Websense, Inc.

V10000 G2 Web Gateway Appliance v7.6

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.0

Prepared for:

Websense, Inc.

10240 Sorrento Valley Road
San Diego, CA 92121
United States of America

Phone: +1 800 723 1166
Email: info@websense.com
http://www.websense.com

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

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 Target of Evaluation (TOE) is the Websense V10000 G2 Web Gateway Appliance v7.6, and will hereafter be referred to as the TOE throughout this document. The TOE is a web proxy and traffic filter with real-time threat scanning. The TOE can block or allow user traffic to various websites or protocols based on the categorization of the website or protocol and the policies defined on the TOE.

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 functions 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 Summary 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 - ST and TOE References

ST Title	Websense, Inc. V10000 G2 Web Gateway Appliance v7.6 Security Target
ST Version	Version 1.0
ST Author	Corsec Security, Inc.
ST Publication Date	2011-12-22
TOE Reference	Websense V10000 G2 Web Gateway Appliance v7.6
Keywords	Proxy, filter, web, protocol, V10000 G2, Websense.

1.3 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 V10000 G2 Web Gateway Appliance is a protocol filtering appliance that provides two major features: web proxy and traffic filtering. Web proxy allows the TOE to inspect web content accessed by users and determine if it is malicious or undesirable. Traffic filtering allows the TOE to inspect non-web traffic in order to determine whether the traffic should be allowed or not, based on the protocol. Web proxy and traffic filtering work together to prevent security breaches, productivity loss, and legal issues that might arise due to inappropriate or careless browsing and network usage habits.

1.3.1 Web Proxy

Web proxy offers three features to help prevent users from accessing unwanted web content: dynamic script inspection, script filtering, and content classification.

Dynamic script inspection allows the TOE to inspect scripts in real-time to determine if they contain known malicious code. If malicious code is found within proxy content, then the TOE can block access to that content to prevent a security breach.

Script filtering is used when malicious code is found within proxy content, but instead of blocking access the TOE removes only the malicious content. This is useful if a site contains useful content, but has been compromised in some way, since the useful content can still be accessed while denying access to malicious scripts. This feature is particularly applicable to Web 2.0 sites, which allow custom user-generated content that may include malicious code.

Content classification allows administrators to use predefined or custom content classifications to block or limit access to certain categories of content, such as adult or political websites. The default list of categories includes:

- Security Filtering – includes sites that host botnets, keyloggers, phishing scams, etc.
- Bandwidth Categories – includes sites that host Internet radio and television, peer-to-peer file sharing, streaming media, etc.
- Productivity Categories – includes sites that host advertisements, freeware and software downloading, instant messaging, etc.
- Abortion – includes sites that host content related to abortion.
- Adult material – sites that contain full or partial nudity or sexual content, lingerie and swimsuit models, or sex education.
- Advocacy Groups – includes sites that promote change or reform in various aspects of public policy, public opinion, social practice, economic activities, or relationships.
- Business and Economy – includes sites that are sponsored by or devoted to business firms, financial and investment sites, and business-oriented web applications.
- Drugs – sites that contain information on legal and illegal drugs.

There are many other categories included in the full list. The entire list of default content categories can be found at: http://www.websense.com/content/URLCategories.aspx.

In addition to the default categories, administrators can define custom categories and assign Uniform Resource Locators (URLs) to these categories manually. This allows easy classification of localized content that may not have been classified yet by Websense.

1.3.2 Traffic Filtering

Traffic (or protocol) filtering works by inspecting the port of user traffic to determine if it matches one of the ports used by restricted protocols. If a protocol is restricted, the TOE blocks the connection. Protocols can be included in predefined protocol groups such as:

- Database – protocols that enable the creation and manipulation of structured sets of information.

- File Transfer – protocols that enable user control over the transfer of files across a network.
- Instant Messaging/Chat – protocols that enable sending and receiving synchronous, real-time messages.

There are many other protocol categories that can be blocked. The full list of protocol categories can be found at: http://www.websense.com/content/ProtocolCategories.aspx.

As with content categories, administrators can define custom protocol groups to be monitored and filtered by the TOE. This allows administrators to control protocols that might not fit into one of the predefined categories, but needs to be controlled on the local network.

1.3.3 Policy Enforcement and Management

Web based management consoles, located on the appliance provide administrators with access to manage various components of the TOE. Administrators can use one of the following web Graphical User Interfaces (GUIs) to connect to the consoles over an HTTPS connection:

- The Appliance Manager GUI is the management user interface used for configuring appliance settings, such as default gateway or hostname.

- The Content Gateway Manger GUI is the management user interface used for configuring proxy settings such as cache size or authentication methods.

- The Triton GUI is the management interface used to for customizing filtering behavior such as configuring proxy filtering rules.

In addition to the web GUIs, the TOE provides administrators with access to a Command Line Interface (CLI). Administrators can connect using the serial port or the monitor and keyboard ports directly on the appliance to access an installation (local) CLI. In general, the installation CLI is only used during the initial setup of the TOE to run a script which prepares the appliance for remote administration. Administrators may also access the CLI remotely using SSH[1] . The CLI provides the same functionally when accessed locally or remotely and offers limited management functionality compared to the web GUIs.

Web proxy and traffic filtering functionality can perform multiple operations on controlled traffic in addition to basic block and allow operations. Advanced operations include:

- Bandwidth – the TOE evaluates the current bandwidth usage against a threshold set for the category, and blocks the connection if the threshold is met or exceeded.
- Confirm – the traffic is blocked until the user confirms that the site is being used for business purposes.
- Quota – the user is presented with a block page asking them whether to use quota time to view the site. Quota time is a preset amount of time assigned to the user each day.
- Block Keywords – if a site URL contains one of the defined keywords then access is blocked.
- Block File Types – if a file contains one of the defined extensions then access access is blocked.

Administrators control the web proxy and traffic filtering functionality via policy. Administrators define and apply policy rules via the Triton web Graphical User Interface (GUI). Policy can be applied to all network traffic, or administrators can define groups of clients (users) or individual clients and apply policies on a group or individual basis. The TOE can be configured to discovers clients by searching for them on a remote directory server, such as Active Directory. User information is copied from the directory into an internal database for use in policy definition and enforcement.

[1] Secure Shell Server

The Triton web GUI provides an interface that allows administrators to manage TOE settings, policy, and audit records. Triton presents management functionality as a series of screens with web form elements that administrators can fill in. Administrators can connect remotely to the Triton GUI over an Internet Protocol (IP) network. In addition to the Triton GUI, the TOE allows administrators to access an installation Command Line Interface (CLI), administrators can connect locally to the CLI via KVM or Series Port cable. The installation CLI is used to configure network settings such as host name and IP address during the initial setup of the TOE. The TOE also provides an Appliance Manager GUI that administrators can use to manage system settings, such as default gateway or hostname, and a Content Management GUI that allows administrators to configure proxy settings such as cache size or authentication methods.

