Cisco Wide Area Application Services (WAAS)

Security Target

Version 20

May 2010

Document Introduction

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

Prepared For:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

Table of Contents

List of Tables

List of Figures

1 Security Target Introduction

This section identifies the Security Target [ST] and Target of Evaluation [TOE] identification, ST conventions, ST conformance claims and the ST organization. The TOE is Wide Area Application Services provided by Cisco Systems, Inc. The Wide Area Application Services [WAAS] is an application acceleration and WAN optimization solution allowing IT organization to consolidate costly branch office servers and storage into centrally-managed data centers and to deploy new applications directly from a data center, while still offering LAN-like application performance regardless of location. The solution helps to optimize the performance of any TCP-based application operating over a Wide Area Network (WAN) environment.

The Security Target contains the following sections:

- TOE Description [Section 2]
- Security Environment [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Protection Profile Claims [Section 7]
- Rationale [Section 8]
- Acronyms [Appendix A]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

1.1 ST and TOE Reference

ST Title	Cisco Wide Area Application Services Security Target
ST Version	20
Publication Date	May 2010
Vendor and ST Author	Cisco Systems

TOE Reference	Cisco Wide Area Application Services solution including:
	Wide Area Virtualization Engine (WAVE) 274, 474, 574;
	Wide Area Application Engine (WAE) 674, 7341 and 7371;
	WAE Network Module (NME-WAE) NME-WAE-502, NME-WAE-522 and WAE Inline Network Adapter

TOE Software Version	Cisco WAAS version 4.2.1
Key Words	WAN, Application Services

1.2 TOE Overview

1.2.1 TOE Product Type

The Cisco WAAS (TOE) is a network application delivery solution for Wide Area Networks (WANs) – geared for branch and mobile employee deployments. By deploying WAAS, IT organizations can consolidate costly branch-office servers and storage in centrally managed data centers, and to deploy new applications directly from the data center, while offering LAN-like application performance for remote users. The WAAS defined in this ST covers multiple hardware appliance products loaded with the WAAS 4.2.1 software package, which comprises the solution.

The TOE consists of hardware and software used to provide application services acceleration between client machines (workstation) and the application servers (e.g., web servers, file servers). The TOE is the WAAS solution running software v4.2.1.

Distributed organizations face significant challenges due to performance and scalability constraints imposed by a Wide Area Network (WAN). Enterprises are looking for ways to control the explosive growth in bandwidth requirements generated by new applications and business processes, while also improving throughput and responsiveness for existing applications in a transparent manner. Cisco® Wide Area Application Services [WAAS] is an application acceleration and WAN optimization solution that optimizes the performance of any TCP-based application operating over a Wide Area network [WAN] environment. This allows IT organizations to consolidate costly branch office servers and storage into centrally-managed data centers and to deploy new applications directly from a data center.

1.2.2 Required non-TOE Hardware/ Software/ Firmware

The TOE requires (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 1: IT Environment Components

IT Environment Component	Required	Usage/Purpose Description for TOE performance
Cisco 2811, 2821, 2851, 3825 and 3845 routers; running Cisco IOS software 12.4(9)T or 12.4(9)T1	Yes, for NME-WAE 502 TOE component only	The NME-WAE which is a pluggable module for routers is dependent on its IT Environment, the router, to supply the power it needs to run.
Cisco 3825 and 3845 routers; running Cisco IOS software 12.4(15)T	Yes, for NME-WAE 522 TOE component only	The NME-WAE which is a pluggable module for routers is dependent on its IT Environment, the router, to supply the power it needs to run.
Web browser	YES	Administrators will use to communicate with the TOE; GUI administrative web interface. The recommended web browser is Internet Explorer version 5.5 or higher.
SSH Client	YES	Administrators will use to communicate with the TOE via CLI administrative interfaces. Any SSH client may be used. Examples include, PuTTy
NAS or File Servers for which CIFS file-caching is optimized by WAAS	YES	These servers will contain the files for which the TOE optimizes access.
Other application servers for which TCP traffic is optimized by WAAS	YES	These servers provide applications that are optimized by the TOE.
Authentication, Authorization, and Accounting (AAA) server (RADIUS, TACACS+ and Windows Authentication servers)	OPTIONAL	The TOE may optionally be configured to use IT Environment supplied services. If configured to use these services, communication is over trusted channels.
Time Server	OPTIONAL	Optionally provide time stamps in deployment scenarios in which an external time source is desirable.

