REF: 2014-41-INF-1393 v1	Created by: CERT9
Target: Expediente	Revised by: CALIDAD
Date: 10.12.2014	Approved by: TECNICO

CERTIFICATION REPORT

File: 2014-41 Cyberoam Firmware v10.5.4

Applicant: U72900GJ19 Cyberoam Technologies

References:

[EXT 2596] Certification request of Cyberoam Firmware v10.5.4

[EXT 2623] Evaluation Technical Report of Cyberoam Firmware v10.5.4.

The product documentation referenced in the above documents.

Certification report of the product Cyberoam Firmware, as requested in [EXT 2596] dated 28-08-2014, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT2623] received on 08/10/2014.

TABLE OF CONTENTS

EXECUTIVE SUMMARY ... **3**

TOE SUMMARY ... 4
SECURITY ASSURANCE REQUIREMENTS ... 8
SECURITY FUNCTIONAL REQUIREMENTS ... 9

IDENTIFICATION ... **9**

SECURITY POLICIES ... **10**

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT ... **10**

CLARIFICATIONS ON NON-COVERED THREATS ... 10
OPERATIONAL ENVIRONMENT FUNCTIONALITY ... 11

ARCHITECTURE ... **11**

DOCUMENTS ... **13**

PRODUCT TESTING ... **13**

EVALUATED CONFIGURATION ... **14**

EVALUATION RESULTS ... **15**

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM ... **15**

CERTIFIER RECOMMENDATIONS ... **15**

GLOSSARY ... **15**

BIBLIOGRAPHY ... **16**

SECURITY TARGET ... **16**

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Cyberoam Firmware.

Cyberoam UTM delivers enterprise-class network security with stateful inspection firewall, virtual private network (VPN), Intrusion Prevention System (IPS), and host of other security features, offering the Human Layer 8 identity-based controls and Layer 7 application controls. It ensures high levels of network security, network connectivity, continuous availability and secure remote access with controlled network access to road warriors, telecommuters, partners, customers.

Current corporate policies surrounding network security often neglect the most critical and weak security component: the human element. Cyberoam UTM's Layer 8 Technology treats user identity as the 8th layer or the “human layer” in the network protocol stack. This allows administrators to uniquely identify users, control the Internet activity of these users in the network, and enable policy-setting and reporting by username.

Cyberoam Unified Threat Management appliances offer multiple features integrated in a single appliance to offer a complete balance of security, connectivity, and productivity to organizations, ranging from large enterprises to small and branch offices. The Layer 8 technology penetrates through each and every security module of the Cyberoam UTM. All security features can be centrally configured and managed from a single firewall page with complete ease. Layer 8 binds security features to create a single, consolidated security unit and enables the administrator to change security policies dynamically while accounting for user movement - joiner, leaver, rise in hierarchy etc.

With granular controls and advanced networking features, Cyberoam UTM offers enterprise-class security and high flexibility with protection against blended threats, malware, Trojans, denial of service (DoS), distributed denial of service (DDoS), IP spoofing attacks, spam, intrusions and data leakage. Cyberoam can be managed through the Web Admin Console, CLI, or SNMP agent.

Developer/manufacturer:
Cyberoam Technologies Pvt. Ltd.
901, Silicon Tower
Ahmedabad 380 006
India

Documentary evidences developed by:
Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033

USA.

Sponsor:

Cyberoam Technologies Pvt. Ltd.
901, Silicon Tower
Ahmedabad 380 006

India

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF:Epoche & Espri S.L.U..

Protection Profile: None

Evaluation Level: EAL4 + ALC_FLR.2

Evaluation end date: 8th October 2014.

All the assurance components required by the evaluation level EAL4+ augmented with Flaw Remediation ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4+ augmented with Flaw Remediation ALC_FLR.2, as defined by the Common Criteria v 3.1 (CC_P1, CC_P2, CC_P3) and the CEM.

