounts and auditing functionality.

1.4.4.6 TOE Access

Remote Security Management Server administrator sessions with the Management Server (i.e. those established via the Check Point REST API) will be terminated after defined periods of inactivity or when termination is initiated by the administrator.

Similarly, when in SP deployment, WebUI sessions with the Orchestrator appliance will be terminated after defined periods of inactivity or when termination is initiated by the Orchestrator administrator.

1.4.4.7 Protection of the TSF

Each TOE component (Security Gateway, Security Management Server and Orchestrator) provides a system clock that is synchronized with a time server (provided in the IT environment).

The TSF data transmitted between TOE components (Gateways and Management Server, and when in SP deployment with Orchestrator appliances) will be protected using VLANs to separate management traffic from user data and encryption of the management traffic using SIC.

The TSF data transmitted (on internal networks) between the Security Management Server administrator and Security Management Server (and when in SP deployment between the Orchestrator administrator and Orchestrator) will be protected from modification and disclosure using TLS v1.3.

[2] The Orchestrator appliances can also be managed using the Orchestrator CLI over SSH, but this is not supported in the evaluated configuration.

2 Conformance Claims

This TOE is conformant to the following CC specifications:

2.1 Common Criteria Conformance Claims

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
  - Part 3 Conformant

2.2 Protection Profile Conformance Claims

This Security Target does not make any claims to conform to any published Protection Profile.

2.3 Packages Conformance Claims

The TOE claims conformance to Evaluation Assurance Level 4 (EAL4) and augmented by ALC_FLR.1 – Basic Flaw remediation.

2.4 Conformance Rationale

The Security Target makes no Protection Profile conformance claims and so there is no requirement for a conformance rationale.

3 Security Problem Definition

3.1 Threats

3.1.1 T.NETWORK_DISCLOSURE

An attacker may attempt to “map” a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.

3.1.2 T.NETWORK_ACCESS

With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.

3.1.3 T.MALICIOUS_TRAFFIC

An attacker may attempt to send malformed packets or sequences of network packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash, to gain use of unauthorized services on the target machine or to gain unauthorized access to user data on the target machine.

3.1.4 T.UNAUTHORIZED_ADMIN_ACCESS

An attacker may attempt to gain administrator access to the SGM by nefarious means such as masquerading as an administrator to the SGM.

3.1.5 T.UNDETECTED_ACTIVITY

An attacker may attempt to access, change, and/or modify the security functionality of the SGM without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

3.2 Organizational security policies

There are no organizational security policies imposed on the TOE by this Security Target.

3.3 Assumptions

This section of the security problem definition shows the assumptions that are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment.

Each assumption must be associated with one or more security objective for the TOE operational environment, as indicated.

3.3.1 A.PHYSICAL_PROTECTION

The hardware components on which the TOE executes are assumed to be physically protected in its operational environment (e.g. server room, data center) and not subject to physical attacks that compromise the security and/or interfere with the TOE's physical interconnections and correct operation. This also applies to the Maestro components if deployed as Scalable Platform. This protection is assumed to be sufficient to protect the TOE and the data it contains from physical compromise. As a result, this Security Target does not include any requirements on physical tamper protection or other physical attack mitigations. The Security Target does not expect the TOE to defend against physical access that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate it.

3.3.2 A.LIMITED_FUNCTIONALITY

The TOE components are assumed to only provide services to support networking, filtering and IPS functionality as its core function, either directly by applying the policies, or indirectly by providing management functionality for those features or traffic load-balancing. The TOE components do not provide functionality that could be deemed as general-purpose computing services.

3.3.3 A.TRUSTED_ADMINSTRATOR

The authorized administrator(s) for the TOE are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the TOE. The TOE is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the TOE.

3.3.4 A.CONNECTIONS

It is assumed that the TOE components are connected to distinct networks in a manner that ensures that the TOE traffic filtering security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.3.5 A.LOCAL_NETWORK_PROTECTION

Where the components of the TOE are connected to other trusted IT entities on a dedicated management local area network (such as connection to syslog and NTP servers), the connections are assumed to be physically secure and not to require any additional cryptographic protection to ensure the confidentiality of the communication between the TOE components.

4 Security Objectives

The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition.

There are two types of security objectives, those objectives met by the TOE itself and those that are met by the operational environment.

4.1 Security objectives for the TOE

The following subsections describe objectives for the TOE.

4.1.1 O.ADDRESS_FILTERING

To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, the TOE will implement Packet Filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) and/or receiving (destination) applicable network traffic as well as on established connection information.

SFR Rationale:

- FFW_RUL_EXT.1 specifies requirements to prevent unauthorized access to protected devices and services restricting the flow of network traffic between protected networks based on address filtering.

4.1.2 O.PORT_FILTERING

To further address the issues associated with unauthorized disclosure of information, etc., the TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.

SFR Rationale:

- FFW_RUL_EXT.1 specifies requirements to prevent unauthorized access to protected devices and services restricting the flow of network traffic between protected networks based on port filtering.
- FPT_STM.1 specified requirements to provide system time that can be used to filter traffic based on connection time information.

4.1.3 O.INTRUSION_PREVENTION

To further address the issues associated with attempts to exploit services running on machines that reside on a subnet protected by the TOE, the TOE will provide the means to identify and act upon malformed network traffic and network traffic matching predefined attack signatures and other known malicious sequences of activities.

SFR Rationale:

- FFW_RUL_EXT.1 specifies requirements to prevent unauthorized access to protected devices and services restricting the flow of network traffic between protected networks based on malformed packets.
- IPS_ANL_EXT.1 and IPS_RCT_EXT.1 specify requirements to detect and prevent the onward transmission of network traffic matching predefined attack sequences.

