Cyberoam Technologies Pvt. Ltd.

Cyberoam Firmware v10.5.4

Security Target

Evaluation Assurance Level (EAL): EAL4+
Document Version: 1.7

Prepared for:

Cyberoam Technologies Pvt. Ltd.
Cyberoam House, Saigulshan Complex
Opp. Sanskruti, Beside White House,
Panchwati Cross Road, Ahmedabad 380 006
Gujarat, India

Phone: +91 79 622 16 666
Email: Sales@Cyberoam.com
http://www.cyberoam.com

Prepared by:

Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Cyberoam Firmware v10.5.4, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only Unified Threat Management (UTM)/firewall that runs on the Cyberoam hardware series appliances or in a virtual environment. The TOE offers identity-based comprehensive security to organizations against multiple security services, such as worms, viruses, malware, data loss, identity theft; threats over applications; threats over secure protocols such as HTTPS[1]; and traffic management capabilities.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	Cyberoam Technologies Pvt. Ltd. Cyberoam Firmware v10.5.4 Security Target
ST Version	Version 1.7
ST Author	Corsec Security, Inc.
ST Publication Date	9/17/2014
TOE Reference	Cyberoam Firmware v10.5.4

[1] HTTPS – Hypertext Transfer Protocol Secure

1.3 Product Overview

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[2] 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[3] spoofing attacks, spam, intrusions and data leakage. Cyberoam can be managed through the Web Admin Console, CLI[4], or SNMP[5] agent.

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

CLI
The CLI console provides a collection of tools to administer, monitor, and control certain Cyberoam components through a serial connection, mostly for advanced trouble shooting.

SNMP
SNMP allows administrators to monitor the status of Cyberoam and receive notification of critical events as they occur on the network.

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

External Authentication
Cyberoam provides administrator level authentication that can be performed using an external ADS[6] server, LDAP[7] server or RADIUS[8] server.

[2] It should be noted that throughout the ST, whenever referencing "administrator" starting with a lower case "a", refers to all administrators and their corresponding permission detailed in section 7.1.4. "Administrator", starting with an upper case "A", refers to the Administrator role detailed in section 7.1.4. An authorized administrator refers to a TOE user that has been assigned a legitimate role and valid credentials. .
[3] IP – Internet Protocol
[4] CLI – Command Line Interface
[5] SNMP – Simple Network Management Protocol
[6] ADS – Active Directory Services
[7] LDAP – Lightweight Directory Access Protocol

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[9] Spoofing attacks.

VPN
Cyberoam offers secure remote access to organizations with the flexibility to choose from IPSec[10], L2TP[11], PPTP[12], and SSL[13] VPN technologies over its UTM appliances. Cyberoam enables identity-based access policies to prevent unauthorized network access over VPN, besides controlling 'who accesses what' over VPN.

Intrusion Prevention System
Cyberoam Intrusion Prevention System (IPS) protects against network and application attacks through thousands of automatically updated signatures that enable protection against latest vulnerabilities. It offers security against intrusions, malware, Trojan, DoS and DDoS attacks, malicious code transmission, blended threats and more.

Anti-Virus & Anti-Spyware
Cyberoam's Gateway Anti-Virus and Anti-Spyware protects against malware, including viruses, worms, spyware, backdoors, Trojans, and keyloggers over web, email, and Instant Messaging. With a database of millions of signatures updated periodically, it scans malware over incoming/outgoing traffic to reduce the window of vulnerability in organizations.

Anti Spam
The Gateway Anti-Spam offers real-time spam protection over all email protocols - SMTP[14], POP3[15], IMAP[16], providing protection against blended threats involving spam, malware, botnets, phishing, and more. Cyberoam's signature-less Rapid Pattern Detection technology detects and blocks emerging spam outbreaks for zero-hour spam protection. It also offers 98% spam protection with 1 in a million false positive rate.

Outbound Spam Protection
The Outbound Spam Protection blocks outbound spam in real-time in service provider networks. It enables detection of locally generated outbound spam and spam that is part of a global outbreak, putting an end to IP address blacklisting and loss of corporate reputation, besides identifying the spammer source to eliminate the real source of spam.

Web Filtering
Cyberoam's award-winning Web Filtering blocks access to harmful, inappropriate, and dangerous websites through its comprehensive uniform resource locator (URL) databases with millions of URLs grouped into 82+ categories. Cyberoam enables identity-based web access policies, preventing data and productivity loss, and rightly replacing expensive, best-of-breed web filters.

Bandwidth Management
Cyberoam Bandwidth Management enables prioritization of applications and users for bandwidth allocation that ensures assured application quality of service (QoS) for business critical applications,

[8] RADIUS – Remote Authentication Dial-In User Service
[9] MAC – Media Access Control
[10] IPSec – Internet Protocol Security
[11] L2TP – Layer 2 Tunneling Protocol
[12] PPTP – Point-to-Point Tunneling Protocol
[13] SSL – Secure Socket Layer
[14] SMTP – Simple Mail Transfer Protocol
[15] POP3 – Post Office Protocol 3
[16] IMAP – Internet Message Access Protocol

prevents congestion and bandwidth abuse in networks. Cyberoam enables committed and burstable bandwidth that results in assured bandwidth to critical users and automatic assignment of idle bandwidth to other applications.

Application Visibility & Control
Cyberoam offers Application Visibility and Control to enable application control to accelerate business critical applications, stagger non-critical applications, selectively accelerate socio-business applications, and block undesirable applications to achieve the twin goals of Application QoS and optimal bandwidth utilization. Application controls can be based on users and job roles, time, and network policies.

Web Application Firewall
Cyberoam's Web Application Firewall on its UTM appliances secures websites and web applications in organizations against attacks like SQL[17] injection, cross-site scripting, and more, including the Open Web Application Security Project's Top 10 vulnerabilities. The Cyberoam Web Application Firewall is deployed to intercept the traffic to and from the web servers to provide an added layer of security against attacks before they can reach the Web applications.

3G[18] / WiMAX[19] Connectivity
Cyberoam UTM appliances support 3G and WiMAX WAN connectivity, offering assured security and connectivity over wireless wide area network (WAN) links for continuous business processes. Automatic failover from a wireline to wireless link ensures high availability in WAN connectivity in case the wireless WAN link fails.

Instant Messaging (IM) Archiving & Controls
Cyberoam's IM Archiving and Controls enable identity-based policies to control access to IM applications, providing visibility and archiving facility that meets regulatory compliance requirements. It enables controls over file transfer, voice and video chat that prevent data leakage over IMs, phishing, malware, viruses and other malicious attacks.

Multiple Link Management
As part of the WAN features of Cyberoam, Multiple Link Management provides reliable WAN connectivity while supporting WAN redundancy – giving assured access to business applications involved in collaboration, Cloud and software as a service deployments. Automated Load Balancing of multiple ISP links, link failover, and user-identity-based routing delivers higher return on investment and minimizes overload in organizations.