Considering the obtained evidences during the instruction of the certification request of the product Cyberoam Firmware v10.5.4, a positive resolution is proposed.

TOE SUMMARY

The TOE is the firmware that runs on the Cyberoam series hardware and virtual appliances. The TOE is installed on a network whenever firewall services are required, as depicted in Figure 1 and Figure 2 below. The TOE can be deployed in Gateway or Bridge mode in both configurations. This allows the TOE to be used as a firewall; as well as a gateway for routing traffic. To control Internet access entirely through the TOE, the entire Internet bound traffic from the local area network (LAN) network must first pass through the TOE. The TOE is software-only with the Cyberoam hardware or virtual appliance as part of the TOE environment.

The firewall rules functionality protects the network from unauthorized access and typically guards the LAN and DMZ networks against malicious access. Firewalls rules may also be configured to limit the access to harmful sites for LAN users.

Firewall rules provide centralized management of security policies. From a single firewall rule, you can define and manage an entire set of TOE security policies. Firewall rules control traffic passing through the TOE. Depending on the instruction in the rule, the TOE decides on how to process the access request. When the TOE receives the request, it checks for the source address, destination address, TCP or UDP protocol, and port number and tries to match it with the firewall rule. It also keeps track of the state of connection and denies any traffic that is not part of the connection state.

The TOE provides extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse. These logs can be viewed through the Web Admin Console.

The TOE also provides the following management functionalities:

- System administration and configuration;
- Firewall rules management;
- Configure user authentication ;
- Users management;
- Management of the following Traffic Information Flow Control SFP security attributes:
  - Subject IP address
  - Traffic Source IP address
  - Traffic Destination IP address
  - Traffic TCP or UDP transport protocols
  - Traffic port number

Figure 1 and Figure 2 shows the details of the deployment configurations of the TOE:

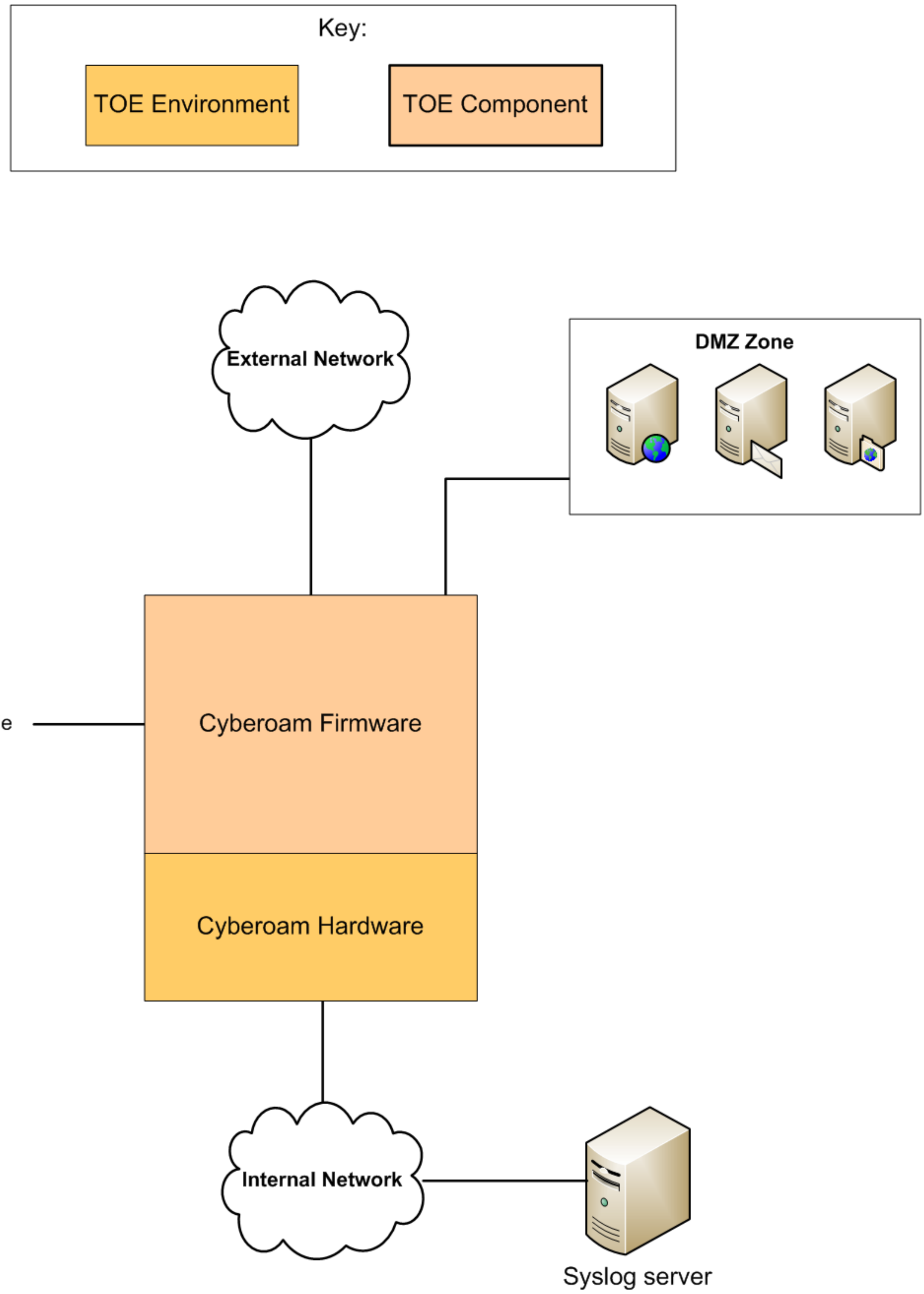


Figure 1 – Hardware Deployment Configuration of the TOE (tests performed on CR500ia representative in the previous evaluation).