4.1.4 O.TOE_ADMINISTRATION

In order to configure the security features and administer the device, the TOE will provide the functions necessary for an administrator to securely manage the TOE. The TOE will protect management data communicated between TOE components, and between the administrator and the TOE components.

SFR Rationale:

- FMT_SMR.1, FMT_SMF.1 specifies requirements to maintain administrator roles and assign users to that role, and to provide the relevant administration functionality.
- FTP_TRP.1, FPT_ITT.2 specifies protection of the TSF data between administrator and TOE components and between TOE components themselves.

4.1.5 O.AUTHENTICATION

The TOE will provide a means to identify and authenticate the user to ensure they are communicating with an authorized administrator. Any remote session established with a authenticated user will terminate after a predefined period of inactivity or when termination is initiated by the user.

SFR Rationale:

- FIA_UID.1, FIA_UAU.1 specify requirements to identify and authenticate administrators attempting to establish a session to the TOE, masking credentials entered.
- FIA_AFL.1 specifies requirements to limit the number of failed authentication attempts to prevent brute force password attacks.
- FTA_SSL.3, FTA_SSL.4 specify requirements to terminate administrator sessions after a defined period of inactivity or when termination is initiated by the administrator.

4.1.6 O.SYSTEM_MONITORING

The TOE must provide a means to generate and store an audit trail of security-related events.

SFR Rationale:

- FAU_GEN.1, FAU_GEN.2 specify requirements for the generation of audit events to record the occurrence of specified security relevant events.
- FAU_STG_EXT.1 specifies requirements for the storage of the audit events on the TOE and on an external log server.

- FPT_STM.1 specifies requirements for a time stamp to be provided by the TOE to record the time an event occurred in the audit record.

4.2 Security Objectives for the Operational Environment

The following subsections describe objectives for the Operational Environment.

4.2.1 OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment to TOE components.

Addresses: A.PHYSICAL_PROTECTION

4.2.2 OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the hardware components on which the TOE executes, other than those services necessary for the operation, administration and support of the TOE.

Addresses: A.LIMITED_FUNCTIONALITY

4.2.3 OE.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

Addresses: A.TRUSTED_ADMINSTRATOR

4.2.4 OE.CONNECTIONS

TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic of monitored networks.

Addresses: A.CONNECTIONS

4.2.5 OE.LOCAL_NETWORK

NTP and syslog servers are connected to the same dedicated management LAN as the Management Server appliance.

Addresses: A.LOCAL_NETWORK_PROTECTION

4.3 Security objectives rationale

The security objectives for the operational environment are mapped in Section 4.2 above. The rationale for the security objectives for the operational environment is trivial as each objective is the restatement of the single assumption to which it is mapped and all assumptions are mapped to exactly one security objective for the operational environment. Therefore, no further rationale of those objectives is necessary. Hence, this security objectives rationale addresses the security objectives for the TOE.

The rationale for the TOE security objectives contains two sections:

- a tracing that shows which TOE security objectives address which threats and OSPs;
- a set of justifications that shows that all threats and OSPs are effectively addressed by the TOE security objectives.

There are no OSPs for the TOE so these are not considered in the rationale for the TOE security objectives.

4.3.1 Security objectives rationale tracing

The mapping in the following table that shows which TOE security objectives address which threats.

	T.NETWORK_DISCLOSURE	T.NETWORK_ACCESS	T.MALICIOUS_TRAFFIC	T.UNAUTHORIZED_ADMIN_ACCESS	T.UNDETECTED_ACTIVITY
O.ADDRESS_FILTERING	X	X			
O.PORT_FILTERING	X	X			
O.INTRUSION_PREVENTION		X	X		
O.TOE_ADMINISTRATION				X	X
O.AUTHENTICATION				X	
O.SYSTEM_MONITORING					X

Table 8 Threats and assumptions tracing

As can be seen from the table above, the tracing is complete. Each threat maps to at least one objective for the TOE or operational environment; each assumption maps to at least on objective for the operational environment and there are no spurious objectives, that is there are no objectives that do not map to a threat or assumption.

4.3.2 Justification for the effectiveness of the security problem solution

This section demonstrates that each threat is effectively met by one security objective or a combination of objectives working together.

Threat	Rationale
T.NETWORK_DISCLOSURE An attacker may attempt to “map” a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.	By meeting the security objectives O.ADDRESS_FILTERING and O.PORT_FILTERING, the TOE is able to prevent the mapping of a protected subnet by effectively filtering ports and addresses.
T.NETWORK_ACCESS With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.	By meeting the security objectives O.ADDRESS_FILTERING and O.PORT_FILTERING, the TOE is able to control access to services on the protected network effectively filtering ports and addresses and enforcing stateful filtering of traffic flow. Furthermore, by meeting the security objective O.INTRUSION_PREVENTION, the TOE identifies and responds to signatures and sequences identifying malicious network activity.
T.MALICIOUS_TRAFFIC An attacker may attempt to send malformed packets or sequences of network packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash, to gain use of unauthorized services on the target machine or to gain unauthorized access to user data on the target machine.	By meeting the security objective O.INTRUSION_PREVENTION, the TOE identifies and responds to malformed network traffic and network traffic matching signatures and sequences identifying malicious network activity, thereby preventing loss of availability, access to services or data on the target machine.
T.UNAUTHORIZED_ADMIN_ACCESS An attacker may attempt to gain administrator access to the SGM by nefarious means such as masquerading as an administrator to the SGM.	By meeting the security objectives O.TOE_ADMINISTRATION and O.AUTHENTICATION the TOE is able to ensure that any administrator access is from genuine, authorized administrators with knowledge of the administrator authentication credentials.