1.3 TOE Description

This section provides an overview of the Cisco WAAS Target of Evaluation (TOE). This section also defines the physical and logical boundaries, summarizes the security functions, and describes the evaluated configuration.

1.4 Physical Scope of the TOE

The following lists the products included in the TOE physical scope of the TOE and described in the following sections.

1. Cisco WAE 674, 7341 and 7371;
2. Cisco WAVE 274, 474, 574;
2. Cisco NME-WAE 502 and 522;
3. Cisco WAAS 4.2.1 Software;
4. Cisco Wide Area Application Services Configuration Guide software release 4.2.1;
5. Cisco Wide Area Application Services Command Reference Software release 4.2.1

1.4.1 Cisco WAVE 274, 474, 574, Cisco WAE 674, 7341 and 7371

The TOE includes the complete hardware and software solution provided in the Cisco appliances WAVE 274, 474, 574 and WAE 674, 7341 and 7371. All these appliances execute the same software load WAAS 4.2.1. The difference between the WAVE appliances and the WAE appliances is that the WAVE appliances include the ability to provide virtualization services for locally hosted IT services. Virtualization is excluded from the evaluated configuration. In the evaluated configuration all TOE appliance operate identically. The following tables identify the physical configurations of the WAE and WAVE appliances.

Table 2: TOE WAE Devices Physical Specification

	WAE 674	WAE 7341	WAE 7371
SW Version	4.2.1	4.2.1	4.2.1
DRAM	4 or 8 GB	12 GB	24 GB
Hard Drive	600 GB Hard Drive	900 GB	1.5 TB
Inline Card	4-port inline card	4-port inline card	4-port inline card
Interfaces	(2) 10/100/1000BASE-T	(2) 10/100/1000BASE-T	(2) 10/100/1000BASE-T
Power	(1) 835W hot-swap AC Redundant power available	(2) 835W hot-swap AC	(2) 835W hot-swap AC

Table 3: TOE WAVE Devices Physical Specification

	WAVE 274	WAVE 474	WAVE 574
SW Version	4.2.1	4.2.1	4.2.1
DRAM	3 GB	3 GB	3 GB or 6 GB
Hard Drive	250 GB Hard Drive	250 GB Hard Drive	500 GB Hard Drive
Inline Card	4-port inline card	4-port inline card	4-port inline card
Interfaces	(1) 10/100/1000BASE-T	(1) 10/100/1000BASE-T	(2) 10/100/1000BASE-T
Power	One 240W AC	One 240W AC	One 400W AC

These WAE and WAVE appliances can be logically configured as either a Central Manager (CM) or as an application accelerator. The following table describes the configurations of the WAE and WAVE appliances.

Table 4: TOE Device Role Description

Device Role	Description
Application Accelerator: Branch (WAE/WAVE//NME-WAE)	The branch device is a client-side, optionally file-caching device that serves client requests at remote sites and branch offices. As a general optimization device, the device acts as a client-side optimization entity of the two-device solution, optimizing the TCP connections going through the device. As a file-caching device, the device is deployed at each branch office or remote campus providing near-LAN access to a cached view of data center server files/folders. For non-cached files the branch device forwards the request to the data center WAE. On getting a response, the branch device can choose to cache the file that the client requested and is getting served.
Application Accelerator: Data Center (WAE/WAVE only)	The data center device is a server-side component that resides at the data center and connects directly to one or more application servers, file servers, or network-attached storage (NAS). As a general optimization device, the device acts as a server-side optimization entity of the two-device solution, optimizing the TCP connections going through the device. As a head-end of a file-caching solution, requests received from branch devices over the WAN are translated by the data center device into its original file server protocol and forwarded to the appropriate file server. When the data center file server responds, the device forwards the response back to the branch device.
Central Manager (CM) (WAE/WAVE only)	For every WAAS solution, the TOE must have one primary WAAS Central Manager (CM) device that is responsible for managing the other devices in the solution. The CM device hosts the WAAS Central Manager GUI which is a Web-based interface that allows administrators to configure, manage, and monitor the WAAS devices that make up the TOE solution. The CM resides on a dedicated WAE/WAVE appliance.