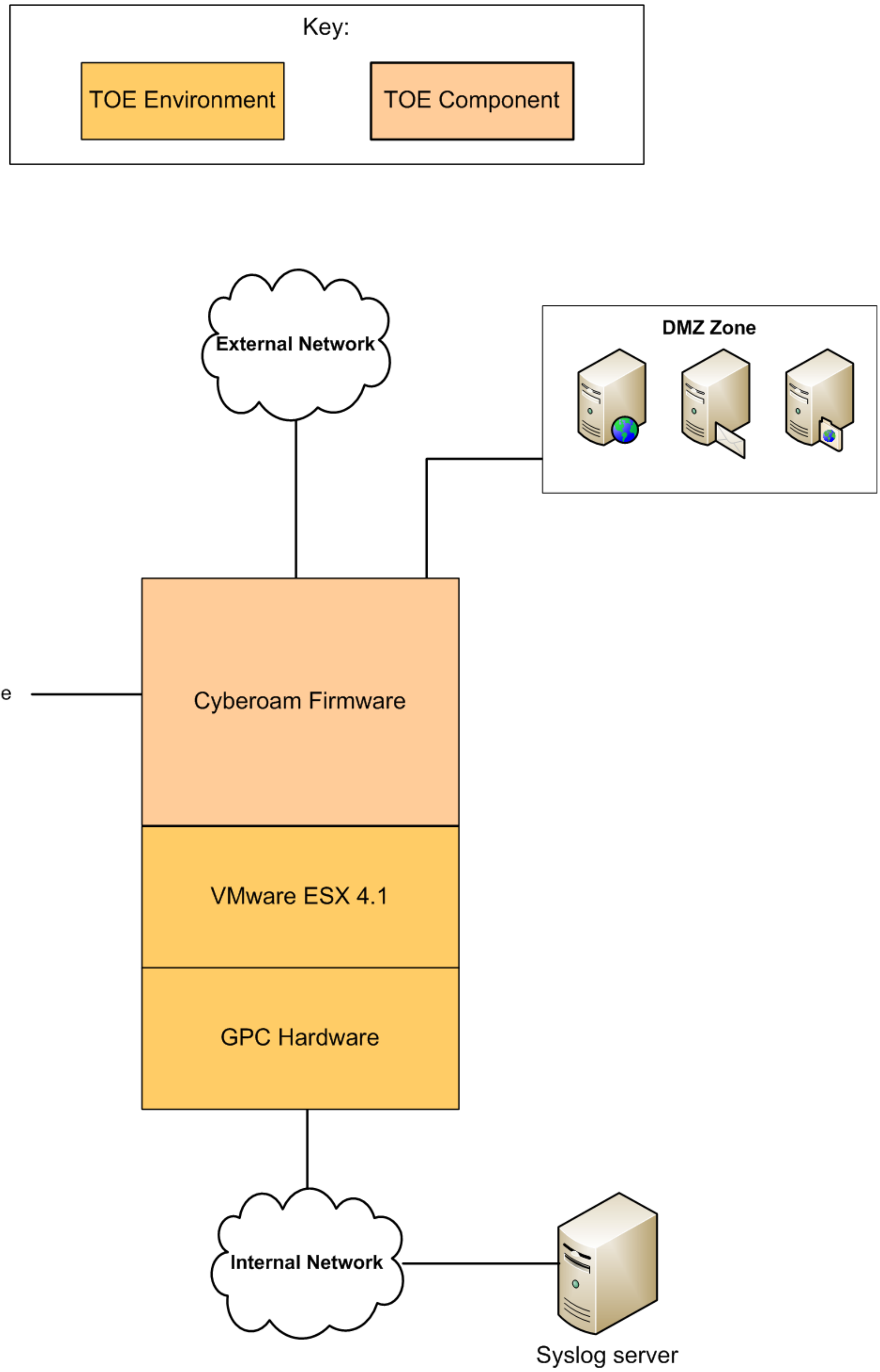


Figure 2 – Virtual Deployment Configuration of the TOE (tests performed on VMware ESX 5.0 in the previous evaluation)

A high-level overview of the different types of features and functionalities included in the TOE are listed below:

- Web Admin Console

The Web Admin Console is a web-based graphical interfaced used to configure and manage the Cyberoam appliance.

- Local Authentication

The TOE provides administrator level authentication that can be performed using the local database on the TOE.

- Firewall

Cyberoam’s stateful and deep packet inspection firewall allows identity-based policy creation for its multiple security features through a single interface, giving ease of management and high security with flexibility. Cyberoam UTM Firewall protects organizations from DoS, DDoS and IP/MAC Spoofing attacks.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4+ augmented with Flaw Remediation ALC_FLR.2 according to Common Criteria v 3.1 (CC_P1, CC_P2, CC_P3).

Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	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 ALC : Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM Coverage
	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
	ALC_FLR.2 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	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 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

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v 3.1 (CC_P1, CC_P2, CC_P3)::

Name	Description
FAU_GEN.1	Audit Data Generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.3	TSF-initiated termination
FTA_TAB.1	Default TOE access banners

IDENTIFICATION

Product: Cyberoam Firmware v10.5.4

Security Target: “Cyberoam Technologies Pvt. Ltd. Cyberoam Firmware v10.5.4 Security Target Version 1.7, September 2014 ”.

Protection Profile: None

Evaluation Level: EAL4+ augmented with Flaw Remediation ALC_FLR.2

.