Threat	Rationale
T.UNDETECTED_ACTIVITY An attacker may attempt to access, change, and/or modify the security functionality of the SGM without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.	By meeting the security objective O.TOE_ADMINISTRATION the TOE ensures that only authorized administrators can manage the TOE. In addition by meeting the security objective O.SYSTEM_MONITORING the TOE generates and stores an audit trail of security-related events which includes administrative access and use of security functions, which facilitates reviews of the audit data from the TOE to look for signs of any unauthorized activity.

Table 9 TOE threat prevention rationale

5 Extended Components Definition

5.1 Security Audit (FAU)

A new family is defined for the existing Security Audit class.

5.1.1 Protected Audit Event Storage (FAU_STG_EXT)

Family Behaviour

This family defines extends the requirements for audit storage on the TOE (as specified in the [CC] FAU_STG.1 family) by requiring the audit evidence also to be transmitted to an external server for storage.

Component Levelling

Management:

The following actions could be considered for the management functions in FMT:

a) None.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) No audit necessary.

5.1.1.1 Protected Audit Event Storage (FAU_STG_EXT.1)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3 The TSF shall [selection: *drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records*], [assignment: other action]] when the local storage space for audit data is full.

5.2 Intrusion Prevention System (IPS)

The Intrusion Prevention System class is modelled on the analysis and anomaly detection aspects of the [CC] FAU: Security Audit class. The IPS Analyser analysis (IPS_ANL_EXT) family is modelled on a combination of FAU_SAA.1 Potential violation analysis and the first

component of FAU_SAA.2 Profile based anomaly detection. The IPS Analyser React (IPS_RCT_EXT) family is modelled on FAU_ARP.1 Security alarms.

5.2.1 IPS Analyser analysis (IPS_ANL_EXT)

Family Behaviour

This family defines requirements for automated means that analyse network traffic received by the TOE looking for possible or real security violations. This analysis may work in support of automatic response to a potential security violation.

Component Levelling

Management:

The following actions could be considered for the management functions in FMT:

a) The ability to configure the analyser reactions (addition, removal, or modification) of actions.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms;

5.2.1.1 IPS Analyser analysis (IPS_ANL_EXT.1)

Hierarchical to: No other components

Dependencies: None.

IPS_ANL_EXT.1.1 The TSF shall be able to apply a set of rules in analysing all network traffic received and based upon these rules indicate a potential violation of the enforcement of the SFRs.

Application Note:

The set of rules shall be applied by a pattern matching engine.

IPS_ANL_EXT.1.2 The TSF shall be able to apply database of attack signatures represent the patterns of network intrusion attempts.

Application Note:

A database of signatures is used by the pattern matching engine to identify network intrusions.

IPS_ANL_EXT.1.3 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [assignment: *additional information to be recorded*].

5.2.2 IPS Analyser React (IPS_RCT_EXT)

Family Behaviour

This family defines the response to be taken in case of detected intrusions.

Component Levelling

Management:

The following actions could be considered for the management functions in FMT:

a) The ability to configure the analyser reactions (addition, removal, or modification) of actions.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) None.

5.2.2.1 IPS_RCT_EXT.1 IPS Analyser React

Hierarchical to: No other components

Dependencies: None.

IPS_RCT_EXT.1.1 The TSF shall take [assignment: *list of actions*] when an intrusion is detected.

5.3 Firewall (FFW)

The Firewall class is taken from collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+ Errata 20180314, 14 March 2018. This class defines the requirements for filtering of network traffic to be performed by a network device (such as a firewall).

5.3.1 Stateful Traffic Filtering (FFW_RUL_EXT)

Family Behaviour

This requirement is used to specify the behaviour of a Stateful Traffic Filter Firewall. The network protocols that the TOE can filter, as well as the attributes that can be used by an administrator to construct a rule set are identified in this component. How the rule set is processed (i.e., ordering) is specified, as well as any expected default behaviour on the part of the TOE.

Component Levelling

Management:

The following actions could be considered for the management functions in FMT:

a) enable/disable a rule set on a network interface
b) configure a rule set
c) specifying rules that govern the use of resources.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal:
    - Result (i.e., drop, allow) of applying a rule in the rule set to a network packet;
    - Configuration of the rule set;
    - Indication of packets dropped due to too much network traffic.

5.3.1.1 Stateful Traffic Filtering (FFW_RUL_EXT.1)

Hierarchical to: No other components

Dependencies: None.

FFW_RUL_EXT.1.1 The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

FFW_RUL_EXT.1.2 The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields: [assignment: *list of attributes supported by the rule set*].

FFW_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: permit, deny, and log.

FFW_RUL_EXT.1.4 The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.

FFW_RUL_EXT.1.5 The TSF shall:

a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: [assignment: *list of supported protocols for which state is maintained*] based on the following network packet attributes [assignment: *list of attributes associated with each of the protocols*].:
b) Remove existing traffic flows from the set of established traffic flows based on the following: [selection: *session inactivity timeout, completion of the expected information flow*].

FFW_RUL_EXT.1.6 The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic: [assignment: *list of default rules that are applied to network traffic flow*].

FFW_RUL_EXT.1.7 The TSF shall be capable of dropping and logging according to the following rules: [assignment: *list of specific rules that the TOE is capable of enforcing*].

FFW_RUL_EXT.1.8 The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.

FFW_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FFW_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [assignment: *rules governing the use of resources*].

5.4 Extended Components Rationale

The extended classes defined above were included to reflect the modelling of firewall filtering and intrusion prevention functionality, which are not readily captured by the existing CC Part 2 components. In addition, the extended family for the Security Audit class (FAU) has been defined to readily capture the storage of audit records on the TOE and also on an external IT entity (as also used in some collaborative Protection Profiles).

6 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

This security Target is for an EAL4 evaluation augmented by ALC_FLR.1 – Basic Flaw remediation and by reference this document contains all of the SARs that are relevant to the EAL4 package.