On-Appliance Reporting
Cyberoam's on-appliance reporting gives user identity-based logs and reports on the UTM appliance itself, providing real-time information on who is doing what in the network, including dynamic Wi-Fi environments. This supports regulatory compliance requirements and instant security action, besides eliminating the need to invest in a separate reporting solution, minimizing investment cost and operational expense.

IPv6 Ready
Cyberoam is "IPv6 Ready" Gold logo certified by the international IPv6 Forum. The Gold logo assures that Cyberoam's UTM appliances are IPv6 Ready and can identify and process IPv6 traffic, which makes Cyberoam appliances future-ready for the move to IPv6 technology.

Wi-Fi Appliances
Cyberoam enables identity-based Wi-Fi access that enhances network and data security, and protects remote offices and public hotspots from intrusions, identity theft through MAC spoofing, DoS attacks and

[17] SQL – Structured Query Language
[18] 3G – Third Generation
[19] WiMAX – Worldwide Interoperability for Microwave Access

malware entry. The appliances support 802.11n/b/g wireless standards while combining the features of a router along with offering Cyberoam's complete set of UTM features.

Virtual Appliances
Cyberoam provides a virtual appliance that allows companies to reduce hardware ownership and cost by deploying the Cyberoam firmware in a virtual environment. Cyberoam supports the following virtual environments and platforms:

- VMware Workstation 7.0/8.0
- VMware vSphere
- VMware ESX/ESXi 3.5/4.0/4.1/5.0
- Microsoft Hyper-V
- Citrix XenServer 5.6 SP2/6.0
- Open Source Xen 3.4.3/4.1
- VMware Player 3.0/4.0
- Virtual Box
- Microsoft Virtual PC
- Kernel-based Virtual Machine (KVM)

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

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[20] 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 ;

[20] DMZ – Demilitarized Zone

- 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:

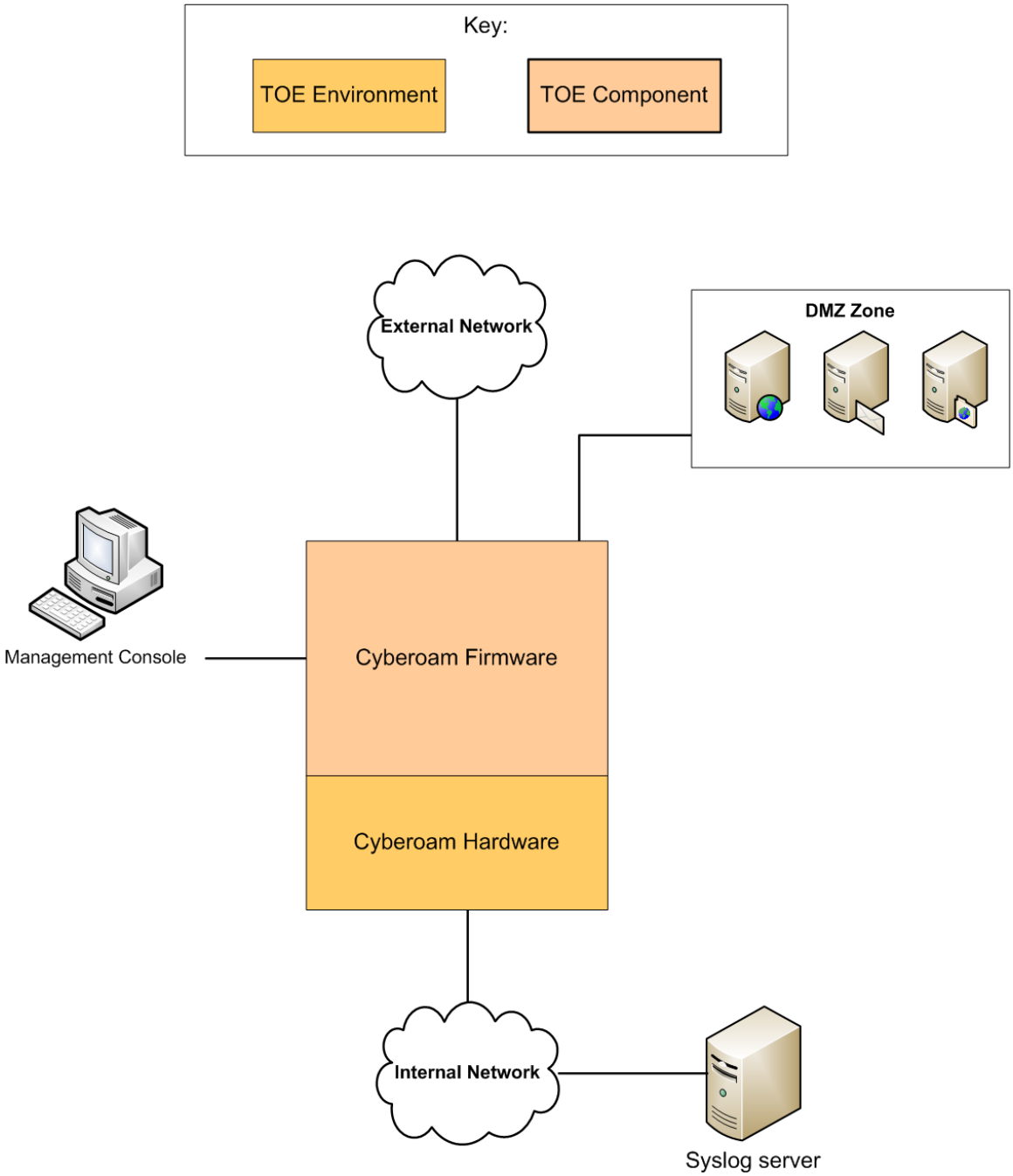

Figure 1 – Hardware Deployment Configuration of the TOE

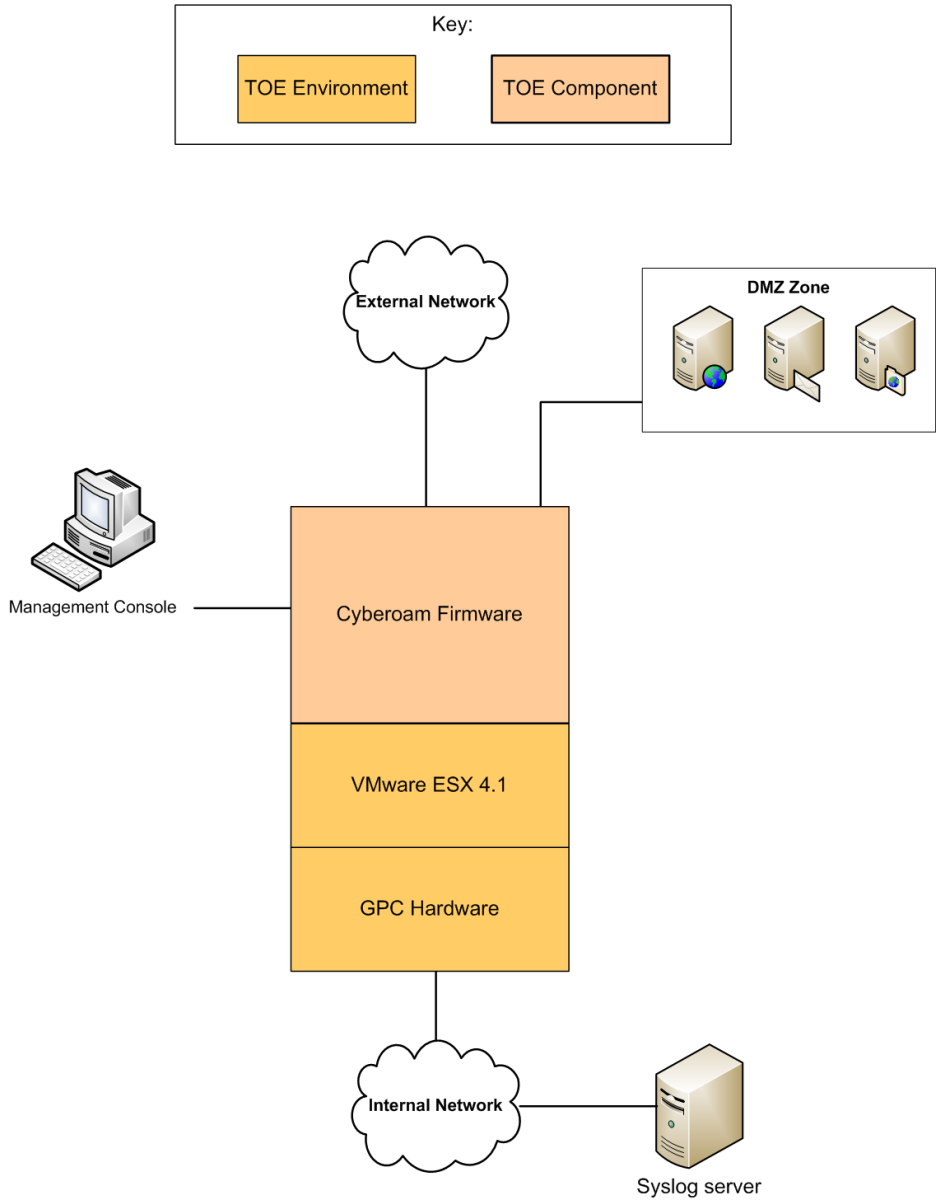

Figure 2 – Virtual Deployment Configuration of the TOE

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.

The following are the Product Physical/Logical Features and Functionality that are not included in the TOE:

CLI
The CLI console provides a collection of tools to administer, monitor, and control certain Cyberoam components through a serial connection, mostly for advanced trouble shooting.

SNMP
SNMP allows administrators to monitor the status of Cyberoam and receive notification of critical events as they occur on the network.

External Authentication
Cyberoam provides administrator level authentication that can be performed using an external ADS server, LDAP server or RADIUS server.

VPN
Cyberoam offers secure remote access to organizations with the flexibility to choose from IPSec, L2TP, PPTP, and SSL VPN technologies over its UTM appliances. Cyberoam enables identity-based access policies to prevent unauthorized network access over VPN, besides controlling 'who accesses what' over VPN.

Intrusion Prevention System
Cyberoam Intrusion Prevention System (IPS) protects against network and application attacks through thousands of automatically updated signatures that enable protection against latest vulnerabilities. It offers security against intrusions, malware, Trojan, DoS and DdoS attacks, malicious code transmission, blended threats and more.

Anti-Virus & Anti-Spyware
Cyberoam's Gateway Anti-Virus and Anti-Spyware protects against malware, including viruses, worms, spyware, backdoors, Trojans, and keyloggers over web, email, and Instant Messaging. With a database of millions of signatures updated periodically, it scans malware over incoming/outgoing traffic to reduce the window of vulnerability in organizations.

Anti Spam
The Gateway Anti-Spam offers real-time spam protection over all email protocols – SMTP, POP3, IMAP providing protection against blended threats involving spam, malware, botnets, phishing, and more. Cyberoam's signature-less Rapid Pattern Detection technology detects and blocks emerging spam outbreaks for zero-hour spam protection. It also offers 98% spam protection with 1 in a million false positive rate.

Outbound Spam Protection
The Outbound Spam Protection blocks outbound spam in real-time in service provider networks. It enables detection of locally generated outbound spam and spam that is part of a global outbreak, putting an end to IP address blacklisting and loss of corporate reputation, besides identifying the spammer source to eliminate the real source of spam.

Web Filtering
Cyberoam's award-winning Web Filtering blocks access to harmful, inappropriate, and dangerous websites through its comprehensive uniform resource locator (URL) databases with millions of URLs grouped into

82+ categories. Cyberoam enables identity-based web access policies, preventing data and productivity loss, and rightly replacing expensive, best-of-breed web filters.

Bandwidth Management
Cyberoam Bandwidth Management enables prioritization of applications and users for bandwidth allocation that ensures assured application quality of service (QoS) for business critical applications, prevents congestion and bandwidth abuse in networks. Cyberoam enables committed and burstable bandwidth that results in assured bandwidth to critical users and automatic assignment of idle bandwidth to other applications.

Application Visibility & Control
Cyberoam offers Application Visibility and Control to enable application control to accelerate business critical applications, stagger non-critical applications, selectively accelerate socio-business applications, and block undesirable applications to achieve the twin goals of Application QoS and optimal bandwidth utilization. Application controls can be based on users and job roles, time, and network policies.

Web Application Firewall
Cyberoam's Web Application Firewall on its UTM appliances secures websites and web applications in organizations against attacks like SQL injection, cross-site scripting, and more, including the Open Web Application Security Project's Top 10 vulnerabilities. The Cyberoam Web Application Firewall is deployed to intercept the traffic to and from the web servers to provide an added layer of security against attacks before they can reach the Web applications.

3G / WiMAX Connectivity
Cyberoam UTM appliances support 3G and WiMAX WAN connectivity, offering assured security and connectivity over wireless wide area network (WAN) links for continuous business processes. Automatic failover from a wireline to wireless link ensures high availability in WAN connectivity in case the wireless WAN link fails.

Instant Messaging (IM) Archiving & Controls
Cyberoam's IM Archiving and Controls enable identity-based policies to control access to IM applications, providing visibility and archiving facility that meets regulatory compliance requirements. It enables controls over file transfer, voice and video chat that prevent data leakage over Ims, phishing, malware, viruses and other malicious attacks.

Multiple Link Management
As part of the WAN features of Cyberoam, Multiple Link Management provides reliable WAN connectivity while supporting WAN redundancy – giving assured access to business applications involved in collaboration, Cloud and software as a service deployments. Automated Load Balancing of multiple ISP links, link failover, and user-identity-based routing delivers higher return on investment and minimizes overload in organizations.

On-Appliance Reporting
Cyberoam's on-appliance reporting gives user identity-based logs and reports on the UTM appliance itself, providing real-time information on who is doing what in the network, including dynamic Wi-Fi environments. This supports regulatory compliance requirements and instant security action, besides eliminating the need to invest in a separate reporting solution, minimizing investment cost and operational expense.

