REF: 2012-28-INF-1239 v1	Created by: CERT3
Target: Expediente	Revised by: CALIDAD
Date: 30.09.2013	Approved by: TECNICO

CERTIFICATION REPORT

File: 2012-28 Cyberoam Firmware

Applicant: U72900GJ19 Elitecore Technologies

References:

[EXT 1905] Certification request of Cyberoam Firmware

[EXT 2262] Evaluation Technical Report of Cyberoam Firmware.

The product documentation referenced in the above documents.

Certification report of the product Cyberoam Firmware, as requested in [EXT 1905] dated 27-09-2012, and evaluated by the laboratory EPOCHE AND ESPRI, as detailed in the Evaluation Technical Report [EXT 2262] received on 01/08/2013.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

EXECUTIVE SUMMARY **3**
TOE SUMMARY 4
SECURITY ASSURANCE REQUIREMENTS 8
SECURITY FUNCTIONAL REQUIREMENTS 9
IDENTIFICATION **9**
SECURITY POLICIES **9**
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT **10**
CLARIFICATIONS ON NON-COVERED THREATS 10
OPERATIONAL ENVIRONMENT FUNCTIONALITY 11
ARCHITECTURE **12**
DOCUMENTS **13**
PRODUCT TESTING **14**
EVALUATED CONFIGURATION **14**
EVALUATION RESULTS **17**
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM **17**
CERTIFIER RECOMMENDATIONS **18**
GLOSSARY **18**
BIBLIOGRAPHY **18**
SECURITY TARGET **18**

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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:

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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 AND ESPRI.

Protection Profile: None.

Evaluation Level: EAL4 + ALC_FLR.2.

Evaluation end date: 01/08/2013.

All the assurance components required by the evaluation level EAL 4 (augmented with ALC_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory EPOCHE AND ESPRI assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 + 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 v10.5.3, 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.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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:

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

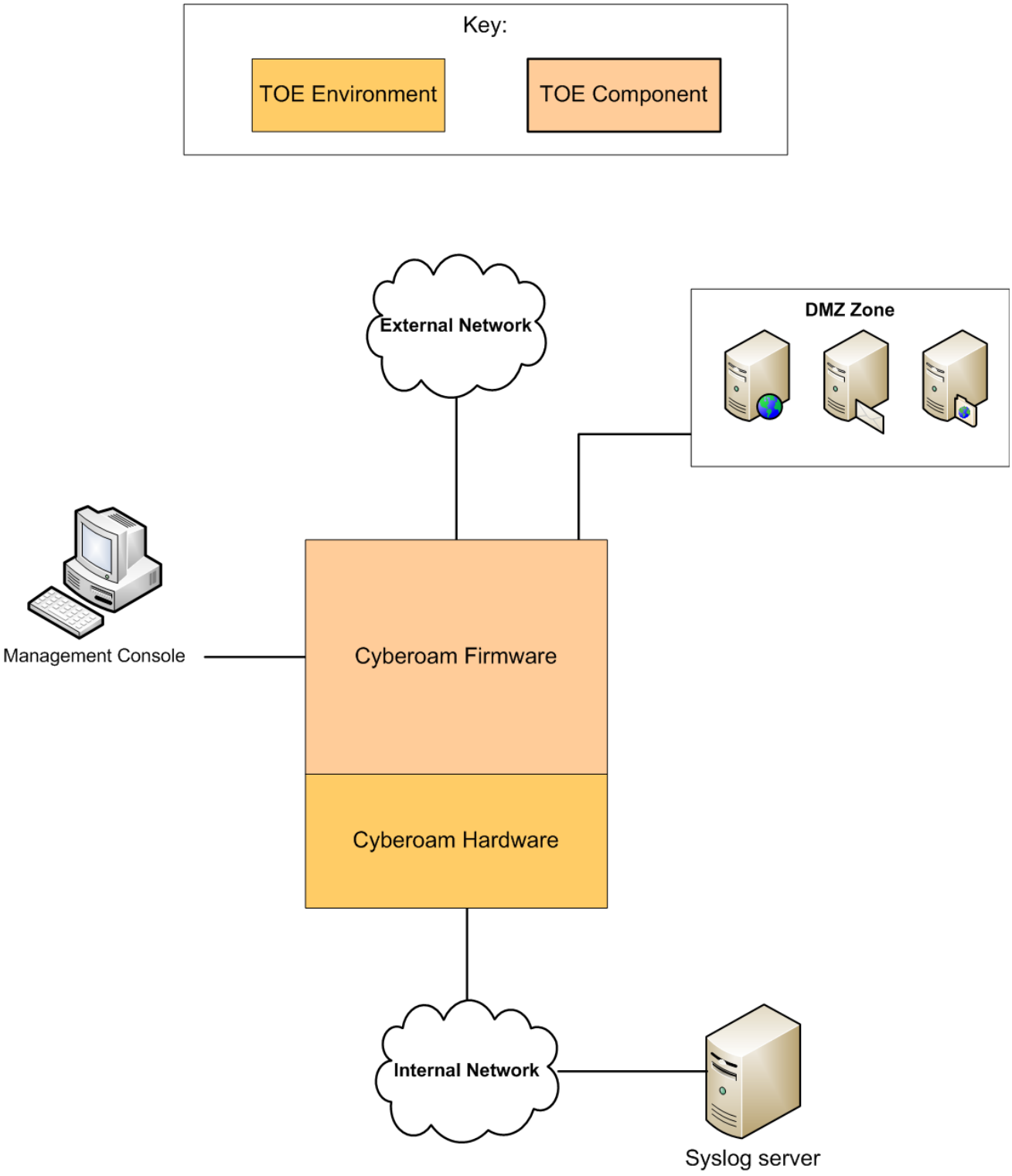

Figure 1 – Hardware Deployment Configuration of the TOE

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

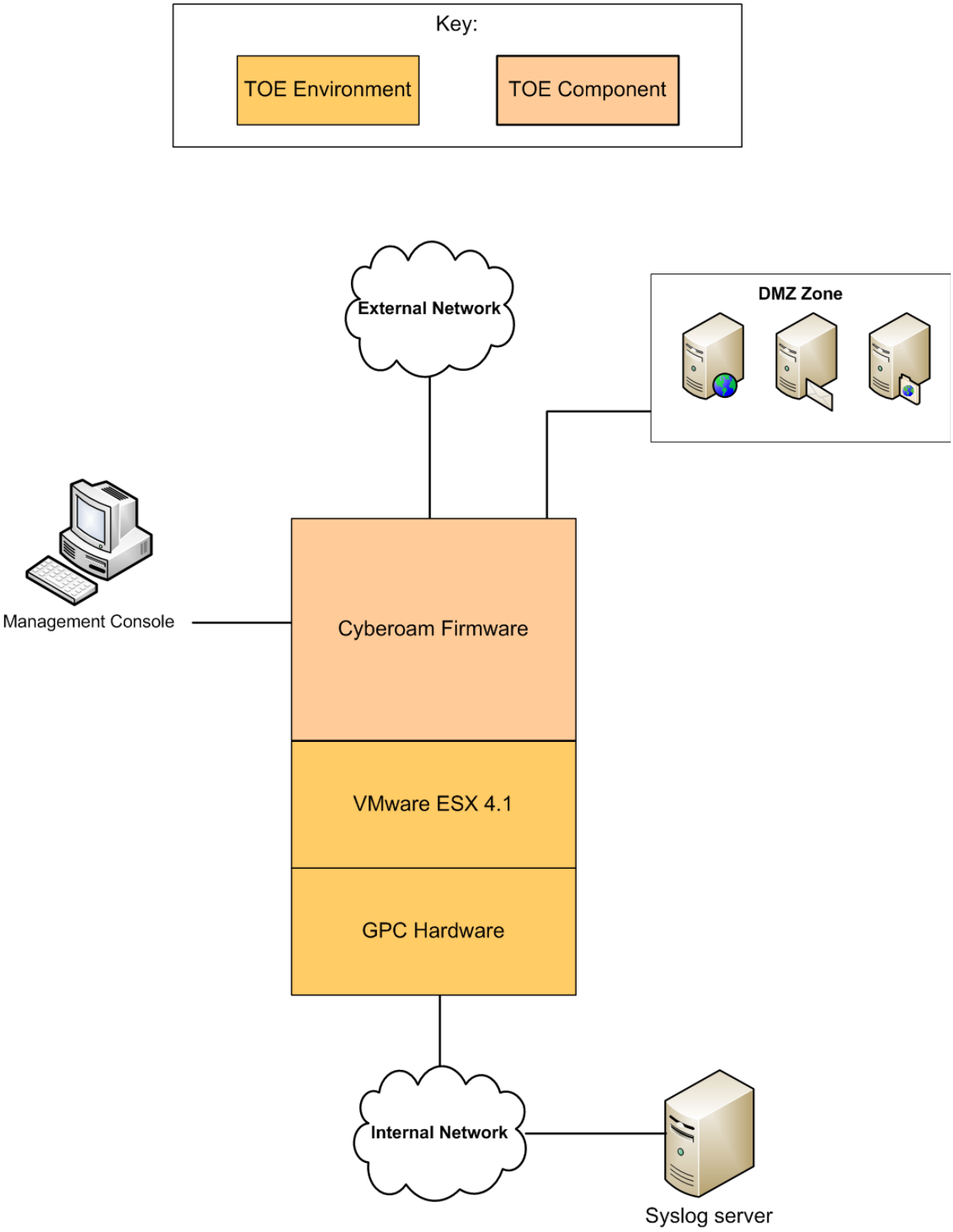

Figure 2 – Virtual Deployment Configuration of the TOE

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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 + 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

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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 v10.5.3

Security Target: Cyberoam Firmware v 10.5.3 Security Target v 1.4, July 2013.