6.1 TOE Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1 Audit Data Generation
	FAU_GEN.2 User Identity Association
	FAU_STG_EXT.1 Protected Audit Event Storage
FFW: Stateful Traffic Filtering Firewall	FFW_RUL_EXT.1 Stateful Traffic Filtering
IPS: Intrusion Prevention System	IPS_ANL_EXT.1 IPS Analyser analysis
	IPS_RCT_EXT.1 Analyser React
FIA: Identification and authentication	FIA_UID.1 Timing of Identification
	FIA_UAU.1 Timing of authentication
	FIA_AFL.1 Authentication Failure Management
FMT: Security management	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security Roles
FTA: TOE access	FTA_SSL.3 TSF-initiated Termination
	FTA_SSL.4 User-initiated Termination
FPT: Protection of the TSF	FPT_STM.1 Reliable time stamps
	FPT_ICT.1 Inter-TSF confidentiality during transmission

Table 10 TOE Security Functional Requirements

6.1.1 Security audit (FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [All administrative actions comprising:

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Security Management Server and Orchestrator administrators).*
- *Changes to TSF data related to traffic filtering policy and Security Group configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Resetting passwords (name of related user account shall be logged).*
- *no other actions;*

d) *Specifically defined auditable events listed in Table 11.]*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of Table 11*].

Requirement	Auditable Events	Additional Audit Record Contents	TOE component generating audit record
FAU_GEN.1	Start-up and shut-down of the audit functions	None.	SGM Management Server (Orchestrator when in SP deployment)
FAU_GEN.2	None.	None.	n/a
FAU_STG_EXT.1	None.	None.	n/a
FFW_RUL_EXT.1	Result: Application of rules configured with the ‘log’ operation	Source and destination addresses Source and destination ports	SGM

Requirement	Auditable Events	Additional Audit Record Contents	TOE component generating audit record
		TOE Interface	
IPS_ANL_EXT.1	Enabling and disabling of IPS blade	None.	SGM
IPS_RCT_EXT.1	None	None.	n/a
FIA_UID.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	Management Server (Orchestrator when in SP deployment)
FIA_UAU.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	Management Server (Orchestrator when in SP deployment)
FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).	Management Server (Orchestrator when in SP deployment)
FMT_SMF.1	Administrator action performed.	None.	Management Server (Orchestrator when in SP deployment)
FMT_SMR.1	None.	None.	n/a
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	Management Serve (Orchestrator when in SP deployment)
FTA_SSL.4	The termination of an interactive session.	None.	Management Server (Orchestrator when in SP deployment)
FPT_STM.1	None	None	n/a
FPT_ITT.2	None	None	n/a

Table 11 Security Functional Requirements and Auditable Events

6.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule*: [audit is stored in a circular buffer and oldest records are overwritten first]*] when the local storage space for audit data is full.

6.1.2 Stateful Traffic Filtering Firewall (FFW)

6.1.2.1 FFW_RUL_EXT.1 Stateful Traffic Filtering

FFW_RUL_EXT.1.1 The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

FFW_RUL_EXT.1.2 The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields:

- [*ICMPv4*
  - *Type*
  - *Code*
- *IPv4*
  - *Source address*
  - *Destination Address*
  - *Transport Layer Protocol*
- *TCP*
  - *Source Port*
  - *Destination Port*
- *UDP*
  - *Source Port*
  - *Destination Port*]

and distinct interface.

FFW_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules: permit, deny, and log.

FFW_RUL_EXT.1.4 The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.

FFW_RUL_EXT.1.5 The TSF shall:

a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols: [*TCP, UDP*] based on the following network packet attributes:

1. [*TCP: source and destination addresses, source and destination ports, sequence number, Flags;*
2. *UDP: source and destination addresses, source and destination ports*].

b) Remove existing traffic flows from the set of established traffic flows based on the following: [session inactivity timeout].

FFW_RUL_EXT.1.6 The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic:

a) [*The TSF shall drop and be capable of logging packets which are invalid fragments;*

b) The TSF shall drop and be capable of logging fragmented packets which cannot be re-assembled completely;

c) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a broadcast network;

d) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a multicast network; The TSF shall drop and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;

e) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address "reserved for future use" (i.e. 240.0.0.0/4) as specified in RFC 5735 for Ipv4;

f) *The TSF shall drop and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified*].

FFW_RUL_EXT.1.7 The TSF shall be capable of dropping and logging according to the following rules:

a) [*The TSF shall drop and be capable of logging network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;*

b) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is a link-local address;

c) The TSF shall drop and be capable of logging network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received].

FFW_RUL_EXT.1.8 The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.

FFW_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FFW_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [*counted*].

6.1.3 Intrusion Prevention System (IPS)

6.1.3.1 IPS_ANL_EXT.1 IPS Analyser analysis

IPS_ANL_EXT.1.1 The TSF shall be able to apply a set of rules in analysing all network traffic received and based upon these rules indicate a potential violation of the enforcement of the SFRs.

IPS_ANL_EXT.1.2 The TSF shall be able to apply database of attack signatures represent the patterns of network intrusion attempts.

Application Note:

The TSF shall be able to maintain an internal representation of attack signature events and event sequences of known intrusion scenarios, encoded as IPS protections enabled by an Security Management Server administrator, and to compare the signature events and event sequences against the record of system activity discernible from an examination of the network traffic mediated by the TOE;

IPS_ANL_EXT.1.3 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [*none*].

6.1.3.2 IPS_RCT_EXT.1 Analyser React

IPS_RCT_EXT.1.1 The TSF shall take [*actions as configured by a Security Management Server administrator which can be one of:*

a) *Log the suspected traffic and allow it to pass;*

b) *Silently drop the suspected traffic;*

c) Log and drop the suspected traffic;

d) *Reject the suspected traffic;*

e) *Log and reject the suspected traffic*]

when an intrusion is detected.