Cyberoam i-View
This feature provides logs and reports outside of the Web Admin Console. These same logs and reports are available in the Web Admin Console.

Ipv6 Ready
Cyberoam is "Ipv6 Ready" Gold logo certified by the international Ipv6 Forum. The Gold logo assures that Cyberoam's UTM appliances are Ipv6 Ready and can identify and process Ipv6 traffic, which makes Cyberoam appliances future-ready for the move to Ipv6 technology.

Wi-Fi Appliances
Cyberoam enables identity-based Wi-Fi access that enhances network and data security, and protects remote offices and public hotspots from intrusions, identity theft through MAC spoofing, DoS attacks and malware entry. The appliances support 802.11n/b/g wireless standards while combining the features of a router along with offering Cyberoam's complete set of UTM features.

NTP
Synchronizing time with an extneral NTP server is excluded from the evaluation and not allowed in the evaluated configuration.

1.4.1 TOE Environment

The TOE environment consists of the Cyberoam hardware or virtual platform. The TOE minimum requirements are listed below in Table 2 for both deployment methods. A management console for managing the TOE is required in both configurations.

Table 2 – TOE Minimum Requirements

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)

In addition, the TOE needs cable and connectors that allow all of the TOE and environmental components to communicate with each other.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

The TOE can be configured for HTTPS web-based administration from a management console. To connect to the Web Admin Console, the administrator must input a username and password. The Web Admin Console supports multiple languages, but by default appears in English. The Web Admin Console provides the following management functionalities for an Administrator and Security Admin:

- Add users
- Set time
- Configure syslog server
- Configure firewall rules
- Configure lock-out, logout, and block administrator sessions
- View Logs (Administrator and Audit Admin only)

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.

The responsibility of the firewall is to grant access from Internet to DMZ or Service Network according to the Rules and Policies configured. It also keeps track of the state of connection and denies any traffic that is not part of the connection state.

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.

The TOE provides extensive logging capabilities for traffic, system, and network protection functions. Detailed log information and reports are available locally through the Web Admin Console until a system shutdown for analysis of current network activity. An external syslog server is required in the TOE environment to provide historical analysis of network activity to help identify security issues and reduce network abuse.

For further information about the TOE security functionality, please refer to section 1.5.2.

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a firewall which runs on a Cyberoam UTM series hardware or a virtual appliance. The TOE is installed on a network whenever a firewall/UTM services are required as depicted in the Figure 3 and Figure 4 below. The essential components for the proper operation of the TOE in the evaluated configuration are:

- Cyberoam Firmware v10.5.4

The TOE is downloaded from Cyberoam's download center. The download center provides a Cyberoam Firmware v10.5.4 link that downloads an encrypted binary file for either the Cyberoam hardware or virtual appliance. The encrypted file will not have an extension, but will include the TOE version. The file is

downloaded to the location specified by the authorized user. This file includes the firmware and any configurations specific to the appliance on which it will be installed. Only the Cyberoam hardware or virtual appliance is capable of decrypting, verifying, and installing the encrypted file.

If the intended installation is a virtual configuration, an older version of the Cyberoam firmware is initially downloaded in a pre-activated .ovf file format, upon which the TOE binary firmware can be installed.