Protection Profile: None.

Evaluation Level: EAL4 + ALC_FLR.2.

SECURITY POLICIES

This Security Target defines no Organizational Security Policies

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

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 v10.5.3, although the agents implementing attacks have the attack potential

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

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.

Name	Description
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

	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;

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- 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 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 v10.5.3 Guidance Documentation Supplement v0.9, July 03, 2013
- Cyberoam Virtual UTM Appliance VMware ESX/ESXi Installation Guide Version 10, Document version 10.04.0255-26/03/2013

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Cyberoam Unified Threat Management QUICK START GUIDE CR500ia Appliance, Document version PL QSG 500ia/96000/10.02.0.0.473/05252013

These documents can be downloaded from http://docs.cyberoam.com and are sent with the TOE as part of a documentation CD.

The following Knowledge Base article is also required reading and part of the TOE:

- Cyberoam Unified Threat Management How To – Add an External Certificate Authority to Cyberoam, 10.5.3-05.07.2013, Knowledge Base Article

This article can be found at kb.cyberoam.com.

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.
During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises. Likewise, he has selected and repeated about 25% of the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Cyberoam Firmware v10.5.3 it is necessary the disposition of the following software components:

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

The TOE is deployed in two configurations: appliance and virtual configuration as depicted in Figure 1 and Figure 2. Both configurations have been tested during the evaluation.