6.1.4 Identification and authentication (FIA)

6.1.4.1 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow [*None*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.2 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [*identification as stated in FIA_UID.1*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

1. FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when [*3*] unsuccessful authentication attempts occur related to [*Administrators attempting to authenticate remotely*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*prevent the offending remote Administrator from successfully authenticating until 30 minutes have elapsed*].

Application Note:

This requirement applies to both Security Management Server administrator and Orchestrator administrator roles.

6.1.5 Security Management (FMT)

6.1.5.1 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*Security Management Server Administrator, and (when in SP deployment) Orchestrator Administrator*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

[*On Security Management Server:*

- *Ability to create, delete, modify Security Management Server administrator accounts;*
- *Ability to configure the Management API session inactivity time before session termination;*
- *Ability to manually update (import) Threat Protection signatures*
- *Ability to configure firewall rules, including:*
  - *enable/disable a rule set on a network interface*
  - *configure a rule set*
  - specifying rules that govern the use of resources
- *Ability to configure IPS rules, including:*
  - *configure the analyser reactions configure actions to be taken when signature matches are detected;*
  - *management (addition, removal, or modification) of actions*
- *Ability to configure trusted path between Security Management Server administrator and Security Management Server (TLS between Security Management Server and Administrator PC);*

- *Ability to configure secure channels between TOE components (SIC and VLAN protection between Security Management Server and SGMs, and between SGMs);*

[*and (when in SP deployment) on Orchestrator appliances:*

- *Ability configure objects and Security Groups;*
- *Ability to create, delete, modify Orchestrator administrator accounts;*
- *Ability to configure Orchestrator administrator session inactivity time before session termination;*
- *Ability to configure trusted path between Orchestrator administrator and Orchestrator (TLS between Orchestrator and MHO Administrator PC)*].

Application Note:

The trusted channels between TOE components and the following trusted paths between administrators and TOE components can only be configured during the initial installation of the TOE:

- Security Management Server Administrator and the Security Management Server,
- Orchestrator Administrator and Orchestrator appliance.

6.1.6 TOE access (FTA)

6.1.6.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after a [*Security Management Server Administrator-configurable time interval of session inactivity, and (when in SP deployment) Orchestrator administrator-configuration time interval*].

6.1.6.2 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

Application Note:

This requirement applies to both Security Management Server administrator and Orchestrator administrator roles.

6.1.7 Protection of the TSF (FPT)

6.1.7.1 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.7.2 TSF data transfer separation

FPT_ITT.2.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

FPT_ITT.2.2 The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

6.1.7.3 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication, [*transfer of TSF management data*]].

6.2 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 4 components as specified in Part 3 of the Common Criteria. The EAL4 assurance components have been augmented with the addition of ALC_FLR.1.

Assurance class	Assurance components
Class ADV: Development	ADV_FSP.4 Complete functional specification
	ADV_ARC.1 Security architecture description
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ALC: Life Cycle Support	ALC_CMS.4 Problem tracking CM coverage
	ALC_FLR.1 Basic flaw remediation
	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition

Assurance class	Assurance components
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis

Table 12 EAL 4 Assurance Components

6.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL4 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

6.3 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

6.3.1 Security Functional Requirements for the TOE

A mapping and rationale of the SFRs meeting each security objective for the TOE is provided in Section 4.1 above.

6.3.2 Security Functional Requirements Dependency Rationale

The following table shows that all SFR dependencies are met by the TSF.

Requirement Component	Dependency	Notes
FAU_GEN.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	
FAU_STG_EXT.1	FAU_GEN.1	
FFW_RUL_EXT.1	None	
IPS_ANL_EXT.1	None	
IPS_RCT_EXT.1	IPS_ANL_EXT.1	
FIA_UID.1	None	
FIA_UAU.1	FIA_UID.1	
FIA_AFL.1	FIA_UAU.1	
FMT_SMR.1	FIA_UID.1	
FMT_SMF.1	None	
FTA_SSL.3:	None	
FTA_SSL.4:	None	
FPT_STM.1	None	
FPT_ITT.2	None	
FPT_TRP.1	None	

Table 13 SFR Dependencies

7 TOE Summary Specification

This chapter describes the security functions provided by the TOE:

- Security audit
- Packet filtering and stateful traffic filtering firewall
- Intrusion Prevention Systems
- Identification and authentication
- Security management
- TOE access
- Protection of the TSF

7.1 Security audit

The SGM and Management Server generate audit logs of security events (see Table 11).

GAiA generates OS-related security events on both the SGM and the Management Server. The SGM kernel is responsible for generating the traffic logs and a Security Management process is responsible for generating security management audit logs (these are the logs relating to all Security Management Server administrator activities on the Management Server).

The SGM sends its traffic logs to the Management Server and sends its OS (GAiA) logs to the external syslog server. In the event of failure, e.g. loss of power on the SGM, queued audit records that have not been successfully transmitted to the log server may be lost. The maximum number of records that may be lost is equal to the queue size: 4096 records.

The Management Server sends to the external syslog server the security management audit logs, its own OS (GAiA) logs and the traffic logs received from the SGM.

The Management Server has a disk cleanup procedure where it removes old audit logs to allow space for new ones. This is configurable by the Security Management Server administrator. The Management Server also has the ability to prevent new connections if the Management Server runs out of space for new audit logs.

When disk space on the Management Server falls below a predefined threshold, the server stops collecting audit records. As explained above, SGMs will queue the records, and eventually start logging them to the local disk, until connectivity is resumed.

When in SP deployment, Orchestrator generates audit logs of security events (see Table 11).

GAiA generates OS-related security events on Orchestrator, while the Orchestrator kernel is responsible for generating security management audit logs (these are the logs relating to the Orchestrator administrator activities on Orchestrator).