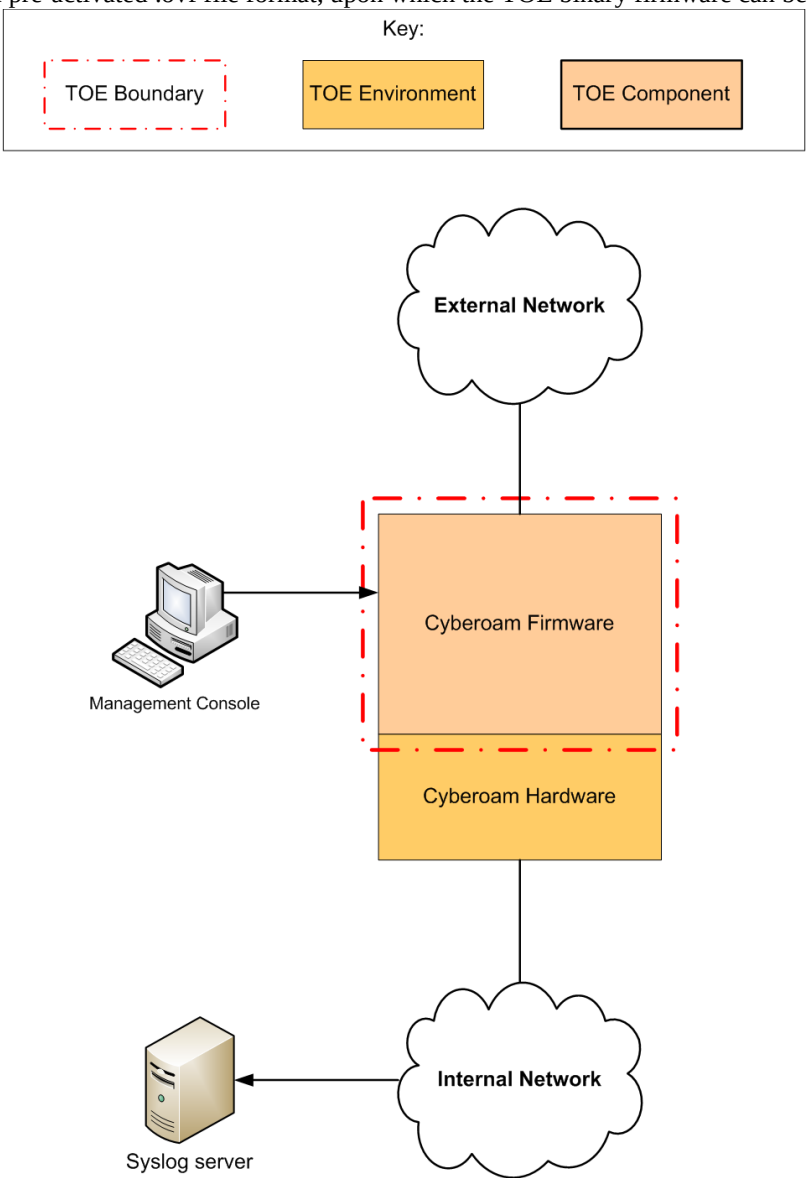

Figure 3 – Physical TOE Boundary

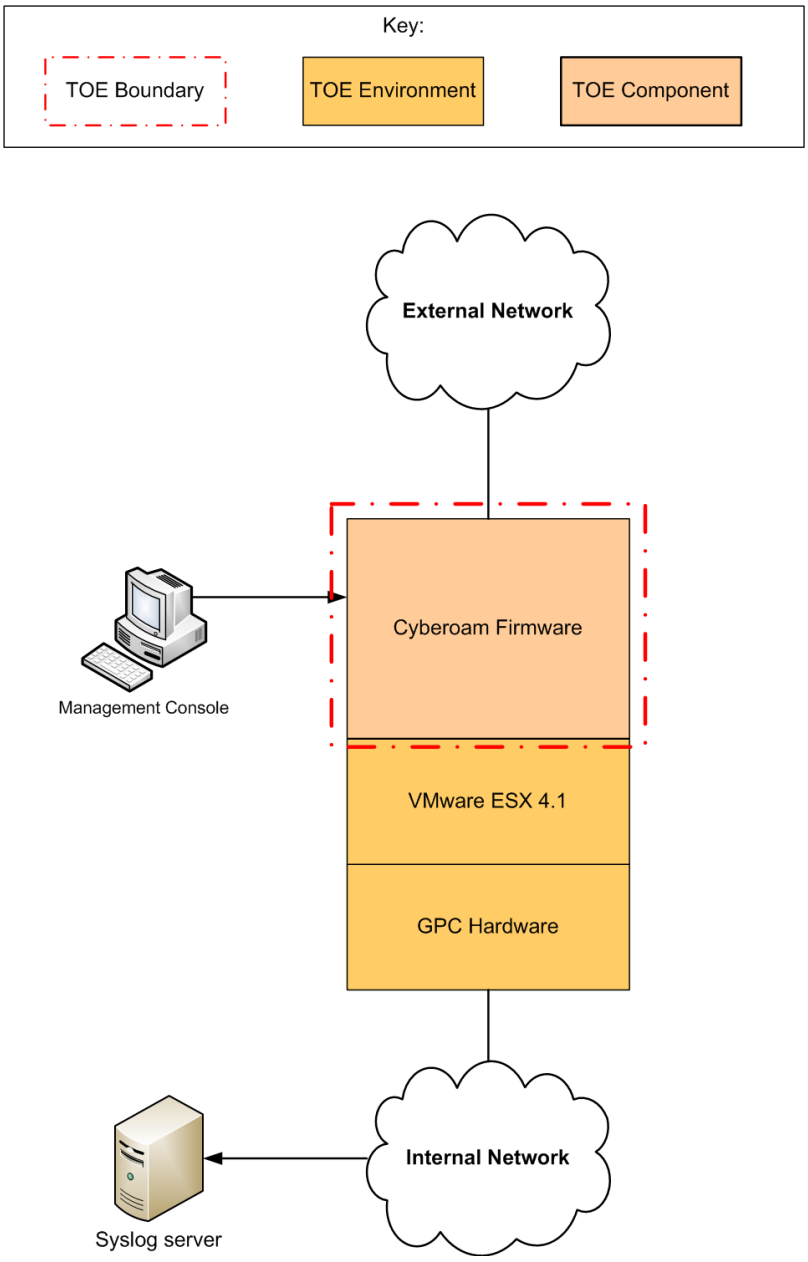

Figure 4 – Virtual TOE Boundary

1.5.1.1 TOE Firmware

The TOE consists of the firmware that runs on the Cyberoam firewall hardware or virtual appliance.

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- 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
- 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[21].

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.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access

1.5.2.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit functions, rejected and blocked traffic, administrator account activity, firewall rule modification, firewall activity, and login attempts. An Administrator or Audit Admin can view, sort, search, and order the audit records based on different factors that vary between administrator logs and invalid traffic log files. Audit records are available in the local audit log only until a reboot or system shutdown occurs. All audit records are maintained and stored in the external syslog server. The TOE protects audit records in the audit trail from unauthorized deletion and modification. In addition, the TOE can be configured to send audit data to a syslog server.

1.5.2.2 User Data Protection

The TOE controls network traffic via the Traffic Information Flow Control Security Functional Policy (SFP). The Traffic Information Flow SFP relies on source and destination IP addresses, TCP or UDP protocol, port numbers, and rules defined in the Traffic Information Flow Control Lists to determine how to treat the network traffic. The rules determine whether traffic should be accepted through the TOE to its destination, passage rejected through the network, or dropped.

1.5.2.3 Identification and Authentication

Users are required to successfully identify and authenticate with the TOE prior to any actions on the TOE. Username, password, and role are stored locally in the TOE and are compared against the username and

[21] CD – Compact Disk

password entered by a user before assigning a role and allowing access. The TOE provides a way of preventing unauthorized users from gaining access to the TOE by configuring a settable number of unsuccessful login attempts from an IP address, before the address is locked out by the TOE.

1.5.2.4 Security Management

The TOE offers a Web Admin Console that administrators can use to configure and manage TOE settings and the Traffic Information Flow Control SFP. The TOE supports the roles of Administrator, Audit Admin, Crypto Admin, HAProfile, Custom, and Security Admin roles. Administrator and Security Admin roles have the ability to modify and delete the restrictive default security attributes for the Traffic Information Flow Control SFP. The HAProfile role's functionality is excluded from the evaluation. The Custom role covers any profiles created by an administrator.

1.5.2.5 Protection of the TOE Security Functionality

The TSF provides a reliable timestamp for operations in the TOE.

1.5.2.6 TOE Access

An Administrator and Security Admin can configure the TOE to lock an interactive session after an administrative-configurable amount of minutes of inactivity, 3 minutes being the default value. The TOE can terminate management sessions after one to 99 minutes of inactivity. The default time for termination is 10 minutes. An Administrator and Security Admin can configure the TOE to display a warning message regarding unauthorized use of the TOE before an authentication session occurs.

2 Conformance Claims

This section and Table 3 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim none; Parts 2 and 3 Interpretations of the CEM as of 9/17/2014 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL4+ augmented with Flaw Remediation ALC_FLR.2

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[22] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess an enhanced basic skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation and moderate time to perform an attack. The IT assets requiring protection are the TSF[23] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

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.

3.2 Organizational Security Policies

This Security Target defines no Organizational Security Policies.

[22] IT – Information Technology
[23] TSF – TOE Security Functionality

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 5 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

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.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 6 below.

Table 6 – Security Objectives for the TOE

Name	Description
O.ACCOUNT	The TOE must provide accountability for information flows through the TOE and for TOE users' use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means for TOE users to search, sort, and order the audit trail based on relevant attributes.
O.AUTHENTICATE	The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials.
O.LIMEXT	The TOE must provide the means for TOE users to control and limit access to TOE security functions by an authorized external IT entity.
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.
O.SECFUN	The TOE must provide functionality that enables TOE users to use the TOE security functions, and must ensure that only TOE users are able to access such functionality.
O.TIME	The TOE must provide a reliable time stamp.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

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.

4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

Name	Description
NOE.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
NOE.NOEVIL	TOE users are non-hostile and follow all administrator guidance.
NOE.PHYSEC	The physical environment must be suitable for supporting a computing device in a secure setting.
NOE.PUBLIC	The TOE does not host public data.
NOE.REMACC	TOE users may only access the TOE locally.
NOE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
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		✓		

Name	Description	S	A	R	I
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				

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*Other specifically defined auditable events –* ***see Table 10 below***].