SECURITY POLICIES

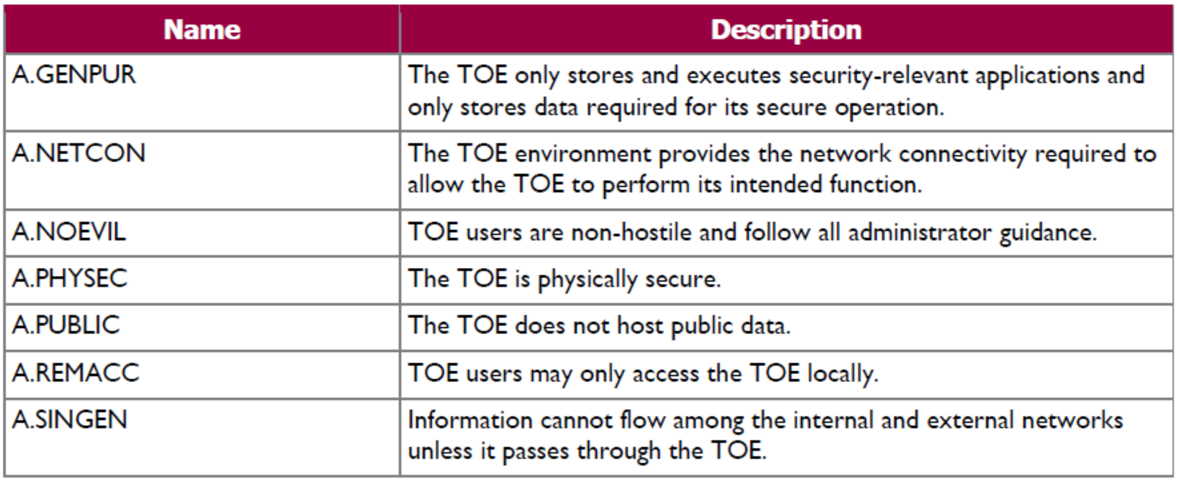
This Security Target defines no Organizational Security Policies

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

Table 5 – Assumptions



Name	Description
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended function.
A.NOEVIL	TOE users are non-hostile and follow all administrator guidance.
A.PHYSEC	The TOE is physically secure.
A.PUBLIC	The TOE does not host public data.
A.REMACC	TOE users may only access the TOE locally.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

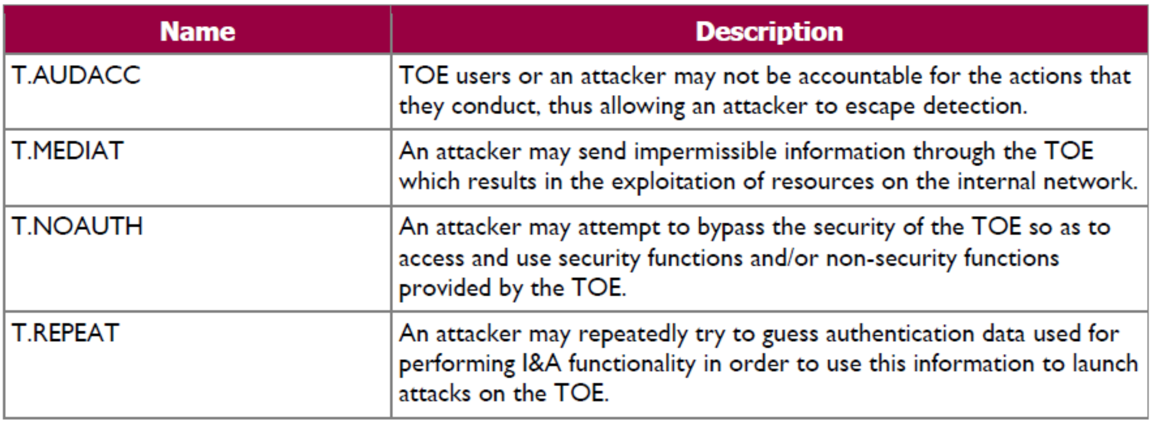
CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Cyberoam Firmware v10.5.4, although the agents implementing attacks have the attack potential according to the “Enhanced basic” of EAL4 + ALC_FLR.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Table 4 – Threats