Orchestrator sends to the external syslog server the security management audit logs and the OS (GAiA) logs. Orchestrator has a disk cleanup procedure where it removes old audit

logs to allow space for new ones. This is configurable by the Orchestrator administrator. Orchestrator also has the ability to prevent new connections if the Orchestrator runs out of space for new audit logs.

When disk space on Orchestrator falls below a predefined threshold, Orchestrator stops collecting audit records.

It should be noted that events indicating the start-up and shutdown of auditing are generated by GAiA for both the SGM and the Management Server, and when in SP deployment also for Orchestrator.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE is able to generate logs for the required range of events. Each event log is unique with the date/time of the event, type of event, subject identity (e.g. IP address), and the outcome of the event
- FAU_GEN.2: The TOE is able to identify each auditable event with specific IP addresses and the TOE's interfaces and SGMs
- FAU_STG_EXT.1: The TOE is able to send audit log data to an external log server.
- FPT_STM.1: The TOE provides timestamps for use in audit records.

7.2 Packet Filtering and Stateful Traffic Filtering Firewall

If the TOE is configured as a Scalable Platform the Orchestrator appliance(s) will distribute the traffic to the appropriate SGM according to the distribution algorithm on the Orchestrator appliance. (This all happens within the TOE environment, before the traffic is forwarded to the TOE. No traffic inspection is performed by the Orchestrator appliance.)

Every IPv4 packet received by the Check Point Security SGM is intercepted by the firewall kernel. Fragmented packets are first reassembled. IPv4 packets with unauthorized IP options (e.g. source route option) are dropped.

When an IP packet is received on a network interface, its source address is compared to topology information configured by the Security Management Server administrator. If the source address does not correspond to the set of network addresses that match the given network interface, the packet is dropped as a spoofed packet. Note that broadcast and loopback addresses are never considered valid source addresses and are therefore rejected.

The packet header attributes are used to match the packet against state tables that contain accepted 'connections'.

For all other packets, inspection is performed against the firewall rules. The rules have 4 possible outcomes:

1. Accept - the packet is allowed through;
2. Drop – the packet is dropped without notification to the sender;
3. Reject – the packet is dropped and the presumed sender is notified.
4. If no rule is matched, packets are dropped.

Firewall rules can be set to filter on protocol, source address, destination address, source port, destination port, ICMP type or ICMP code. All protocols including ICMPv4, IPv4, TCP, and UDP may be used in firewall rules. If any interface is overwhelmed with traffic, it will drop the packets and will increase the counter of any half open connections.

The firewall will drop all of the following types of packet:

1. Packets which are invalid fragments, including a description of what constitutes an invalid fragment
2. Fragments that cannot be completely re-assembled
3. Packets where the source address is equal to the address of the network interface where the network packet was received
4. Packets where the source address does not belong to the networks associated with the network interface where the network packet was received, including a description of how the TOE determines whether a source address belongs to a network associated with a given network interface
5. Packets where the source address is defined as being on a broadcast network
6. Packets where the source address is defined as being on a multicast network
7. Packets where the source address is defined as being a loopback address
8. Packets where the source address is defined as being a reserved address as specified in RFC 1918 for IPv4
9. Packets where the source or destination address of the network packet is a link-local address
10. Packets where the source or destination address of the network packet is defined as being an address 'reserved for future use' as specified in RFC 5735 for IPv4
11. Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified

During the Check Point SGM boot process, there is a lag between the time when the network interface is operational, and the time that the Stateful Traffic Filtering functionality is fully functioning. During this time, Boot Security is enforced:

- Traffic flow through the SGM is disabled; and
- Traffic to and from the SGM is controlled by a Default Filter that drops all external traffic to the SGM

The Stateful Traffic Filtering Firewall function is designed to satisfy the following security functional requirements:

- FFW_RUL_EXT.1: The TOE supports all of the required protocols, which include ICMPv4 (RFC 792), IPv4 (RFC 791), TCP (RFC 793), and UDP (RFC 768). Conformance with the RFCs defining these protocols is asserted by the Check Point based upon the Check Point’s implementation and design The firewall rules implement the SPD rules (permit, deny, bypass).

7.3 Intrusion Prevention Systems

Network traffic that passes through the firewall and IPS security policies is compared with signatures encoded as regular expressions, keywords, and INSPECT language code. The signatures database can be manually updated by the Security Management Server administrator.

INSPECT is a Check Point script language that specifies packet handling by evaluating packet content and state. INSPECT scripts are compiled by a Security Management Server into low-level inspection code that is executed on SGMs using a stack-based virtual machine.

An INSPECT script applies a conditioned sequence of pattern matching operations on packets flowing through the SGM. An INSPECT operator can be used to enforce an information flow control decision to permit or deny the flow and generate log records. The operator can read and modify state information encoded in transient registers and in persistent state tables.

INSPECT operators can be configured to modify state tables in the incoming packets. Pattern matching on incoming packets is a function of state table information. So signature protections can be configured to detect both simple single-packet and complex multi-packet events that may indicate an attempt to violate the Security Requirements (SFRs). Compound Signature Identification (CSI) supports matching sequences of events.

Encoded signature protections can be set to log the detected potential violation. Check Point SGM record within each analytical result (manifested as a match against an IPS protection) the following information required by IPS_ANL_EXT.1:

- The date and time of the result.
- The type of result.
- Identification of the data source (IP address, port and protocol).

Incoming network traffic is matched against a combined set of protocol enforcement and pattern matching logic that identifies suspicious traffic and assigns security attributes:

- Confidence Level (that the traffic contains an attack)
- Severity (the potential impact of the attack on protected resources)

Based on these attributes and on Security Management Server administrator-specified security policy settings, the IPS engine may take action by generating applicable log records (Detect) and optionally blocking the traffic (Prevent).