Figure 1 shows the details of the deployment configuration of the TOE:

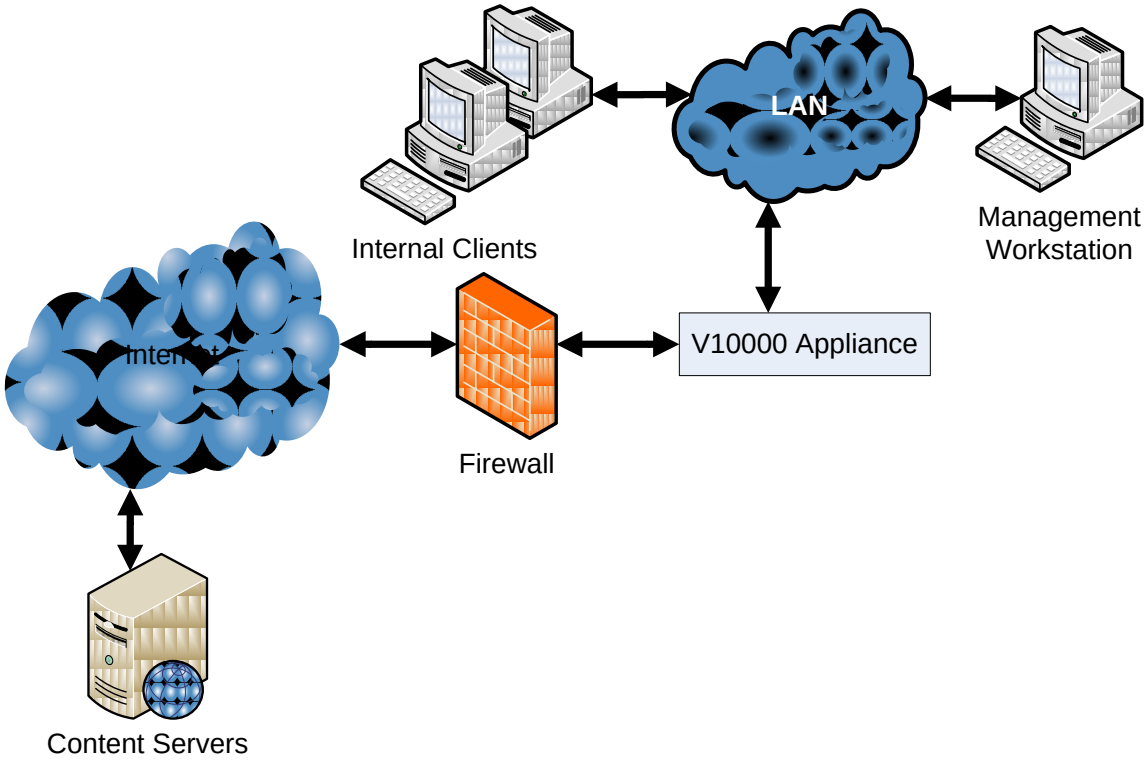

Figure 1 - Deployment Configuration of the TOE

1.3.4 TOE Environment

The TOE is intended to be deployed in a physically-secured cabinet room, room, or data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). Access to the physical console or USB ports on the appliance should be restricted via a locked data cabinet within the data center. The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE provides a layer of security between an internal and external network (such as between a Local Area Network (LAN) and the Internet). The TOE is meant to control, protect, and monitor the internal network's access to content on the external network. For this behavior to be properly implemented, all controlled protocol traffic must traverse the TOE. The TOE environment is required to provide the necessary configuration to allow this.

1.4 TOE Description

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

1.4.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a proxy filter application that runs on the G2 version of the V10000 appliance as depicted in the figure below. The appliance hardware is a standard Dell R610 server running a customized version of the CentOS[2] Linux operating system. All of the essential physical components in the evaluated configuration are located on the TOE which include:

- Application software,
- Operating system, and
- Appliance hardware.

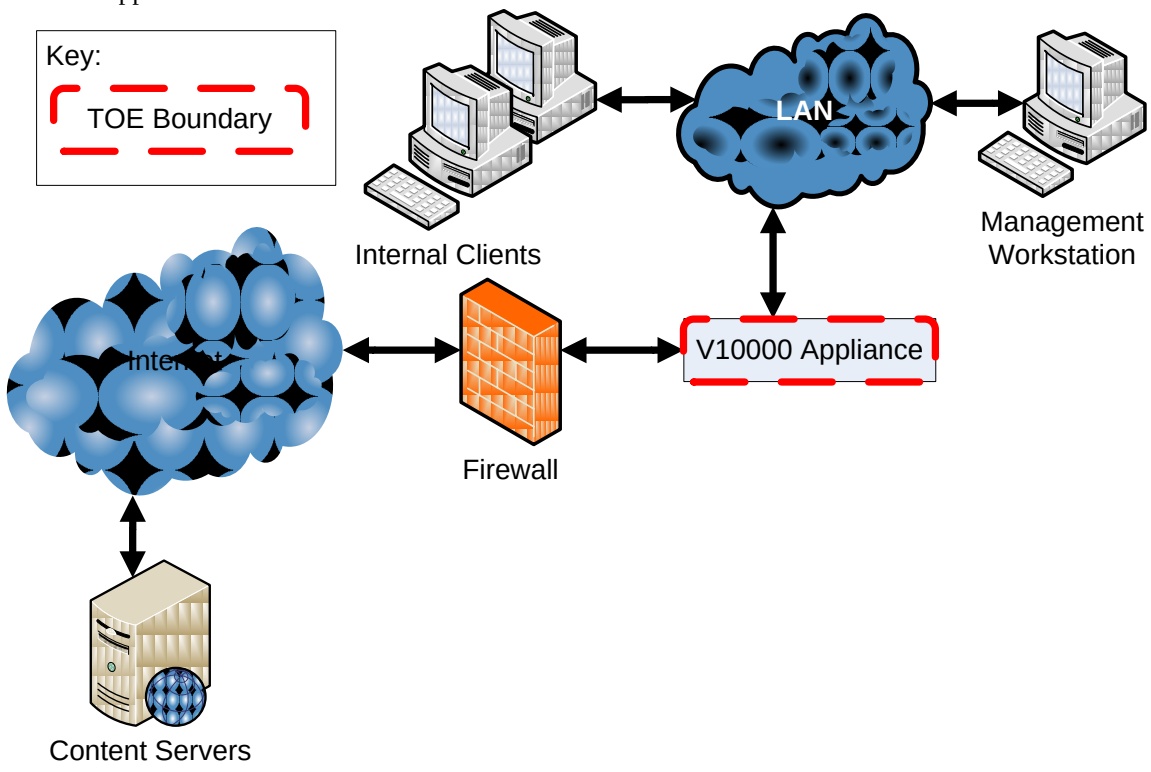

Figure 2 - Physical TOE Boundary

1.4.1.1 TOE Requirements

The TOE is a combination hardware appliance and software application suite that provides proxy filtering capabilities.