Table 10 – Auditable Events

Type of Log	Auditable Events
Firewall Rules Logs	Firewall traffic allowed
	Firewall traffic denied
Invalid Traffic Logs	Invalid traffic denied
	Invalid Fragmented Traffic Denied
Administration Logs	Add operation
	Update operation
	Delete operation
	Admin login logout

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 (if applicable), 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, [*no other information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review
Hierarchical to: No other components.
FAU_SAR.1.1

The TSF shall provide [*Administrator or Audit Admin*] with the capability to read [*audit data collected since the last reboot, excluding the audit shutdown event*] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.
FAU_SAR.3.1

The TSF shall provide the ability to apply [*searches, sorting, ordering*] of audit data based on [*Table 13*].

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

6.2.3 Class FDP: User Data Protection

FDP_IFC.1 Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1
The TSF shall enforce the [*Traffic Information Flow Control SFP*] on [
a) SUBJECTS: external IT entities that send or receive information through the TOE;
b) INFORMATION: traffic flowing through the TOE, and;
c) *OPERATIONS: ACCEPT, DROP, REJECT*].
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes
Hierarchical to: No other components.
FDP_IFF.1.1
The TSF shall enforce the [*Traffic Information Flow Control SFP*] based on the following types of subject and information security attributes: [

SUBJECT (external IT entities) attributes:
1. *IP address*

INFORMATION (traffic) attributes:
1. *Source IP address;*
2. *Destination IP address;*
3. *TCP and UDP transport protocols; and*
4. *Port number*].

FDP_IFF.1.2
The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*ACCEPT rules contained in the authorized administrator-defined Traffic Information Flow Control SFP List*].
FDP_IFF.1.3
The TSF shall enforce the [*no additional flow rules*].
FDP_IFF.1.4
The TSF shall explicitly authorize an information flow based on the following rules: [*ACCEPT rules contained in the authorized administrator-defined Traffic Information Flow Control List*].
FDP_IFF.1.5
The TSF shall explicitly deny an information flow based on the following rules: [*DROP, REJECT rules contained in the authorized administrator-defined Traffic Information Flow Control List*].
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

6.2.4 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [an administrator-configurable positive integer within [*1 and 5*]] of unsuccessful authentication attempts occur related to [*authorized TOE administrator access from the same IP in an administrator-configurable 1-120 seconds*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block any administrator account from that IP address for an administrator-configurable timeframe of 1-60 minutes*].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

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

Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [enable, disable, modify the behavior of] the functions [

- *System administration and configuration;*
- *Firewall rules management;*
- *Configure users*[24] *authentication; and*
- *Users management*]

to [*authorized administrators with sufficient permission level*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Traffic Information Flow Control SFP*] to restrict the ability to [[*create*], modify, and delete] the security attributes [

SUBJECT (external IT entities) attributes:

1. *IP address*

INFORMATION (traffic) attributes:

1. *Source IP address;*
2. *Destination IP address;*
3. *TCP and UDP transport protocols; and*
4. *Port number*]

to [*Administrator and Security Admin roles*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Traffic Information Flow Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Administrator and Security Admin roles*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

- The TSF shall be capable of performing the following management functions [
- *System administration and configuration;*
- *Firewall rules management;*
- *Configure user authentication; and*
- *Users management*
- *Management of the following Traffic Information Flow Control SFP security attributes:*

[24] It should be noted that throughout the Security Target, user represents all TOE users and administrators.

- *Subject IP address*
- *Traffic Source IP address*
- *Traffic Destination IP address*
- *Traffic transport protocol type*
- *Traffic port number*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*Administrator, Audit Admin, Crypto Admin, HAProfile, Custom, and Security Admin*].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.
Dependencies: No dependencies

6.2.7 Class FTA: TOE Access

FTA_SSL.1 TSF-initiated session locking

Hierarchical to: No other components.

FTA_SSL.1.1

The TSF shall lock an interactive session after a [*configurable time interval of authorized administrator inactivity at the Web Admin Console from 1 to 99 minutes, defaulting to 3 minutes*] by:

a) Clearing or overwriting display devices, making the current contents unreadable;

b) Disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: [*authorized administrator must re-enter password*].

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*configurable time interval of administrator inactivity at the Web Admin Console from 1 to 99 minutes, defaulting to 10 minutes*].

Dependencies: No dependencies

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an authorized administrator-specified advisory warning message regarding unauthorized use of the TOE.

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL4 augmented with ALC_FLR.2. Table 11 – Assurance Requirements summarizes the requirements.

Table 11 – Assurance Requirements

Assurance Requirements	
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

7 TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 12 lists the security functionality and their associated SFRs.

Table 12 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	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
Protection of TOE Security Functions	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.1	TSF-initiated session locking
	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit records. As administrators manage and configure the TOE, their activities are tracked by recording audit records into the logs. All security-relevant configuration changes are recorded to ensure accountability of the administrator's actions. All logs contain the time, device, type of event, log ID, and priority. Firewall log files additionally contain component, action, username, firewall rule, incoming interface, outgoing interface, source IP, and destination IP.

The TOE generates log files with information about security related events for administrator review to monitor network security and activity, identify security risks, and address these risks. These events are maintained in the local logs until the system is shutdown or rebooted. Records are also sent to an external syslog server, which maintains and stores the audit records.

A log file is a list of events, along with information about those events. An event is an activity that occurs on the TOE. For example, TOE's denying of a packet based on a policy set is an event. The TOE also captures information about allowed events to give a more complete picture of the activities on the network.

The TOE audit events are generated in the form of logs which are generated and saved in several types of log messages. The log message types are:

- Firewall rules – Log records of the entire traffic for firewall
- Invalid traffic log – Log records of the dropped traffic that do not follow the protocol standards, invalid fragmented traffic, and traffic whose packets the TOE is not able to relate to any connection
- Administration log – Administrator logins and changes to configuration parameters and access rules

The TOE administrator has the ability to view all audit events generated since the last system reboot on the local audit logs, as well as search and sort the audit data. Audit events that precede a system power loss can only be viewed on the external syslog server. This includes the audit record of the shutdown of the audith function. The local logs can be searched based on common fields for all events, as well as access firewall rule fields. They can be sorted and ordered based on any of the fields listed in Table 13 below. The TOE protects the stored audit records from unauthorized deletion and modification.

The TOE audit records contain the following information:

Table 13 – Common Fields

Field	Content
Date	Date (yyyy-mm-dd) when the event occurred
Time	Time (hh:mm:ss) when the event occurred
Timezone	Time zone of Cyberoam Appliance
Device_name	Model Number of the Cyberoam Appliance (syslog only)
Device_id	Unique Identifier of the Cyberoam Appliance (syslog only)
Log_id	Unique 12 characters code (syslog only)
Log_type	Type of event occurred in Cyberoam
Log_component	Component responsible for logging
Log_subytpe	Sub type of event occurred in Cyberoam
Priority	Severity level of the event

Field	Content
Message_id	Message identifier for event (local logs only)

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1.

7.1.2 User Data Protection

The security policy of an organization in the context of computer networking is a set of rules to protect the computer networks of an organization and the information that goes through it. By default, the TOE denies all packets that are not specifically allowed. The TOE enables the administrator of the TOE to add a policy. Through the use of policies, the administrator configures a set of firewall rules that tell the TOE to allow or deny traffic based upon factors such as source and destination of the packet, port number, as well as the transport protocol type. Transport protocol that can be filtered are TCP and UDP.