IPS engine logic consists of the following layers:

- Passive Streaming Library (PSL) – an in-kernel TCP stack that assembles IP packets into information streams for protocol parsers.
- Protocol Parsers – implement protocol-specific state machines that enforce protocol compliance and detect protocol anomalies that may be indicative of an intrusion attempt. The protocol parsers extract protocol ‘contexts’ from the information streams. A context is a well-defined part of the protocol on which further security analysis can be

performed, e.g. a HTTP URL, HTTP headers, an HTTP response, etc. The HyperSPECT feature provides performance optimization for the processing of rules involving the body of HTTP packets.

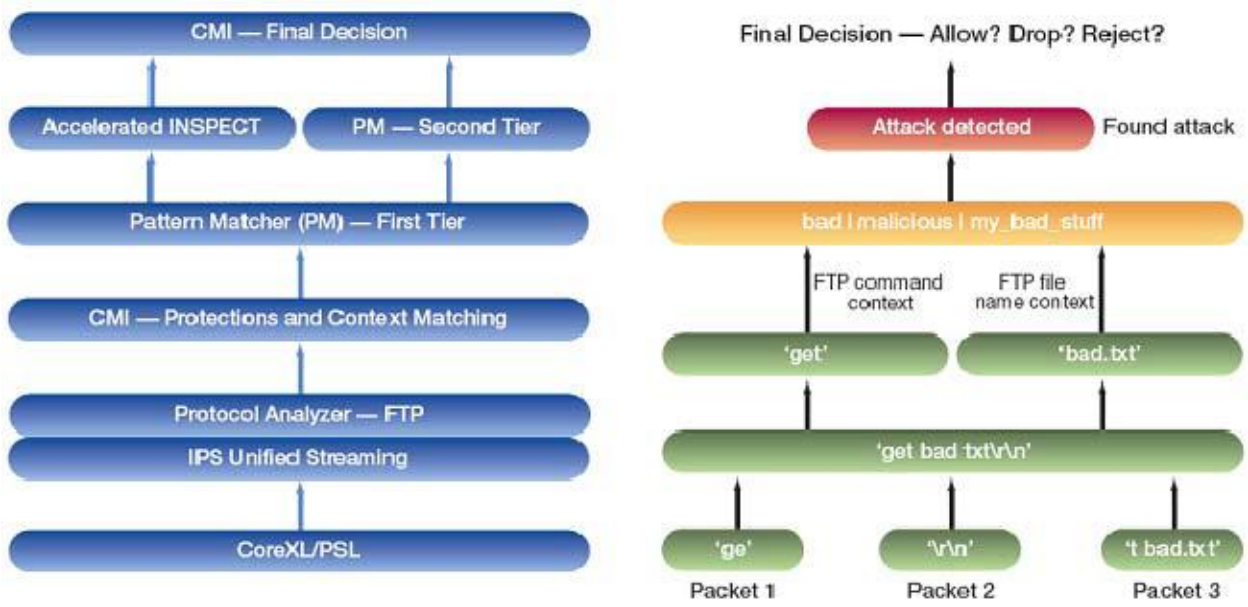
- Context Management Interface – coordinates application of protections defined in the security policy on contexts established by protocol parsers. The contexts created by the parsers are sent to the relevant applications for inspection.
- Pattern Matcher – a two-tier pattern matching engine that matches information streams against IPS protection signatures. The first tier applies simple matching criteria that separate clearly harmless traffic from the rest. Traffic not matched by the first tier is inspected by the second tier, which performs deeper inspection through the use of regular expression signatures or execution of INSPECTv2 signature matching programs for identifying suspicious activity.
- Compound Signature Identification (CSI) – matches complex signatures that are triggered when a defined logical condition over multiple contexts is matched. The logical expression can use AND, OR, NOT and ORDERED-AND to construct its logic. An example of CSI use is a CAPICOM protection which looks for one of three signatures.

IPS signatures updates may be imported manually into the TOE by a Security Management Server administrator.

Updates are installed as regular expressions, keywords, and INSPECTv2 code fragments.

The figure depicts an example IPS signature match for the FTP protocol. The left side of the figure depicts the IPS engine logic layers described above. The right side shows the incoming IP packets (on the bottom right of the figure) and the processing performed by the different logic layers, depicted from the bottom of the figure upwards.

In the example, the attacker attempts to access an unauthorized file (‘bad.txt’) using a FTP ‘get’ command. The attacker attempts to obfuscate the attack by fragmenting the command over three IP packets, reordering them so that the ‘get’ command must be reconstructed from the first and third packets. The PSL layer (bottom left) converts the IP packets received by the SGM into protocol streams that are examined by the FTP protocol analyzer, extracting two contexts: command and file name. The Pattern Matcher matches a protection signature and signals a signature match to allow the SGM to take appropriate action (Allow, Drop, or Reject) and possibly capture packets for future investigation.



Encoded signature protections can be set to log the detected potential violation. The TOE records within each analytical result (manifested as a match against an IPS protection) the following information required: date and time of the result, type of result, and identification of the data source (IP address, port and protocol).

The Intrusion Prevention Systems function is designed to satisfy the following security functional requirements:

- IPS_ANL_EXT.1: The TOE supports signature-based detection and generates a record of detected anomalies.
- IPS_RCT_EXT.1: The TOE can be configured to perform logging and or blocking (drop or reject) actions if an intrusion is detected.
- FPT_STM.1: The TOE provides a clock for use in traffic analysis rules that relate to date/time.

7.4 Identification and authentication

The TOE provides a password mechanism for authenticating users to the Management Server. Users are associated with a username, password, and one or more roles. Users may authenticate to the Management Server locally or via the web interface. Passwords can be composed of any alphabetic, numeric, and a wide range of special characters. Internally the TOE keeps track of failed login attempts. If a Security Management Server administrator fails 3 consecutive attempts, the administrator is locked out for 30 minutes.