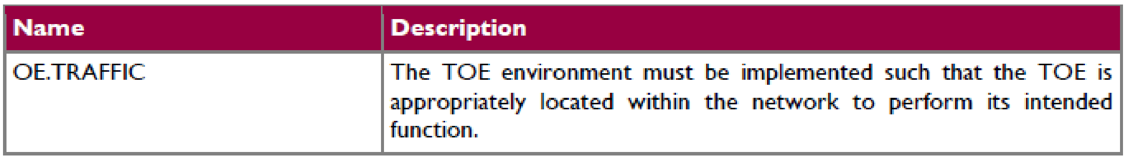
Name	Description
T.AUDACC	TOE users or an attacker may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.
T.MEDIAT	An attacker may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An attacker may repeatedly try to guess authentication data used for performing I&A functionality in order to use this information to launch attacks on the TOE.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Table 7 – IT Security Objectives



Name	Description
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

The TOE is the firmware that runs on the Cyberoam series hardware and virtual appliances. The TOE is installed on a network whenever firewall services are required. The TOE can be deployed in Gateway or Bridge mode in both configurations. This allows the TOE to be used as a firewall; as well as a gateway for routing traffic. To control Internet access entirely through the TOE, the entire Internet bound traffic from the local area network (LAN) network must first pass through the TOE. The TOE is software-only with the Cyberoam hardware or virtual appliance as part of the TOE environment.

The firewall rules functionality protects the network from unauthorized access and typically guards the LAN and DMZ networks against malicious access. Firewalls rules may also be configured to limit the access to harmful sites for LAN users.

Firewall rules provide centralized management of security policies. From a single firewall rule, you can define and manage an entire set of TOE security policies. Firewall rules control traffic passing through the TOE. Depending on the instruction in the rule, the TOE decides on how to process the access request. When the TOE receives the request, it checks for the source address, destination address, TCP or UDP protocol, and port number and tries to match it with the firewall rule. It also keeps track of the state of connection and denies any traffic that is not part of the connection state.

The TOE provides extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse.

These logs can be viewed through the Web Admin Console.

The TOE also provides the following management functionalities:

- System administration and configuration;
- Firewall rules management;
- Configure user authentication ;
- Users management;

- Management of the following Traffic Information Flow Control SFP security attributes:
  - Subject IP address
  - Traffic Source IP address
  - Traffic Destination IP address
  - Traffic TCP or UDP transport protocols
  - Traffic port number

A high-level overview of the different types of features and functionalities included in the TOE are listed below:

- **Web Admin Console**: The Web Admin Console is a web-based graphical interfaced used to configure and manage the Cyberoam appliance.
- **Local Authentication**: The TOE provides administrator level authentication that can be performed using the local database on the TOE.

- **Firewall**: Cyberoam's stateful and deep packet inspection firewall allows identity-based policy creation for its multiple security features through a single interface, giving ease of management and high security with flexibility. Cyberoam UTM Firewall protects organizations from DoS, DDoS and IP/MAC Spoofing attacks.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- Cyberoam Firmware v 10.5.4 Security Target v 1.7, September 2014
- Cyberoam UTM Onlinehelp Version – 1.0 – 10.5.3 – 05/07/2013
- Cyberoam Unified Threat Management Failsafe Troubleshooting for Hardware Appliance Version 10, Document Version 10.5.3 – 05/07/2013
- Cyberoam Unified Threat Management Failsafe Troubleshooting for Virtual UTM Appliance Version 10, Document Version 10.5.3 – 05/07/2013
- Cyberoam Unified Threat Management User Guide Version 10, Document Version 10.5.3 – 05/07/2013
- Cyberoam Unified Threat Management Release Notes Version 10.5.3, Document Version 1.04-05/07/2013
- Cyberoam Firmware v10.5.4 Guidance Documentation Supplement v1.1, September 2014
- Cyberoam Virtual UTM Appliance Vmware ESX/ESXi Installation Guide Version 10, Document version 10.04.0255-26/03/2013
- Cyberoam Unified Threat Management QUICK START GUIDE CR500ia Appliance, Document version PL QSG 500ia/96000/10.02.0.0.473/05252013

Note: guidance from the previous certified TOE (version 10.5.3), are also applicable to TOE version 10.5.4 as they have not been modified. They will be made available to the final users with this evaluated version.