1.4.2 Cisco NME-WAE 502 and 522

The TOE includes the router pluggable module, NME-WAE. This module executes the WAAS 4.2.1 software load. The NME-WAE can only be configured to be an application accelerator device in the evaluated Redirection Configuration. The only differences between the NME-WAE (502 and 522) and the Cisco appliances WAVE 274, 474, 574 and WAE 674, 7341 and 7371 are that (a) the NME-WAE is loadable/pluggable into a Cisco router and (b) NME-WAE cannot be used in inline configuration. The TOE boundary for the NME-WAE encompasses the complete hardware and software product of the NME-WAE. The router is considered part of the IT environment and considered a remote trusted IT product. The following table identifies the physical configurations of the NME-WAE module.

Table 5: TOE NME-WAE Physical Specification

	NME-WAE 502	NME-WAE 522
SW Version	4.2.1	4.2.1
DRAM	1 GB	2 GB
Hard Drive	120 GB	160 GB
Inline Card	Not supported	Not supported
Interfaces	10/100/1000 Gigabit Ethernet connectivity to router backplane	10/100/1000 Gigabit Ethernet connectivity to router backplane
Power	Provided by router	Provided by router

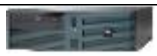
Supported Routers	Cisco 2811, 2821, 2851, 3825, or 3845	Cisco 3825 or 3845
Supported Router SW	12.4(9)T or 12.4(9)T1	12.4(15)T

1.4.3 Cisco WAE Inline Network Adapter

The TOE includes the Cisco WAE inline network adapter which provides an inline traffic interception capability - attributes may be set by the administrator to control which interfaces are to be used over which VLANs. By default, the inline adapter operates on all inline-capable interfaces and VLANS. The administrator may configure the inline redirection feature using the CLI or Central Manager GUI. The inline network adapter is a PCI-X or PCIe network interface card that contains two pairs of Gigabit Ethernet ports (LAN and WAN).

The following table shows each TOE component and identifies the roles that each can assume:

Table 6: TOE NME-WAE Physical Specification

TOE Component		Possible Roles
WAE 674		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAE 7341		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAE 7371		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAVE 274		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAVE 474		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
WAVE 574		Application Accelerator: Branch Application Accelerator: Data Center Central Manager (CM)
NME-WAE 502		Application Accelerator: Branch Application Accelerator: Data Center
NME-WAE 522		Application Accelerator: Branch Application Accelerator: Data Center

1.4.4 Cisco WAAS 4.2.1 Software

The TOE includes the software load WAAS 4.2.1. The physical boundary is the complete image binary of the WAAS 4.2.1 release. This software includes a version of Linux kernel version 2.6 customized for use as part of the WAAS solution.

1.5 Logical Scope of the TOE

This section summaries the security functionality of the TOE:

- Security Management
- Access Control
- Audit
- CIFS File Cache
- Identification and Authentication
- Self Protection

1.5.1 Security Management

The TOE's Security Management functionality provides management support functionality that enables a human user to manage and configure the TOE securely. The Security Management functionality guarantees that management actions can only be performed after an authorized user has been authenticated. An authorized user is one who has been successfully identified and authenticated. The TOE manages user roles to ensure restricted access to the security functions, acceleration services, and data of the TOE to only those users that are authorized for a specific service. The TOE can be managed locally or remotely by the administrator.

The TOE's Security Management functionality ensures that users are only allowed access to resources that they have been explicitly authorized to use. Authorized users are only allowed to carry out operations associated with their assigned role, as follows:

- The TOE controls which users can modify and configure the security settings of the TOE.
- This security function controls which users can change and configure the file services acceleration policies and file caching policies of the TOE as defined by FDP_ACC.1(2) and FDP_ACF.1(2).

1.5.2 Access Control

The TOE provides the ability to control traffic flow through the TOE.

An IP ACL (permit/deny) policy is an administratively configured access control list that is applied to traffic destined for the TOE management interfaces. IP ACLs can filter traffic (permit or deny traffic flow) based on the following: Source IP address, Destination IP address, Protocol, Source Port, and Destination Port.

Note: These access controls are designed as protection for access to the TOE itself and not meant to filter traffic passed through the TOE.

1.5.3 Audit

The TOE's Audit functionality supports audit record generation, storage, and audit review by authorized users. Audit records are stored in a combination of syslog and errlog files on the hard drive of the TOE devices. The appliance (WAE/WAVE) and module (NME-WAE) TOE devices maintain time to generate a reliable timestamp which is applied to each audit event record. The TOE solution can optionally be configured to receive initial time from the IT environment (i.e., NTP Server).