The TOE requires identification and authentication before allowing access to the Management Server. Only the banner may be presented before authentication is complete.

When in SP deployment, the TOE provides a password mechanism for authenticating users to Orchestrator via the WebUI. Users are associated with a username and password. Passwords can be composed of any alphabetic, numeric, and a wide range of special characters. Internally the TOE keeps track of failed login attempts. If an Orchestrator administrator fails 3 consecutive attempts, the administrator is locked out for 30 minutes.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_UID.1: The TOE's identification and authentication mechanism employs a locally stored database of identification data.
- FIA_UAU.1: The TOE's identification and authentication mechanism employs a locally stored database of authentication data.
- FIA_AFL.1: The TOE supports the capability to lock an account for 30 minutes.

7.5 Security management

User accounts on the Management Server are associated with the profile "read write all". User accounts associated with this profile are called Security Management Server administrators.

Once authenticated, Security Management Server administrators have access to the following security functions on the Management Server:

- Ability to create, delete, modify Security Management Server administrator accounts;
- Ability to configure the Management API session inactivity time before session termination;
- Ability to manually update (import) Threat Protection signatures;
- Ability to configure firewall rules, including:
  - *enable/disable a rule set on a network interface*
  - *configure a rule set*
  - specifying rules that govern the use of resources
- Ability to configure IPS rules, including:
  - configure the analyser reactions configure actions to be taken when signature matches are detected;
  - management (addition, removal, or modification) of actions
- Ability to configure trusted path between Security Management Server administrator and Security Management Server (TLS between Security Management Server and Administrator PC);
- Ability to configure secure channels between TOE components (SIC and VLAN protection between Security Management Server and SGMs, and between SGMs).

The TOE offers two administrative interfaces to the Management Server:

- CLI: The command line interface is a text based interface that is accessible via a directly connected console. These command line functions can be used to effectively perform most administrative activities, but it is most typically used during initial installation of the TOE.
- Management API: The Management API is a REST interface that can be used to manage objects, policies, rules and administrative functionality. This API is defined at https://sc1.checkpoint.com/documents/latest/APIs/#web. Typically, most Security Management Server administrators use the API interface for management.

When is Scalable Platform deployment the management of the Orchestrator appliances is performed through the Orchestrator WebUI. There is a single type of administrator account on Orchestrator, although multiple users can be defined to performed management activities on the Orchestrator appliance.

Once authenticated, Orchestrator administrators have access to the following security functions on the Orchestrator appliance:

- Ability configure objects and Security Groups;
- Ability to create, delete, modify Orchestrator administrator accounts;
- Ability to configure administrator session inactivity time before session termination;
- Ability to configure trusted path between an Orchestrator administrator and Orchestrator (TLS between Orchestrator and MHO Administration PC)

The TOE offers two administrative interfaces to the Orchestrator appliance:

- CLI: The command line interface is a text based interface that is accessible via SSH. These command line functions can be used to effectively perform most administrative activities, but it is most typically used during initial installation of the TOE.
- WebUI: The WebUI is a browser based interface that can be used to manage objects, Security Groups and administrative functionality. This WebUI is defined at by the Maestro R81.10 Getting Started Guide and the Maestro R81.10 Administration Guide.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified above.
- FMT_SMR.1: The TOE supports Security Management Server administrator and Orchestrator administrator roles. The single administrator profile “read write all” is supported in the evaluated configuration. A Security Management Server administrator can login to the Security Management Server locally or remotely. A single Orchestrator administrator profile is supported on the Orchestrator appliance, and Orchestrator administrators can log in local or remotely to the Orchestrator appliance.

7.6 TOE access

The TOE provides an inactivity timeout for Check Point REST API sessions to the Management Server and (when in SP deployment) to Orchestrator. The (Security

Management Server and Orchestrator) administrator can set the inactivity timeout. When an inactivity period is exceeded, the session is terminated. The user will be required to login in after any session has been terminated due to inactivity or after voluntary termination.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE allows inactive sessions to disconnect after a set period of time configurable in the GUI.
- FTA_SSL.4: The TOE allows session disconnect via a logout command.

7.7 Protection of the TSF

Each TOE component (SGM, Security Management Server and (when in SP deployment) Orchestrator) provides a system clock. During installation the TOE is configured to synchronize its clock with a time server. The TOE uses the clock to support several security functions including timestamps for audit records, triggering time-based firewall rules, recording when potential violations have been detected, and inactivity timeouts.

All TSF data transmitted between TOE components (SGM, Security Management Server and (when in SP deployment) Orchestrator) is communicated using the proprietary SIC protocol to protect the integrity and confidentiality of the transmitted data. VLANs are used to separate the TSF data from user data transmitted over the same physical network connections.

All TSF data transmitted between the administrators, both Security Management Server and Orchestrator in Scalable deployment, is protected using TLS v1.3. The administrators have to connect to the management ports of the Security Management Server and Orchestrator (respectively) from the internal network, and the browsers on the workstations must be configured to only support TLS v1.3.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_STM.1: The TOE provides reliable time stamps using an internal clock maintained by the OS, which is synchronized with the NTP service provide on the Management LAN (as configured during installation).
- FPT_ITT.2: SIC is used to encrypt the management traffic between TOE components to protect it from modification and disclosure. When in SP deployment, the TSF data transmitted between TOE components (Gateways and Management Server, meditated by Orchestrator appliances) will be protected using VLANs to separate management traffic from user data.
- FPT_TRP.1: The TSF data transmitted on internal networks between the Security Management Server administrator and Security Management Server (and when in SP deployment between the Orchestrator administrator and Orchestrator) will be protected from modification and disclosure using TLS.