[2] Community Enterprise Operating System

1.4.1.2 Guidance Documentation

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

- Websense Content Manager Help v7.6
- Websense TRITON – Web Security Help v.76
- Websense Appliance Manager Help v7.6
- Websense Release Notes for TRITON Unified Security Centerv7.6
- Websense Quick Start Guide V10000 G2

1.4.2 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 TSF[3],
- Resource Utilization, and;
- TOE Access

1.4.2.1 Security Audit

The TOE enforces the ability to generate audit records for administrator login attempts, policy changes, and configuration changes. The TOE also audits the startup and shutdown of the audit function[4]. Only Super Administrators can review the audit records and select the types of events to record.

1.4.2.2 User Data Protection

The TOE enforces a Proxy Filtering Policy on internal Information Technology (IT) entities attempting to access content hosted on the external network. The Proxy Filtering Policy prevents internal entities from accessing potentially harmful or inappropriate content based on a set of administrator-defined rules.

The TOE also permits rollback of changes to its internal database.

1.4.2.3 Identification and Authentication

The TOE enforces identification and authentication for administrators before they can access any management functionality besides the installation CLI. Administrators who fail to provide valid credentials after attempting to login via the web GUIs must wait five seconds before being able to attempt to log in again.

The TOE also prevents users from accessing content before providing and authenticating a valid identity. The TOE maintains a list of security attributes (such as login credentials) for users and administrators.

[3] TSF – TOE Security Functionality

[4] The TOE does not offer the option to shut down or restart the audit system under normal operating conditions. The audit system is considered to be always invoked when the TOE is active.

1.4.2.4 Security Management

The TOE provides robust management interfaces that authorized administrators can use to manage the TOE and configure policies to control access to content. By default proxy filtering is enabled, but all traffic is allowed; therefore, the TOE has a permissive default posture.

The TOE defines two roles — Super Administrator and Delegated Administrator — and can associate users with roles. Delegated Administrators can have custom permission sets.

Administrators can log into the TOE and view real-time management data within the 'Today', 'History', and 'Alerts' pages without being logged out. After thirty minutes on one of these pages, if the administrator attempts to navigate to any other page, the TOE will force the administrator to log in again before continuing.

1.4.2.5 Protection of the TSF

The TOE provides reliable timestamps to accurately record the sequence of events within the audit records.

During a failure where the category database license key fails to be updated on schedule, the TOE is still capable of enforcing the Proxy Filtering Policy for fourteen days before the database is shut down. If the category database shuts down then the TOE is unable to continue enforcing policy rules on traffic.

1.4.2.6 Resource Utilization

The TOE can recover from a failure where the category database license key fails to be updated on schedule. If the license key is loaded within fourteen days, a complete database shutdown will be avoided.

The TOE enforces maximum limits on usage and availability of controlled traffic.

1.4.2.7 TOE Access

The TOE can assign a limit on the number of concurrent sessions that users are allowed to have. If this limit is reached, the TOE prevents any new sessions from being created.

The TOE terminates administrative sessions after 30 minutes of inactivity.

1.4.3 Product Physical/Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Data Security
- Email Security

2 Conformance Claims

This section provides 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 2 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 2010-10-15 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ 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 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 a low 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. The IT assets requiring protection are the TSF 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. The following threats are applicable:

Table 3 - Threats

Name	Description
T.EXTERNAL_CONTENT	A user or process on the internal network may access or post content to an external network that has been deemed inappropriate or potentially harmful to the internal network.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.NACCESS	An unauthorized person or external IT entity may be able to view or modify TOE data by hijacking an unattended administrator session.
T.UNAUTHORIZED_ACCESS	A user may gain access to security data on the TOE that they are not authorized to access.
T.RESOURCE	TOE users or attackers may cause network connection resources to become overused and therefore unavailable.
T.DB_FAILURE	A TOE user or attacker may cause the TOE's internal database to fail or become corrupted.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this ST.

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. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 4 - Assumptions

Name	Description
A.INSTALL	The TOE has been installed and configured according to the appropriate installation guides.
A.NETWORK	All Proxy Filtering Policy-controlled traffic between the internal and external networks traverses the TOE.
A.LOCATE	It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.
A.NOEVIL	It is assumed that administrators who manage the TOE are not careless, negligent, or willfully hostile; are appropriately trained; and follow all guidance.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.EXCLUSIVE	All administrative interfaces are not accessible to non-administrators and only administrators have access to the administrative interfaces to ensure the network is secure.

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 as follows:

Table 5 – Security Objectives for the TOE

Name	Description
O.AUTHENTICATE	The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their controlled protocol traffic matches a Proxy Filtering Policy rule that requires user authentication.
O.AUDIT	The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record the resulting actions of the Proxy Filtering Policy and allow trained administrators to review security-relevant audit events.
O.MANAGE	The TOE must provide secure management of the system configuration and the Proxy Filtering Policy over one or more concurrent sessions.
O.RESOURCE_CONTROL	The TOE must control access to network resources as defined by the Proxy Filtering Policy.
O.QUOTA	The TOE must be able to place quotas on network connection resources.
O.TIMESTAMP	The TOE must provide a timestamp for its own use.
O.HARMFUL_CONTENT	The TOE must disallow access to malicious content hidden within legitimate network resource requests for controlled protocol traffic.
O.DB_RESILIENCY	The TOE must be resilient against the potential failure of its internal database.
O.PROTECT	The TOE must have the capability to protect management traffic from unauthorized reading or modification.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 6 – IT Security Objectives

Name	Description
OE.NETWORK	All Proxy Filtering Policy-controlled protocol traffic between the internal and external network must traverse the TOE.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives 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 7 – Non-IT Security Objectives

Name	Description
NOE.ADMIN	The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.
NOE.LOCATE	The physical environment must be suitable for supporting a computing device in a secure setting.

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

This section specifies the extended SFR for the TOE. The extended SFR is organized by class. Table 8 identifies the extended SFR implemented by the TOE.