Both the application accelerator and Central Manager TOE components generate and store audit records. The application accelerator TOE component provides that ability to view locally stored audit record relevant to the device. The Central Manager provides the ability to view all audit records relevant to all TOE devices. The application accelerator TOE components forward local audit records to the Central Manager at regular intervals.

1.5.4 CIFS File Cache

The TOE's File Cache security function relies on the IT Environment file server(s) to enforce file permission access controls for cached files.

The TOE's File Cache security function also protects user data by using encrypted storage (encrypted file system) for the cached files.

The TOE's File Cache function includes user data pre-positioning capability – a feature to fill the cache periodically in order to provide cache-hit performance even for a first user. This feature includes: (1) initiating CIFS connection to the server, (2) passing server authentication, and (3) reading file data and meta-data and storing them in the cache. File meta-data that is stored in cache include various file attributes, file access control lists (ACLs) and permissions. The File Cache function uses a "pre-position user" credential that has been configured in the IT environment. This is similar to other users that access the file server except that the TOE itself initiates the connection with the user credentials for the purposes of pre-positioning files. Branch WAE devices use user name and password to retrieve preposition from the file server via Data Center WAE device. The credentials associated with the "pre-position user" are input by the TOE administrator into the IT environment file server as an authorized user. The Credentials are also input into the TOE during configuration by the TOE administrator. The credentials are stored internal to the TOE and are never output to unauthorized users. No direct user access is provided to any cached file using the preposition credentials. These credentials are input into the TOE and stored within the TOE as other TOE configuration information. Only the default TOE administrator and administrators whose associated role is defined with the necessary permission can access the credentials. Access is only granted after the authorized administrator is successfully authenticated by the TOE.

1.5.5 Identification and Authentication

This functionality requires administrators that manage and configure the TOE to successfully authenticate before they are allowed to carry out any other actions that are mediated by the TOE. Proper and successful authentication is required for all user interfaces of the TOE. Successful identification and authentication of administrators is required whether the administrator is security relevant or non-security relevant. A non-security relevant administrator is an administrator for which the associated role has no access to security relevant functionality. The

TOE supports local and remote administration. Remote administration is only allowed using SSH or HTTPS protected communications. By default, the TOE uses the local authentication database to verify user credentials. The TOE can optionally be configured to use an external authentication server instead of the TOE's local authentication database. To support external authentication, the administrator must explicitly configure the TOE to support additional authentication methods. The TOE administrator can configure the types of authentication supported, and order in which the authentication methods are applied.

When an application accelerator device is activated, a unique hash tag is associated with the device and exchanged with the device. This tag is used by the device to identify itself in all future communication with the CM.

1.5.6 Self Protection

The TOE solution includes multiple hardware components containing non-modifiable software, in which, all operations in the TSF scope of control are protected from interference and tampering by untrusted subjects. All administration and configuration operations are performed within the physical boundary of the TOE. The TOE has been designed so that TSF data, User data, and Security Attributes within the TSF Scope of Control can only be manipulated via the TOE CLI and GUI interfaces which mediate all actions through these interfaces.

Communications between TOE components (branch, data center, and CM) are protected by Transport Layer Security (TLS) with the exception of the Print Services UI which is not used in the evaluated configuration. The TOE protects remote management and configuration sessions with SSH version 2 and HTTPS.

The TOE can control the termination of a CLI or GUI session based on a settable inactive session parameter. After the set amount of time of inactivity has been reached, the TOE will terminate the interactive session. The TOE will also terminate a Secure Shell (SSH) session that is being negotiated after a configurable inactivity period while the negotiation occurs.

All sensitive data on the TOE in persistent storage, such as files and database, are encrypted using strong encryption (AES 256). Strong encryption is enforced when Secure Store feature is enabled on both CM and WAE.

The cryptography within the TOE has not been FIPS validated. The strength of the cryptographic operations performed by the TOE is vendor asserted.

The TOE cannot be bypassed, corrupted, or otherwise compromised.

1.6 TOE Evaluated Configuration

The TOE is configured to provide end-to-end application acceleration and provides for the central management of multiple hardware appliances and pluggable modules.