PRODUCT TESTING

The vendor starts an assurance continuity process the 21st July 2014 sending to the CB-CCN the corresponding certification request and the security impact analysis.

The baseline TOE for this certificate maintenance has been the Cyberoam Firmware v10.5.3, which completed an EAL4+ Common Criteria evaluation on 5th November 2013.

The CB-CCN categorized some of the changes as MINOR and some of them as MAJOR. A set of re-evaluation activities have been carried out according to [AC], mainly regarding the ALC activity. A site visit to the new development site was performed to check the physical security measures of the new area and also to be sure that the repositories were imported properly and the procedures were still applying.

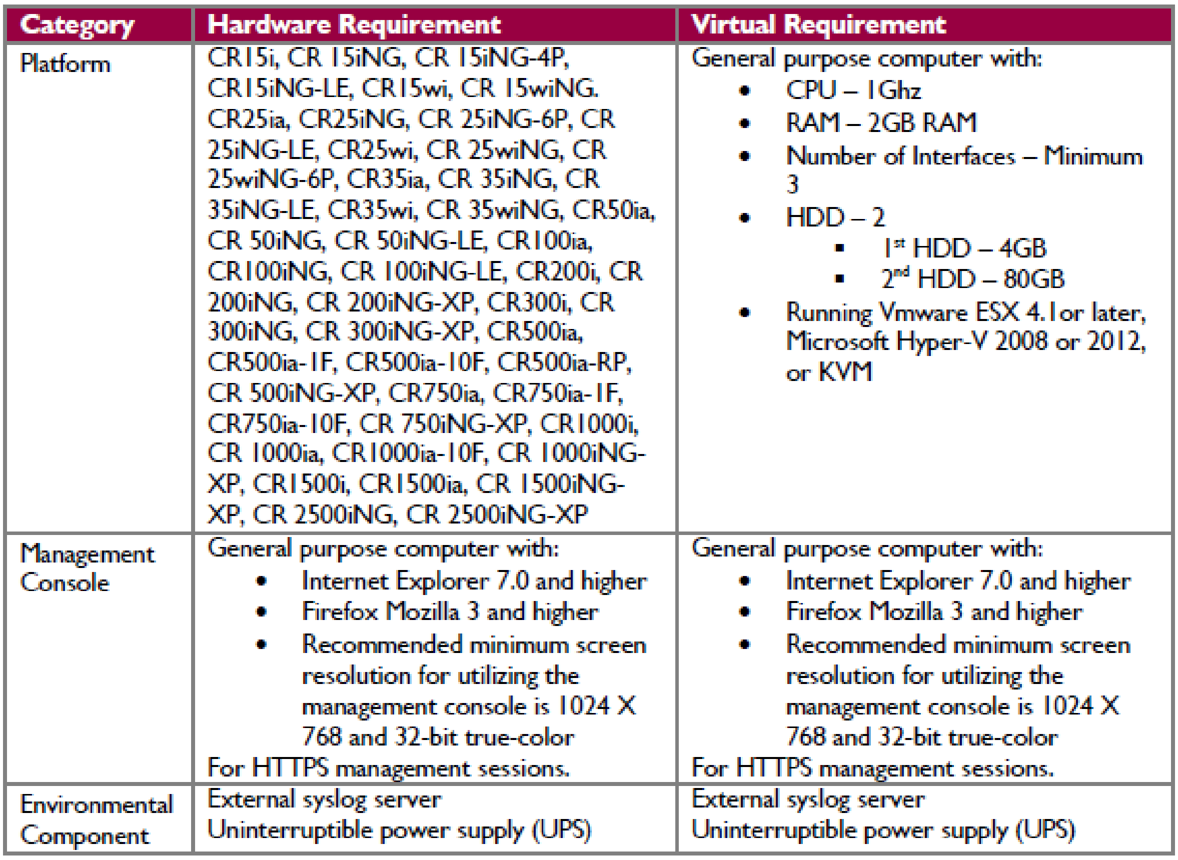
In addition, the new ST was reviewed and the ASE activity revisited to reflect the new version of the TOE and the existence of new supported platforms.