Table 8 – Extended TOE Security Functional Requirements

Name	Description
EXT_FDP_ROL	Rollback of TOE configurations

5.1.1 Class FDP: User Data Protection

Families in this class address the requirements for specifying requirements related to protecting user data.

The extended family "EXT_FDP_ROL: Rollback of TOE configurations" was modeled after FDP_ROL.

5.1.1.1 Rollback of TOE configurations (EXT_FDP_ROL)

Family Behavior

This family defines the set of rules which the V10000 G2 Web Gateway Appliance v7.6 uses to rollback configuration changes, policy rules, and setting.

Component Leveling

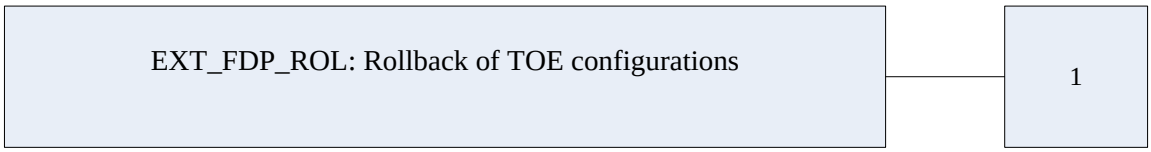

Figure 3 – EXT_FDP_ROL Rollback of TOE configurations family decomposition

EXT_FDP_ROL Rollback of TOE configurations, defines the set of rules which the V10000 G2 Web Gateway Appliance v7.6 uses to rollback TOE configuration changes, proxy-filtering policy rules, and TOE settings. It was modeled after FDP_ROL.2

EXT_FDP_ROL Rollback of TOE configurations

Hierarchical to: No other components

Dependencies: No Dependency

Rollback of TOE configurations defines the type of operations that are permitted to be rolled back.
EXT_FDP_ROL The TSF shall permit the rollback of all the operations on the

A. **)[assignment: TOE *configuration changes, proxy-filtering policy rules, and TOE settings*].**

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

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(a)	Audit Data Generation	✓	✓		✓
FAU_GEN.1(b)	Audit Data Generation	✓	✓		✓
FAU_SAR.1(a)	Audit review		✓		✓
FAU_SAR.1(b)	Audit review – Event Log		✓		✓
FAU_SAR.2	Restricted audit review				
FAU_SEL.1	Selective audit	✓	✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
EXT_FDP_ROL	Rollback of TOE configurations		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓	✓	
FIA_UAU.1	Timing of authentication		✓	✓	
FIA_UAU.2	User authentication before any action				

Name	Description	S	A	R	I
FIA_UID.1	Timing of identification		✓	✓	
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SAE.1	Time-limited authorisation		✓		
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1	Security roles		✓	✓	
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_STM.1	Reliable time stamps				
FRU_FLT.2	Limited fault tolerance		✓		
FRU_RSA.1(a)	Maximum quotas	✓	✓		✓
FRU_RSA.1(b)	Maximum quotas	✓	✓		✓
FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions		✓		
FTA_SSL.3	TSF-initiated termination		✓	✓	

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1(a) Audit Data Generation – Access Log
Hierarchical to: No other components.
FAU_GEN.1.1a

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) [*successful administrator logins, policy changes, selective URL categories, and configuration changes*].

FAU_GEN.1.2a

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, [*server affected by the change (IP address) and role affected*].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: The TOE does not offer the option to shut down or restart the audit system under normal operating conditions. The audit system is considered to be always invoked when the TOE is active.

FAU_GEN.1(b) Audit Data Generation – Event Log
Hierarchical to: No other components.
FAU_GEN.1.1b

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

d) Start-up and shutdown of the audit functions;
e) All auditable events, for the [not specified] level of audit; and
f) [*administrator login attempts and content classification database updates*].

FAU_GEN.1.2b

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

c) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
d) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no additional information*].

Dependencies: FPT_STM.1 Reliable time stamps

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

The TSF shall provide [*Super Administrators*] with the capability to read [*all audit data*] from the audit records.

FAU_SAR.1.2a

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.1(b) Audit review – Event Log
Hierarchical to: No other components.

FAU_SAR.1.1b

The TSF shall provide [*Super Administrators, Delegated Administrators*] with the capability to read [*all audit data as specified by FAU_GEN.1(a)*] from the audit records.

FAU_SAR.1.2b

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.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [subject identity]
b) [*selective URL categories*].

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1
The TSF shall enforce the [*Proxy Filtering Policy*] on
[
1. *Subjects: internal IT entities*
2. *Objects: external IT entities hosting content*
3. *Operations: retrieving hosted content*

].
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Proxy Filtering Policy*] to objects based on the following:
[
Subject attributes:
1. *User name*
2. *User group*
3. *IP address*
4. *Quotas for Access*

Object attributes:
1. *Assigned category*
2. *IP address*
3. *URL*
4. *Protocol*
5. *Keywords*
6. *Web Objects*

].
FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
1. *If a bandwidth usage quota is defined for the category or protocol, evaluate the current bandwidth:*
   a. *If the bandwidth currently in use is below the defined threshold for the category or protocol, allow access to the content.*
   b. *If the bandwidth currently in use is above or at the defined threshold for the category or protocol, deny access to the content.*
2. *If a "block" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "block page".*
3. *If a "permit" rule is defined for the category or protocol group, allow access to the content.*
4. *If a "confirm" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "confirmation page" until the user confirms that the access is for business-related purposes.*
5. *If a "quota" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "quota confirmation page". If the user agrees to continue to the content, begin the quota timer for the user.*

6. *If a "block keywords" rule is defined for the category, deny access to the content if the keyword or keywords are present within the content, and redirect the user to the "block page".*
7. *If a "block file types" rule is defined for the category, deny access to the content, and redirect the user to the "block page".*
8. *If malicious content is hidden within a web object, block access to the malicious content, while allowing access to the legitimate content.*
9. *If no rule is defined for the content, allow access to the content*

].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*if a "quota" rule is defined and a user has no more browsing quota, the TOE denies access to the user and shows the "block" page*].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

EXT_FDP_ROL Rollback of TOE Configurations

Hierarchical to: No other components

EXT_FDP_ROL

The TSF shall permit the rollback of all the operations on the [*configuration changes, policy rules, and TOE settings*].