In order to deploy the TOE in the evaluated configuration, the solution requires at least three devices: one device to act in the Central Manager role and two devices in the data path to act as Application Accelerators. The Central Manager role can be provided by the Cisco WAVE 274, Cisco WAVE 474, Cisco WAVE 574, Cisco WAE 674, Cisco WAE 7341, or Cisco WAE 7371 TOE components. The Application Accelerator role can be provided by the Cisco NME-WAE 502, Cisco NME-WAE 522, Cisco WAVE 274, Cisco WAVE 474, Cisco WAVE 574, Cisco WAE 674, Cisco WAE 7341, or Cisco WAE 7371. Each of these components loads the Cisco WAAS 4.2.1 Software.

The TOE performs two key accelerations: (a) generic optimization for any TCP connection that is configured to be optimized and (b) application aware optimization, including file-caching for CIFS typically used on Microsoft Windows Client-Server Network.

Two configurations are in the evaluation:

- Redirection Configuration [see Figure 1]
- Inline-Redirection Mixed Configuration [see Figure 2]

Figure 1: TOE Network – Redirection-only Configuration

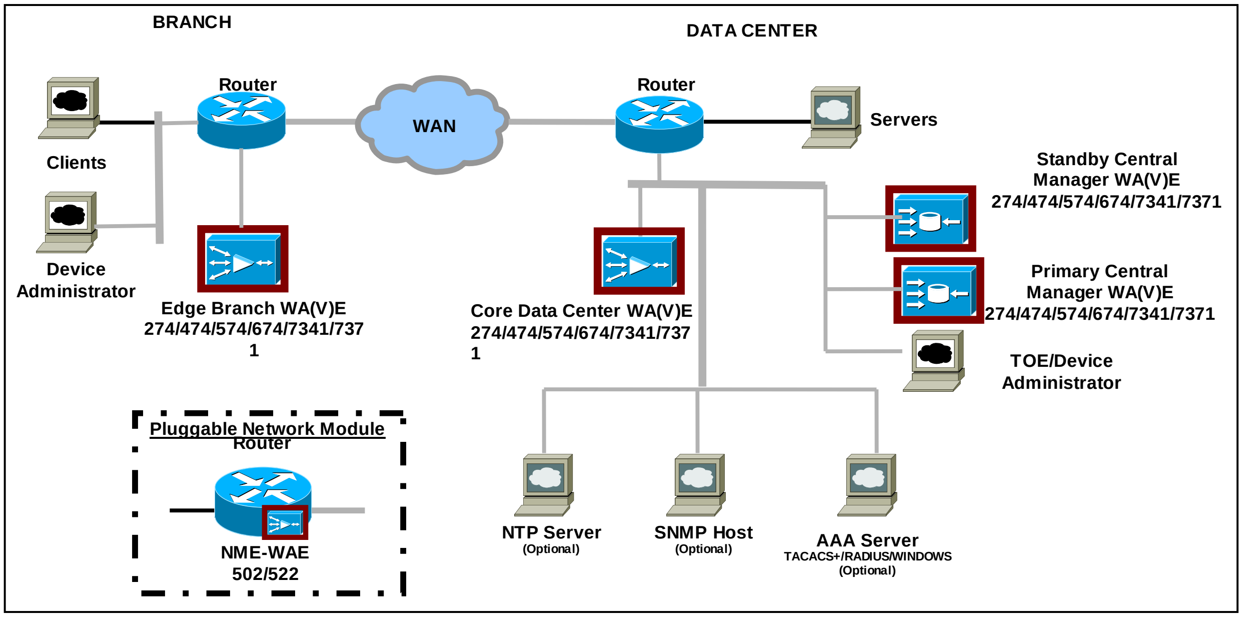
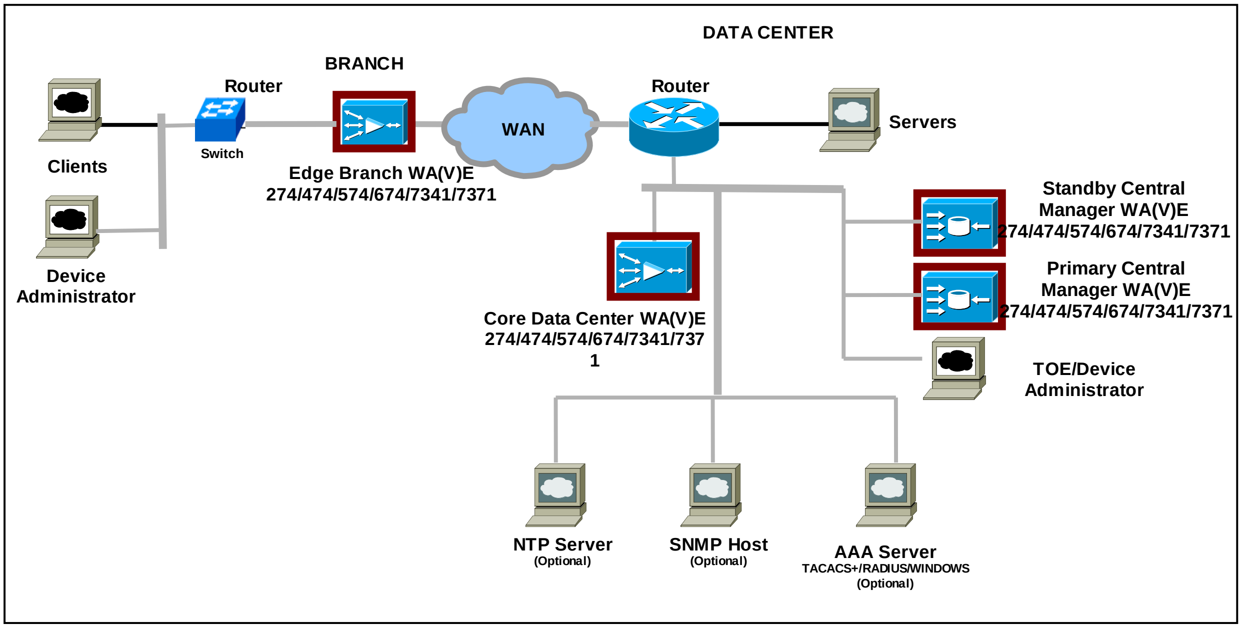