No other assurance activities were carried out as part of this re-evaluation.

Both ASE and ALC partial report were updated to reflect these changes and the corresponding results.
No more assurance activities have been performed for the certificate maintenance.

EVALUATED CONFIGURATION

The following figure shows the operational environment of the TOE providing information regarding the supported platforms and software components for Cyberoam Firmware v10.5.4:



Category	Hardware Requirement	Virtual Requirement
Platform	CR15i, CR 15iNG, CR 15iNG-4P, CR15iNG-LE, CR15wi, CR 15wiNG. CR25ia, CR25iNG, CR 25iNG-6P, CR 25iNG-LE, CR25wi, CR 25wiNG, CR 25wiNG-6P, CR35ia, CR 35iNG, CR 35iNG-LE, CR35wi, CR 35wiNG, CR50ia, CR 50iNG, CR 50iNG-LE, CR100ia, CR100iNG, CR 100iNG-LE, CR200i, CR 200iNG, CR 200iNG-XP, CR300i, CR 300iNG, CR 300iNG-XP, CR500ia, CR500ia-1F, CR500ia-10F, CR500ia-RP, CR 500iNG-XP, CR750ia, CR750ia-1F, CR750ia-10F, CR 750iNG-XP, CR1000i, CR 1000ia, CR1000ia-10F, CR 1000iNG-XP, CR1500i, CR1500ia, CR 1500iNG-XP, CR 2500iNG, CR 2500iNG-XP	General purpose computer with: • CPU – 1Ghz • RAM – 2GB RAM • Number of Interfaces – Minimum 3 • HDD – 2 ▪ 1st HDD – 4GB ▪ 2nd HDD – 80GB • Running Vmware ESX 4.1or later, Microsoft Hyper-V 2008 or 2012, or KVM
Management Console	General purpose computer with: • Internet Explorer 7.0 and higher • Firefox Mozilla 3 and higher • Recommended minimum screen resolution for utilizing the management console is 1024 X 768 and 32-bit true-color For HTTPS management sessions.	General purpose computer with: • Internet Explorer 7.0 and higher • Firefox Mozilla 3 and higher • Recommended minimum screen resolution for utilizing the management console is 1024 X 768 and 32-bit true-color For HTTPS management sessions.
Environmental Component	External syslog server Uninterruptible power supply (UPS)	External syslog server Uninterruptible power supply (UPS)

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the previous evaluation is referenced in section TOE SUMMARY of this certification report.

EVALUATION RESULTS

The product Cyberoam Firmware v10.5.4 has been evaluated against the Security Target “Cyberoam Technologies Pvt. Ltd. Cyberoam Firmware v10.5.4 Security Target Version 1.7, September 2014 ”.

All the assurance components required by the evaluation level EAL4+ augmented with Flaw Remediation ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” VERDICT” to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_FLR.2, as defined by the Common Criteria v 3.1 (CC_P1, CC_P2, CC_P3) and the CEM.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment.

The following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Cyberoam Firmware v10.5.4, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level

ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, Sept. 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, Sept. 2012.

[AC] Assurance Continuity: CCRA requirements. V 2.1, June 2012

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: “Cyberoam Technologies Pvt. Ltd. Cyberoam Firmware v10.5.4 Security Target Version 1.7, September 2014”.