Dependencies: No dependencies

6.2.3 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 [*one*] unsuccessful authentication attempts occur related to [*authenticating with the web interface*].
FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*delay future login attempts for five seconds*].
Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **administrators**: [*user name, role, password*].
Dependencies: No dependencies

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
FIA_UAU.1.1
The TSF shall allow [*access to the installation CLI*] on behalf of the ~~user~~ **administrator** to be performed before the ~~user~~ **administrator** is authenticated.
FIA_UAU.1.2
The TSF shall require each ~~user~~ **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.
Dependencies: FIA_UID.1 Timing of identification

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.1 Timing of identification
Hierarchical to: No other components.
FIA_UID.1.1
The TSF shall allow [*access to the installation CLI*] on behalf of the ~~user~~ **administrator** to be performed before the ~~user~~ **administrator** is identified.
FIA_UID.1.2
The TSF shall require each ~~user~~ **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.
Dependencies: No dependencies

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

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1
The TSF shall restrict the ability to [disable, enable, modify the behaviour of] the functions [*filter components, protocol filter rules, category filter rules*] to [*authorised Super Administrators and authorised Delegated Administrators*].
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 [*Proxy Filtering Policy*] to restrict the ability to [create, change default, query, modify, delete] the security attributes [*proxy rules, URL categories, and protocol categories*] to [*authorised Super Administrators and authorised Delegated Administrators*].
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1
The TSF shall enforce the [*Proxy Filtering Policy*] to provide [permissive] default values for security attributes that are used to enforce the SFP[5].
FMT_MSA.3.2
The TSF shall allow the [*authorised Super Administrators and authorised Delegated Administrators*] 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_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1
The TSF shall restrict the ability to [query], [*search, sort, select, and export*] the [*audit data*] to [*authorised Super Administrators*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SAE.1 Time-limited authorisation
Hierarchical to: No other components.
FMT_SAE.1.1
The TSF shall restrict the capability to specify an expiration time for [*the administrator management session time*] to [*Super Administrators and Delegated Administrators*].
FMT_SAE.1.2
For each of these security attributes, the TSF shall be able to [*terminate the administrative session unless the administrator is at one of the 'Today', 'History', and 'Alerts' pages, otherwise*

[5] SFP – Security Functional Policy

terminate the session after the administrator navigates away from one of these pages] after the expiration time for the indicated security attribute has passed.

Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

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: [*management of security functions behavior, management of security attributes, and management of TSF data*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Super Administrator, Delegated Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate ~~users~~ **administrator** with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*the category database fails to receive a license key update on schedule*].
Dependencies: No dependencies.

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

6.2.6 Class FRU: Resource Utilization

FRU_FLT.2 Limited fault tolerance
Hierarchical to: FRU_FLT.1 Degraded fault tolerance
FRU_FLT.2.1
The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [*the category database does not receive a license key update on schedule*].
Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_RSA.1(a) Maximum quotas
Hierarchical to: No other components.
FRU_RSA.1.1a
The TSF shall enforce maximum quotas of the following resources: [*access to restricted approved categories*] that [individual user] can use [over a specified period of time].
Dependencies: No dependencies

FRU_RSA.1(b) Maximum quotas
Hierarchical to: No other components
FRU_RSA.1.1b
The TSF shall enforce maximum quotas of the following resources [*bandwidth*] that [defined group of users] can use [simultaneously].
Dependencies: No dependencies

6.2.7 Class FTA: TOE Access

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.2.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [*if a user exceeds the bandwidth quota for a protocol category defined by policy, any new concurrent sessions within that category will be blocked*].

FTA_MCS.2.2

The TSF shall enforce, by default, a limit of [*limit based on available bandwidth*] sessions per user.

Dependencies: FIA_UID.1 Timing of identification

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The ~~TSF~~ **Appliance Manager GUI and the Triton GUI** shall terminate an interactive session after a [*thirty minutes administrator inactivity*].

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 EAL2 augmented with ALC_FLR.2. Table 10 – Assurance Requirements summarizes the requirements.

Table 10 – 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.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary 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 Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 11 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1a	Audit Data Generation
	FAU_GEN.1b	Audit Data Generation
	FAU_SAR.1a	Audit review
	FAU_SAR.1b	Audit review – Event Log
	FAU_SAR.2	Restricted audit review
	FAU_SEL.1	Selective audit
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	EXT_FDP_ROL	Rollback of TOE configurations
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UAU.2	User authentication before any action
	FIA_UID.1	Timing of identification
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SAE.1	Time-limited authorisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

TOE Security Function	SFR ID	Description
Protection of TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
Resource Utilization	FRU_FLT.2	Limited fault tolerance
	FRU_RSA.1a	Maximum quotas
	FRU_RSA.1b	Maximum quotas
TOE Access	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination

7.1.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit functionality, all administrator login and logoff events, policy changes, and configuration changes. The TOE Access Log records contain the following information:

Table 12 – Audit Record Contents

Field	Content
Date	The date and time that the event was recorded.
User	Username of the administrator who performed the action.
Server	IP address of the server or appliance where the change occurred.
Role	Delegated administration role affected by the change.
Type	Configuration element that was changed, such as policy, category filter, or logon/logoff.
Element	Identifier for the specific element changed, such as the category filter name or role name.
Action	Type of change made, such as add, delete, change, log on, etc.
Previous	Value of the element before it was changed.
Current	Value of the element after it was changed.

When the TOE starts up, the TOE's boot process also includes the boot process for all audit log generation processes. Audit log generation processes do not shut down until the TOE itself is shut down. The TOE does not offer the option to shut down or restart the audit log generation processes under normal operating conditions. The audit log generation processes are considered to be always invoked when the TOE is active.

The TOE provides a set of web interfaces that administrators can use to view the recorded audit logs. The Access Log can be viewed via Triton GUI by Super Administrators with policy or higher permissions.

Super Administrators can also select which URL categories to audit or not audit from the Triton GUI. The Event Log can be viewed via the Application Manager GUI by selecting a software module and viewing the audited events for the particular module.

TOE Security Functional Requirements Satisfied: FAU_GEN.1a, FAU_GEN.1b, FAU_SAR.1(a), FAU_SAR.1(b), FAU_SAR.2, FAU_SEL.1.

7.1.2 User Data Protection

The TOE enforces a Proxy Filtering Policy on controlled traffic. The policy allows administrators to define categories of websites and protocols that internal users should be prevented from accessing. Administrators specify the category and protocol restrictions to implement for each user or group of users. User traffic can be controlled in various ways, including allowing access to content, blocking access to content, or enforcing various quotas and bandwidth restrictions.

Policies are based on categories of web content and non-web protocols. Default content categories include adult material, political, business and economy, and many more. Administrators can define policies with these default categories or create new categories to create more customized policies. Default protocol categories include instant messenger, bit torrent, and many others. Like with content categories, administrators can define custom protocol categories to help enforce more customized policies.

Administrators can take regular backups of all important TOE configuration and policy data. Administrators can restore the system to a backup state at any time.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, EXT_FDP_ROL.