The User Data Protection function implements functionality for TOE security functions and TOE security functional policies related to protecting user data. The user data that the TOE is protecting is the information passing through the TOE. This functionality is provided by the application of firewall access rules. The Traffic Information Flow Control Security Functional Policy enforces rules on subjects that send traffic through the TOE, or receive traffic flowing through the TOE. The rules in the security policy determine whether traffic should be accepted from the sender to the receiver, passage rejected, or dropped based on the following security attributes: source IP address, destination IP address, port number, and TCP and UDP protocols.
TOE Security Functional Requirements Satisfied: FDP_IFC.1, FDP_IFF.1.

7.1.3 Identification and Authentication

The Identification and Authentication functionality establishes and verifies a claimed user's identity. The TOE requires successful identification and authentication of all users before allowing access to any management functionality of the Web Admin Console. This ensures that the user has the appropriate privileges associated with the assigned profile. Only authenticated users are allowed access to the TOE and TOE security functions. Users must be identified and authenticated prior to performing any TSF-mediated actions on the TOE. For each user, the TOE stores the following security attributes locally: username, password, and profile. When a TOE user enters a username and password at the Web Admin Console, the information is passed to the TOE, where it is verified against the username and password stored in the TOE. If the provided username and password match, the TOE administrator is assigned the roles associated with that username.

The TOE will lock out all user accounts from an IP address if a user fails to enter the proper credentials after an administrator-configurable number of failed login attempts.
TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_UAU.2, FIA_UID.2.

7.1.4 Security Management

The Security Management function specifies the management of several aspects of the TSF, including security function behavior and security attributes. The TOE provides two built-in administrative accounts: *admin* and *cyberoam*. Both these accounts have default passphrases pre-supplied for them, which must be changed during the initial configuration and both fall into the Administrator profile. The TOE allows administrators to create profiles for various administrator users. Profiles are a function of an organization's security needs and can be set up for special-purpose administrators in areas such as firewall administration, network administration, and logs administration. A profile separates the TOE's features into access control

categories for which an administrator can enable none, read only, or read-write access. Profiles created by an administrator fall in the Custom role. By default, the TOE provides the following five profiles:

- Administrator – super administrator with full privileges
- Audit Admin – read-write privileges for Logs & Reports only
- Crypto Admin – read-write privileges for Certificate configuration only
- HAProfile – read-only privileges. This role is assigned to Administrators accessing the Web Admin Console when HA is configured. HA is not configured in the evaluated configuration, so this role will not be assigned.
- Security Admin – read-write privileges for all features except Profiles and Log & Reports

Adding or deleting rules in the Traffic Information Flow Control SFP (i.e. accept, reject, or discard) is limited only to the Administrator or Security Admin roles.

The TOE provides restrictive default values for the Traffic Information Flow Control SFP security attributes, and allows only the Administrator or Security Admin to set different values. Also, specifying alternative initial values for security attributes to override the default values is limited to Administrator and Security Admin profiles.
TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE firmware maintains a reliable timestamp through function calls to the underlying hardware for audit messages and applications within the TOE.
TOE Security Functional Requirements Satisfied: FPT_STM.1

7.1.6 TOE Access

The TOE Access function specifies requirements for controlling the establishment of an administrator's session, which is configured by Administrator roles with sufficient permission level. The TSF locks an administrator's interactive session after a configurable time interval of administrator inactivity at the Web Admin Console, the default time interval is 3 minutes. The session is terminated after a configurable time interval of administrator inactivity at the Web Admin Console, the default time interval is 10 minutes. If an administrator's session is timed out, the administrator must log back in to the TOE to perform any further functions.

An Administrator or Security Admin can configure the TOE to display an advisory warning message regarding unauthorized use of the TOE before an authentication session occurs.
TOE Security Functional Requirements Satisfied: FTA_SSL.1, FTA_SSL.3, FTA_TAB.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 14 below provides a mapping of the objects to the threats they counter.

Table 14 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.AUDACC TOE users or an attacker may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.	O.ACCOUNT The TOE must provide accountability for information flows through the TOE and for TOE users' use of security functions related to audit.	The O.ACCOUNT objective addresses the T.AUDACC threat by requiring the TOE to provide accountability for information flows through the TOE and for TOE users' use of security functions related to audit.
	O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means for TOE users to search, sort, and order the audit trail based on relevant attributes.	The O.AUDREC objective addresses the T.AUDACC threat by requiring the TOE to provide a readable audit trail of security-related events, thereby allowing an Administrator or Audit Admin to discover attacker actions.
	O.TIME The TOE must provide a reliable time stamp.	The O.TIME objective addresses the T.AUDACC threat by requiring the TOE to provide reliable timestamps for use in audit records. An Administrator, or Audit Admin may use the audit records to identify attacker actions.
T.MEDIAT An attacker may send impermissible information through the TOE which results in the exploitation of resources on the internal network.	O.MEDIATE The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.	The O.MEDIATE objective addresses the T.MEDIAT threat by ensuring that the TOE mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.

Threats	Objectives	Rationale
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.	O.AUTHENTICATE The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials.	The O.AUTHENTICATE objective addresses the T.NOAUTH threat by requiring that the TOE uniquely identify and authenticate the claimed identity of all TOE users before granting access to TOE functions and data, or to a connected network.
	O.LIMEXT The TOE must provide the means for TOE users to control and limit access to TOE security functions by an authorized external IT entity.	The O.LIMEXT objective addresses the T.NOAUTH threat by requiring the TOE to provide a means for TOE users to control and limit access to TOE security functions by an authorized external IT entity.
	O.SECFUN The TOE must provide functionality that enables TOE users to use the TOE security functions, and must ensure that only TOE users are able to access such functionality.	The O.SECFUN objective addresses the T.NOAUTH threat by requiring the TOE to provide functionality that enables TOE users to use the TOE security functions, and ensure that only authenticated TOE users are able to access such functionality.
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.	O.AUTHENTICATE The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network. The TOE must ensure that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials.	The O.AUTHENTICATE objective addresses the T.REPEAT threat by requiring the TOE to provide functionality that enables TOE users to block a login session after a configurable number of failed login attempts from the same IP.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no organizational security policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 15 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 15 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	NOE.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	The NOE.GENPUR objective ensures that 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.	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.TRAFFIC upholds this assumption by ensuring that the environment provides the TOE with the appropriate network configuration to perform its intended function.
A.NOEVIL TOE users are non-hostile and follow all administrator guidance.	NOE.NOEVIL TOE users are non-hostile and follow all administrator guidance.	The NOE.NOEVIL objective ensures that TOE users are non-hostile and follow all administrator guidance.
A.PHYSEC The TOE is physically secure.	NOE.PHYSEC The physical environment must be suitable for supporting a computing device in a secure setting.	The NOE.PHYSEC objective ensures that the TOE is physically secure.
A.PUBLIC The TOE does not host public data.	NOE.PUBLIC The TOE does not host public data.	The NOE.PUBLIC objective ensures that the TOE does not host public data.
A.REMACC TOE users may only access the TOE locally.	NOE.REMACC TOE users may only access the TOE locally.	The NOE.REMACC objective ensures that 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.	NOE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.	The NOE.SINGEN objective ensures that information cannot flow among the internal and external networks unless it passes through the TOE.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended Security Functional Requirements in this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE Security Assurance Requirements in this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 16 below shows a mapping of the objectives and the SFRs that support them.