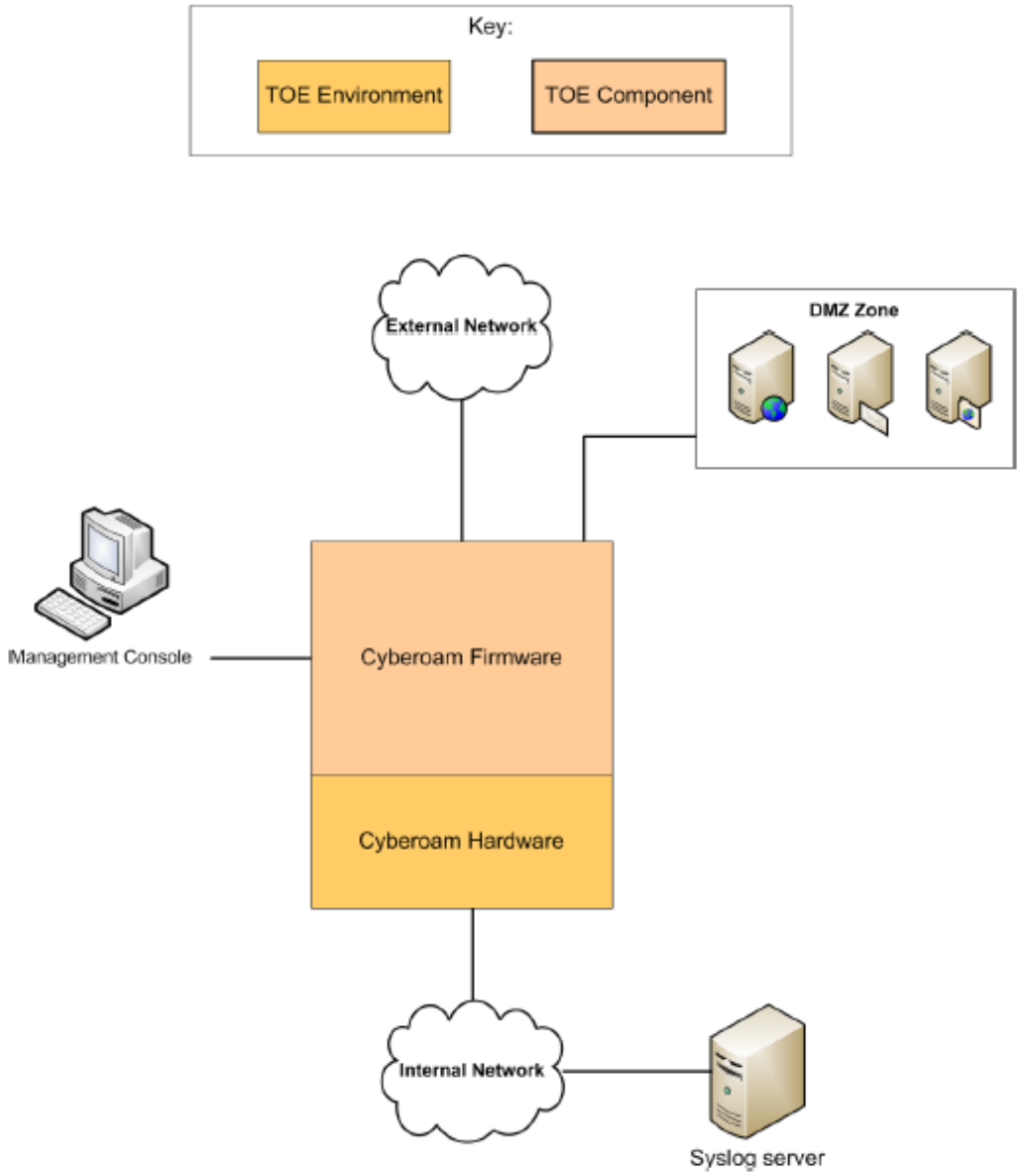

Figure 1 – Hardware Deployment Configuration of the TOE

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

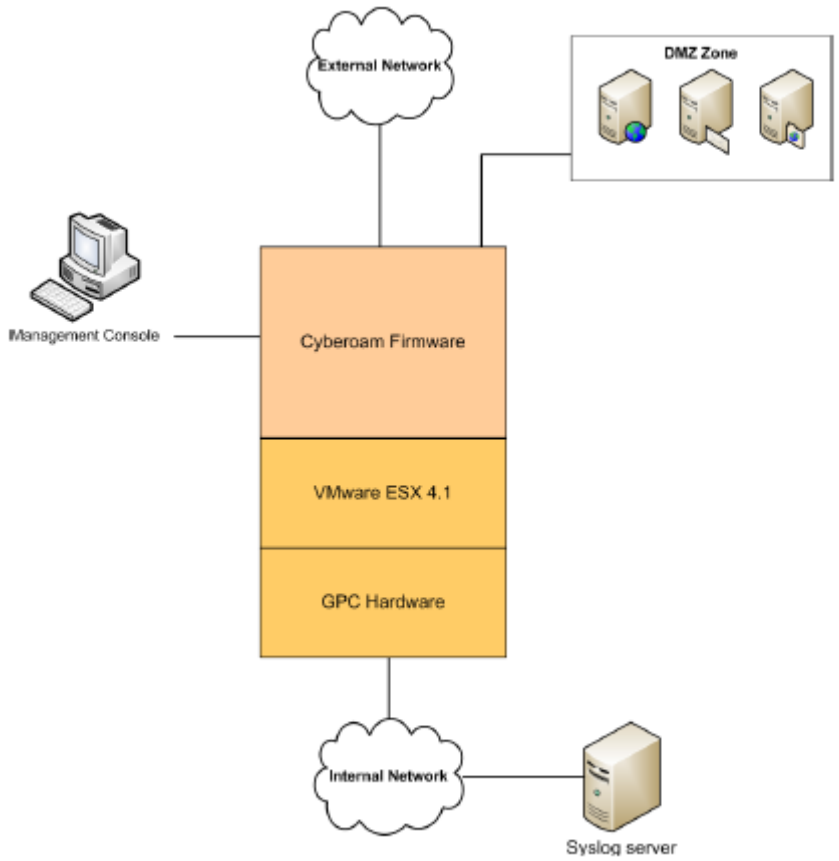

Figure 2 – Virtual Deployment Configuration of the TOE

As mentioned previously, the ST declares, two configurations of the TOE have been evaluated: FW running in an HW appliance and FW running on a virtual platform based in VMWare product. Both TOEs were downloaded and the testing has performed in both configurations for the certification purposes.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Category	Hardware Requirement	Virtual Requirement
Platform	CR15i, CR15wi, CR25ia, CR25wi, CR35ia, CR35wi, CR50ia, CR100ia, CR200i, CR300i, CR500ia, CR700ia, CR1000i, CR 1000ia, CR1500i, CR1500ia	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
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)

For the HW platform, one canonical representative (CR500ia) has selected from the list of supported platforms sated in [ST14] section 1.4.1 TOE environment

EVALUATION RESULTS

The product Cyberoam Firmware v10.5.3 has been evaluated against the Security Target “Cyberoam Firmware v 10.5.3 Security Target v1.4,July 2013”.

All the assurance components required by the evaluation level EAL4 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory EPOCHE AND ESPRI 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:

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- 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 v10.5.3, 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, R3 Final, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R3 Final, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R3 Final, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Cyberoam Firmware v 10.5.3 Security Target v1.4,July 2013

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es