7.1.3 Identification and Authentication

The TOE requires administrators to identify and authenticate themselves with the TOE before gaining access to any of the management functionality available via the web interface. The installation CLI is only available by directly connecting to the serial port or monitor and keyboard ports on the appliance and does not require administrators to be identified and authenticated when accessing it. This is because it is assumed that an administrator has already been granted physical access to the appliance.

The TOE maintains a list of usernames, group membership, and passwords for each administrative account.

The TOE also requires users to identify and authenticate themselves before accessing content through the TOE. Several methods for authenticating users are available. When configured with Legacy NTLM or Integrated Windows Authentication (IWA), the TOE challenges users for proof of their credentials and verifies the credentials directly with a configured domain controller. The TOE can also be configured for LDAP or RADIUS authentication.

Administrators who fail to provide valid credentials after attempting to log in must wait five seconds before being able to attempt to log in again.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.2, FIA_UID.1, FIA_UID.2.

7.1.4 Security Management

The TOE provides a web interface that administrators can use to manage all TOE settings, policies, audit logs, administrator accounts, and user accounts. Administrators are able to access management functionality through a series of screens that contain text boxes, radio buttons, and other Adobe Flex elements. When managing Proxy Filtering Policy rules, administrators can specify alternative values for the default permissive values assigned to the TOE.

Typically administrators are logged out of the web interface after a period of thirty minutes of inactivity. Administrators can enable a feature that allows administrators to remain logged in indefinitely if they are on the 'Today', 'History', or 'Alerts' pages. If the administrator navigates away from one of these pages after thirty minutes of inactivity, the TOE terminates that administrator's session and the administrator must log in again to access any management functionality. This feature is available because these pages contain real-time updated information where it may be legitimate for administrators to monitor for long periods. Administrators monitoring these pages would appear inactive to the TOE without this feature enabled.

The TOE maintains two roles: Super Administrators and Delegated Administrators. Super Administrators have several sub-permissions that can be assigned:

- Unconditional – complete access to the TOE management capabilities.
- Global Security Administrator – administrator permissions with complete access to manage all available TOE modules.[6]
- Policy – allows Super Administrators to create and edit Delegated Administration roles, copy filters and policies to these roles, create and edit filtering components, filters, and policies, and apply policies to clients that are not managed by another role.
- Conditional – Policy administrators that can also access database downloads, directory services, user identification settings, and Network Agent settings. Conditional Super Administrators can add user accounts but not delete them and can create and edit delegated administration roles but cannot delete roles.
- Reporting – allows access to all reporting features and reports for all users.
- Real-Time – allows administrators to monitor all Internet filtering activities
- Auditor – allows administrators to see all of the content filtering features and functions, but cannot save any changes.

The default administrator account is a Super Administrator with unconditional privileges. This account cannot be deleted and its permissions cannot be changed.

The other type of administrator is the Delegated Administrators, which have much more limited access to management functionality. Delegated Administrators have four types of sub-permission sets:

- Policy – allows administrators to apply policies to clients and create, edit, and delete policies and filters (unless the policy or filter has been locked by a Super Administrator).
- Reporting – allows administrators to report on users.
- Real-Time – allows administrators to monitor all Internet filtering activities
- Auditor – allows administrators to see all of the content filtering features and functions, but cannot save any changes.

In addition to having limited permission sets, Delegated Administrators can only perform management actions for users that they have been assigned to manage by a Super Administrator.

[6] Web Security is the only module included in this evaluation

Only Super Administrators will policy or higher permissions can review the audit data

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SAE.1, FMT_SMF.1, FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE can fail into a secure state when a category database fails to receive a license key update on schedule. If the license key update is not received within fourteen days, the category database is considered outdated, and the TOE stops filtering traffic. Until fourteen days have passed, the TOE continues to filter traffic based on the most current category database information.

The TOE has an internal hardware clock that provides reliable timestamps for the TOE.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_STM.1.

7.1.6 Resource Utilization

If the TOE fails to receive an update to the category database license key update on schedule, the TOE continues to filter traffic for fourteen days. If the license key update is received before fourteen days pass, then the TOE continues to filter traffic uninterrupted.

The TOE is capable of limiting access of users to a set of content based on a time limit quota. When the user's time quota has been used up, the TOE then blocks all attempts the user makes to access content within those controlled categories. An example of how this might be used is to allow users an hour each day to browse content that is nonconductive to productivity (such as streaming video sites) without completely restricting the content.

The TOE is capable of limiting the allocation of network bandwidth to certain categories or protocols. Administrators define a threshold that the category or protocol should not exceed. If the threshold is reached or exceeded for the controlled category of protocol, any future attempts by users to establish a connection via that category or protocol are blocked by the TOE until more bandwidth becomes available.

TOE Security Functional Requirements Satisfied: FRU_FLT.2, FRU_RSA.1a, FRU_RSA.1b.

7.1.7 TOE Access

The TOE is capable of limiting the number of concurrent sessions users can have based on available bandwidth. If a user attempts to establish a new concurrent session while the bandwidth threshold for that type of traffic is met or exceeded, the TOE will block the new session from being established.

The web interface enforces a hard-coded thirty-minute timeout period for administrative sessions. If an administrator is inactive while logged into the web interface for thirty or more minutes, the TOE terminates the session and the administrator must log in again.

TOE Security Functional Requirements Satisfied: FTA_MCS.2, FTA_SSL.3.

8 Rationale

8.1 Conformance Claims Rationale

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

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 13 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.EXTERNAL_CONTENT A user or process on the internal network may access or post content to an external network that has been deemed inappropriate or potentially harmful to the internal network.	O.RESOURCE_CONTROL The TOE must control access to network resources as defined by the Proxy Filtering Policy.	O.RESOURCE_CONTROL counters this threat by ensuring that network resources controlled by the Proxy Filtering Policy can be blocked when they contain potentially harmful or inappropriate content.
	O.HARMFUL_CONTENT The TOE must disallow access to malicious content hidden within legitimate network resource requests for controlled protocol traffic.	O.HARMFUL_CONTENT counters this threat by ensuring that malicious content is removed from trusted content prior to being delivered to the internal network, thereby minimizing the risk of attack to the internal network.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their controlled protocol traffic matches a Proxy Filtering Policy rule that requires user authentication.	O.AUTHENTICATE counters this threat by ensuring that TOE administrators and users supply login credentials before being granted access to services or information, thereby reducing the risk of access by masquerading.
T.NACCESS An unauthorized person or external IT entity may be able to view or modify TOE data by hijacking an unattended	O.PROTECT The TOE must have the capability to protect management traffic from unauthorized reading or modification.	O.PROTECT counters this threat by ensuring that unattended management sessions do not permit attackers to access management functionality.