Table 16 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means for TOE users to search, sort, and order the audit trail based on relevant attributes.	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 meets this objective by providing an audit trail listing all security-relevant actions on the TOE and on the information passing through the TOE.
	FAU_SAR.1 Audit review	FAU_SAR.1 meets this objective by ensuring that an Administrator or Audit Admin are able to read and interpret all audit information from the audit records.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 meets this objective by ensuring the an Administrator or Audit Admin can search, sort, and order the audit data based on time, log comp, action, username, Firewall rule, in interface, out interface, source IP, and destination IP.
	FAU_STG.1 Protected audit trail storage	FAU_STG.1 meets this objective by ensuring the TOE restricts the ability to modify or delete the audit trail to an Administrator or Audit Admin and to detect any such behavior by auditing all management operations.
	FPT_STM.1 Reliable time stamps	FPT_STM.1 meets this objective by ensuring the TOE provides a reliable time stamp.
O.AUTHENTICATE The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network. The TOE must ensure that TOE users	FIA_AFL.1 Authentication failure handling	FIA_AFL.1 meets this objective by ensuring that TOE users cannot endlessly attempt to login and authenticate with the wrong credentials. After some configurable number of failed login attempts from the same IP, the IP address is blocked from authenticating again.

Objective	Requirements Addressing the Objective	Rationale
cannot endlessly attempt to login and authenticate with the wrong credentials.	FIA_UAU.2 User authentication before any action	FIA_UAU.2 meets this objective by requiring that all TOE users be successfully authenticated before allowing any other TSF-mediated actions on behalf of those TOE users.
	FIA_UID.2 User identification before any action	FIA_UID.2 meets this objective by requiring that all TOE users be successfully identified before allowing any other TSF-mediated actions on behalf of those TOE users.
O.LIMEXT The TOE must provide the means for TOE users to control and limit access to TOE security functions by an authorized external IT entity.	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 meets this objective by restricting the ability to access and perform security functions to TOE users with sufficient permission level.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 meets this objective by requiring that the TOE provides specification of Management Functions for TOE users.
O.MEDIATE The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.	FDP_IFC.1 Subset information flow control	FDP_IFC.1 meets this objective by specifying the rules by which subjects will accept, reject, or drop information to flow to and from other subjects.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 meets this objective by specifying the rules by which subjects will accept, reject, or drop information to flow to and from other subjects.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 meets this objective by enforcing the Traffic Information Flow Control Security Functional Policy, which restricts the ability create or delete security attributes in the Traffic Information Flow Control List to an Administrator or Security Admin.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 meets this objective by ensuring that the Traffic Information Flow Control Security Functional Policy has a permissive default policy that can be changed only by an Administrator or Security Admin.

Objective	Requirements Addressing the Objective	Rationale
O.SECFUN The TOE must provide functionality that enables TOE users to use the TOE security functions, and must ensure that only TOE users are able to access such functionality.	FIA_UAU.2 User authentication before any action	FIA_UAU.2 meets this objective by requiring that all TOE users be successfully authenticated before allowing any other TSF-mediated actions on behalf of those TOE users.
	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 meets this objective by restricting access and performance of TOE security functions to TOE users with sufficient permission level.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 meets this objective by enforcing the Traffic Information Flow Control Security Functional Policy, which restricts the ability to create or delete security attributes in the Traffic Information Flow Control List to Administrator or Security Admin.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 meets this objective by enforcing the Traffic Information Flow Control Security Functional Policy to provide restrictive default values for security attributes.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 meets this objective by requiring that the TOE provides specification of Management Functions for TOE users.
	FMT_SMR.1 Security roles	FMT_SMR.1 meets this objective by defining the permission levels available to TOE users.
	FTA_SSL.1 TSF-initiated session locking	FTA_SSL.1 meets the objective by ensuring that the TOE restricts TOE users gaining access to the TOE by configuring a settable number of unsuccessful login attempts for the TOE users' accounts, before they are locked out.

Objective	Requirements Addressing the Objective	Rationale
	FTA_SSL.3 TSF-initiated termination	FTA_SSL.3 meets this objective by terminating an interactive session after a configurable time interval of TOE user inactivity at the Management Console. The TOE users must then login again to access the TOE.
	FTA_TAB.1 Default TOE access banners	FTA_TAB.1 meets this objective by allowing the Administrator or Security Admin to configure the TOE by displaying an access banner warning against unauthorized access.
O.TIME The TOE must provide a reliable time stamp.	FPT_STM.1 Reliable time stamps	FPT_STM.1 meets this objective by ensuring the TOE provides a reliable time stamp.

8.5.2 Security Assurance Requirements Rationale

EAL4+ was selected because it is best suited to addressing the stated security objectives. EAL4+ challenges vendors to use best (rather than average) commercial practices. EAL4+ allows the vendor to evaluate their product at a detailed level, while still benefitting from the Common Criteria Recognition Agreement. The chosen assurance level is appropriate for the threats defined in the environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation process.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 17 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 17 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FMT_MSA.3	✓	
	FDP_IFC.1	✓	
FIA_AFL.1	FIA_UID.1	NO	Although FIA_UID.1 is

SFR ID	Dependencies	Dependency Met	Rationale
			not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UAU.2	FIA_UID.1	NO	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	Not applicable	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_IFC.1	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_SMF.1	No dependencies	Not applicable	
FMT_SMR.1	FIA_UID.1	NO	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_STM.1	No dependencies	Not applicable	
FTA_SSL.1	FIA_UAU.1	NO	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FTA_SSL.3	No dependencies	Not applicable	
FTA_TAB.1	No dependencies	Not applicable	

9 Acronyms

This section and Table 18 define the acronyms used throughout this document.

Table 18 – Acronyms and Terms

Acronym	Definition
3G	Third Generation
CC	Common Criteria
CD	Compact Disk
CLI	Command Line Interface
CM	Configuration Management
DdoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DoS	Denial of Service
EAL	Evaluation Assurance Level
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IM	Instant Messengers
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
Ipv6	Internet Protocol Version 6
IT	Information Technology
KVM	Kernel-based Virtual Machine
L2	Layer 2
L2TP	Layer 2 Tunneling Protocol
L7	Layer 7
L8	Layer 8
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol

Acronym	Definition
MAC	Media Access Control
NTP	Network Time Protocol
OS	Operating System
PDF	Portable Document Format
POP3	Post Office Protocol 3
PP	Protection Profile
PPPoE	Point-to-point over Ethernet
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UPS	Uninterruptible power supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com