Threats	Objectives	Rationale
administrator session.		
T.UNAUTHORIZED_ACCESS A user may gain access to security data on the TOE that they are not authorized to access.	O.AUTHENTICATE The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their controlled protocol traffic matches a Proxy Filtering Policy rule that requires user authentication.	O.AUTHENTICATE counters this threat by ensuring that users supply login credentials before being granted access to any security-relevant information.
	O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record the resulting actions of the Proxy Filtering Policy and allow trained administrators to review security-relevant audit events.	O.AUDIT counters this threat by ensuring that the TOE records potential security breaches and suspicious activity, and allows authorized administrators to review this activity.
	O.MANAGE The TOE must provide secure management of the system configuration and the Proxy Filtering Policy over one or more concurrent sessions.	O.MANAGE counters this threat by providing the capability for an administrator to properly configure the management mechanisms of the TOE designed to mitigate this threat.
	O.TIMESTAMP The TOE must provide a timestamp for its own use.	O.TIMESTAMP counters this threat by ensuring that timestamps used in the audit records created by O.AUDIT are reliable. These audit records are used by administrators to observe any suspicious activity.
	O.PROTECT The TOE must have the capability to protect management traffic from unauthorized reading or modification.	O.PROTECT counters this threat by ensuring that the TOE is capable of protecting management data and access to management functionality from unauthorized access via an unattended management session.
T.RESOURCE TOE users or attackers may cause network connection resources to become overused and therefore unavailable.	O.QUOTA The TOE must be able to place quotas on network connection resources.	O.QUOTA counters this threat by ensuring that the TOE is capable of placing administrator-defined quotas on the network resources, thereby ensuring that those resources do not become unavailable.
T.DB_FAILURE A TOE user or attacker may cause	O.DB_RESILIENCY The TOE must be resilient against	O.DB_RESILIENCY counters this threat by ensuring that the TOE

Threats	Objectives	Rationale
the TOE's internal database to fail or become corrupted.	the potential failure of its internal database.	can fail to a secure state, recover from a database failure, and roll back changes that may have caused database corruption.

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 Policies defined for this Security Target. Therefore, there are no Security Objectives relating to Policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 14 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE has been installed and configured according to the appropriate installation guides.	NOE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	NOE.ADMIN upholds this assumption by ensuring that the administrator responsible for the TOE installs and configures the TOE according to the guidance documentation.
A.NETWORK All Proxy Filtering Policy-controlled traffic between the internal and external networks traverses the TOE.	OE.NETWORK All Proxy Filtering Policy-controlled protocol traffic between the internal and external network must traverse the TOE.	OE.NETWORK upholds this assumption by ensuring that the IT environment is configured such that no Proxy Filtering Policy-controlled traffic can travel between the internal and external networks without traversing the TOE.
A.LOCATE It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.	NOE.LOCATE The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.LOCATE upholds this assumption by ensuring that the IT environment is suitable to ensure the proper, secure functioning of the TOE.
A.NOEVIL It is assumed that administrators who manage the TOE are not careless, negligent, or willfully hostile; are appropriately trained; and follow all guidance.	NOE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	NOE.ADMIN upholds this assumption by ensuring that administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.MANAGE There are one or more competent	NOE.ADMIN The administrator must not be	NOE.ADMIN upholds this assumption by ensuring that those

Assumptions	Objectives	Rationale
individuals assigned to manage the TOE and the security of the information it contains.	careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	responsible for the TOE provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.
A.EXCLUSIVE All administrative interfaces are not accessible to non-administrators and only administrators have access to the administrative interfaces to ensure the network is secure.	NOE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	NOE.ADMIN upholds this assumption by ensuring that administrators are willfully not hostile and properly trained to not grant users without privileges to access administrative interfaces.

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

EXT_FDP_ROL is an extended functional requirement that was created to define the rollback operations of the TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

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 15 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the	FIA_ATD.1 User attribute definition	This requirement supports O.AUTHENTICATE by ensuring that the TOE can maintain a list of security attributes used for administrator authentication.

Objective	Requirements Addressing the Objective	Rationale
TOE and users to authenticate if their controlled protocol traffic matches a Proxy Filtering Policy rule that requires user authentication.	FIA_UAU.1 Timing of authentication	This requirement supports O.AUTHENTICATE by requiring administrators to authenticate their identities before being allowed access to any TOE management functionality besides the installation CLI.
	FIA_UAU.2 User authentication before any action	This requirement supports O.AUTHENTICATE by requiring users to authenticate their identities before gaining access to network resources.
	FIA_UID.1 Timing of identification	This requirement supports O.AUTHENTICATE by requiring administrators to identify themselves before being allowed access to any TOE management functionality besides the installation CLI.
	FIA_UID.2 User identification before any action	This requirement supports O.AUTHENTICATE by requiring users to identify themselves before being allowed access to network resources.
O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record the resulting actions of the Proxy Filtering Policy and allow trained administrators to review security-relevant audit events.	FAU_GEN.1a Audit Data Generation	This requirement supports O.AUDIT by ensuring that the TOE generates audit records for events at the "not specified" level of audit.
	FAU_GEN.1b Audit Data Generation	This requirement supports O.AUDIT by ensuring that the TOE generates audit records for events at the "not specified" level of audit.
	FAU_SAR.1a Audit review	This requirement supports O.AUDIT by ensuring that administrators can review the audit records generated by the TOE.
	FAU_SAR.1b Audit review – Event Log	This requirement supports O.AUDIT by ensuring that administrators can review the audit records generated by the TOE, including administrator log in attempts and database updates.
	FAU_SAR.2 Restricted audit review	This requirement supports O.AUDIT by ensuring that only

Objective	Requirements Addressing the Objective	Rationale
		authorized administrators are able to view the audit records generated by the TOE.
	FAU_SEL.1 Selective audit	This requirement supports O.AUDIT by providing administrators with the ability to select audit records for further manipulation, such as exporting a certain set of audit records.
	FMT_MTD.1 Management of TSF data	This requirement supports O.AUDIT by ensuring that only authorized administrators are able to manage audit data.
O.MANAGE The TOE must provide secure management of the system configuration and the Proxy Filtering Policy over one or more concurrent sessions.	FMT_MOF.1 Management of security functions behaviour	This requirement supports O.MANAGE by specifying the management activities available for each administrative role to perform.
	FMT_MSA.1 Management of security attributes	This requirement supports O.MANAGE by specifying which administrative roles can manage security attributes relating to the Proxy Filtering Policy.
	FMT_MSA.3 Static attribute initialisation	This requirement supports O.MANAGE by defining the default security posture of the Proxy Filtering Policy, and specifying the administrative roles that can change the policy from the default posture.
	FMT_SMF.1 Specification of Management Functions	This requirement supports O.MANAGE by specifying which management functionality is available for the TOE.
	FMT_SMR.1 Security roles	This requirement supports O.MANAGE by specifying which roles are available for administrators, and by ensuring that administrators are properly associated with their assigned roles.
	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	This requirement supports O.MANAGE by ensuring that administrators can manage and define the number of concurrent sessions that an end user can run.
O.RESOURCE_CONTROL	FDP_ACC.1	This requirement supports

Objective	Requirements Addressing the Objective	Rationale
The TOE must control access to network resources as defined by the Proxy Filtering Policy.	Subset access control	O.RESOURCE_CONTROL by ensuring that the TOE can control access of subjects (users) to objects (controlled network traffic).
	FDP_ACF.1 Security attribute based access control	This requirement supports O.RESOURCE_CONTROL by ensuring that the TOE can utilize the attributes of the controlled network traffic to enforce the Proxy Filter Policy.
	FMT_MSA.1 Management of security attributes	This requirement supports O.RESOURCE_CONTROL by ensuring that only authorized administrators can modify security attributes associated with the Proxy Filtering Policy.
	FMT_MSA.3 Static attribute initialisation	This requirement supports O.RESOURCE_CONTROL by ensuring that the Proxy Filtering Policy is restrictive by default, and that only authorized administrators can modify this default posture.
O.QUOTA The TOE must be able to place quotas on network connection resources.	FRU_RSA.1a Maximum quotas	This requirement supports O.QUOTA by ensuring that the TOE is capable of placing maximum quotas on the number of connections available during a specified time period.
	FRU_RSA.1b Maximum quotas	This requirement supports O.QUOTA by ensuring that the TOE places maximum quotas on the bandwidth available for use by different types of traffic.
O.TIMESTAMP The TOE must provide a timestamp for its own use.	FPT_STM.1 Reliable time stamps	This requirement supports O.TIMESTAMP by ensuring that the TOE provides a timestamp for its own use.
O.HARMFUL_CONTENT The TOE must disallow access to malicious content hidden within legitimate network resource requests for controlled protocol traffic.	FDP_ACC.1 Subset access control	This requirement supports O.HARMFUL_CONTENT by ensuring that the Proxy Filtering Policy can block harmful content that might exist within trusted content.
	FDP_ACF.1 Security attribute based access	This requirement supports O.HARMFUL_CONTENT by

Objective	Requirements Addressing the Objective	Rationale
	control	ensuring that the TOE can utilize the attributes of the controlled network traffic to enforce the Proxy Filter Policy.
	FMT_MSA.1 Management of security attributes	This requirement supports O.HARMFUL_CONTENT by ensuring that only authorized administrators can modify security attributes associated with the Proxy Filtering Policy.
	FMT_MSA.3 Static attribute initialisation	This requirement supports O.HARMFUL_CONTENT by ensuring that the Proxy Filtering Policy is restrictive by default, and that only authorized administrators can modify this default posture.
O.DB_RESILIENCY The TOE must be resilient against the potential failure of its internal database.	EXT_FDP_ROL Rollback of TOE configurations	This requirement supports O.DB_RESILIENCY by enabling administrators to roll back the database to a previous state if it becomes corrupted or unstable.
	FPT_FLS.1 Failure with preservation of secure state	This requirement supports O.DB_RESILIENCY by allowing the TOE to fail to a secure state when the database fails.
	FRU_FLT.2 Limited fault tolerance	This requirement supports O.DB_RESILIENCY by ensuring that the TOE can still operate when the database fails.
O.PROTECT The TOE must have the capability to protect management traffic from unauthorized reading or modification.	FIA_AFL.1 Authentication failure handling	This requirement supports O.PROTECT by ensuring that administrator accounts are locked after a pre-configured number of failed login attempts.
	FMT_SAE.1 Time-limited authorisation	This requirement supports O.PROTECT by ensuring that authorized administrators can monitor real-time updated data pages without risking an unauthorized individual gaining access to an unattended management session.
	FTA_SSL.3 TSF-initiated termination	This requirement supports O.PROTECT by ensuring that unauthorized individuals do not gain access to the TOE through an

Objective	Requirements Addressing the Objective	Rationale
		unattended management session.

8.5.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package augmented with ALC_FLR.2. EAL2+ was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. Websense V10000 G2 Web Gateway Appliance v7.6 is targeted at an environment with good physical security (A.LOCATE) and competent administrators (NOE.ADMIN, A.MANAGE), where EAL 2 should provide adequate assurance. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack. ALC_FLR.2 was chosen to assure that the developer is able to act appropriately upon security flaw reports from TOE users. This Security Target conforms to Part 2 extended and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3.

As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.5.3 Rationale for Refinements of Security Functional Requirements

The following refinements of SFRs from CC version 3.1 have been made to specify that the SFR applies to administrator identification and authentication instead of user identification and authentication: FIA_ATD.1, FIA_UAU.1, FIA_UID.1.

8.5.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 16 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 16 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1a	FPT_STM.1	✓	
FAU_GEN.1b	FPT_STM.1	✓	
FAU_SAR.1a	FAU_GEN.1	✓	
FAU_SAR.1b	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SEL.1	FAU_GEN.1	✓	
	FMT_MTD.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
EXT_FDP_ROL	None	N/A	
FIA_AFL.1	FIA_UAU.2	✓	
FIA_ATD.1	None	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.2	FIA_UID.1	✓	FIA_UAU.2 applies to user authentication. Although FIA_UID.1 is claimed, it applies to administrator identification. FIA_UID.2 is also claimed, and applies to user identification. Since FIA_UID.2 is hierarchical to FIA_UID.1, this SFR satisfies this requirement.
FIA_UID.1	None	N/A	
FIA_UID.2	None	N/A	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SAE.1	FMT_SMR.1	✓	
	FPT_STM.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_FLS.1	None	N/A	

SFR ID	Dependencies	Dependency Met	Rationale
FPT_STM.1	None	N/A	
FRU_FLT.2	FPT_FLS.1	✓	
FRU_RSA.1a	None	N/A	
FRU_RSA.1b	None	N/A	
FTA_MCS.2	FIA_UID.1	✓	
FTA_SSL.3	None	N/A	

9 Acronyms

This section describes the acronyms.

9.1 Acronyms

Table 17 - Acronyms

Acronym	Definition
CC	Common Criteria
CEM	Common Evaluation Methodology
CentOS	Community Enterprise Operating System
CLI	Command Line Interface
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
URL	Uniform Resource Locator
USB	Universal Serial Bus

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