Figure 2: TOE Network – Inline + Redirection Mixed Configuration


DATA CENTER
BRANCH
Router
Switch
Clients
Device Administrator
Edge Branch WA(V)E 274/474/574/674/7341/7371
WAN
Router
Servers
Standby Central Manager WA(V)E 274/474/574/674/7341/7371
Primary Central Manager WA(V)E 274/474/574/674/7341/7371
Core Data Center WA(V)E 274/474/574/674/7341/737 1
TOE/Device Administrator
NTP Server (Optional)
SNMP Host (Optional)
AAA Server TACACS+/RADIUS/WINDOWS (Optional)

NOTE: the NME-WAE is not included in the "Inline + Redirection Mixed" configuration as NME-WAE is only used at the branch and it cannot support Inline Adapters.

The following table identifies configuration options that can optionally be configured in both "Redirection-only" and "Inline + Redirection Mixed" configurations. These optional configuration settings are an alternative to TOE default settings.

Table 7: Optional TOE Configuration Settings

Function	Default Configuration	Optional Configuration
Time	Use TOE internal clock	Use an External NTP server
AAA	Use Local Authentication Database	Use External AAA Server FTP_ITC.1, FTP_TRP.1
Pre-positioning	Disabled	Enable and configure for Branch WAE devices performing caching

1.6.1 TOE Features excluded from the evaluation

The table below identifies functionality included in the TOE's physical boundary but not included in the TOE's logical boundary or claimed in the TOE's security functionality. The TOE features listed below are outside the scope of the defined TOE Security Functions (TSF) and are therefore not evaluated. The features listed below are non-interfering with the TSF.

Table 8 Excluded Featrues

Item	Relevance
Device Automated Activation	Disabled by the administrative user.
Print Services	Disabled by the administrative user.
Virtualization, SSL Application Accelerator	Disabled by the administrative user.
SNMP	Disabled by the administrative user.
Features include in the TOE with no Security Relevance	
Modem interface	These features are included with in the TOE, however,

Application Traffic Policy (ATP) engine traffic classification and handling definitions	they do not provide any security relevant functionality and do not interfere with any of the security functionality claimed in the Common Criteria evaluation.
TCP Flow Optimization (TFO), interception and auto-discovery. Provides the "plumbing" needed for other services.	
Data Redundancy Elimination (DRE) – segment based redundancy elimination, byte-based LZ compression and byte-caching	
HTTP, MAPI, Video, NFS Application Optimizers	
Non-security related alarms and events	
Appliance USB ports, NME_WAE USB port, NME_WAE RJ45 port, CD ROM, and PS2 port	

1.6.2 Required Configuration Settings

The following list identifies required configuration settings that are needed for the products to be considered the TOE:

- Disable Telnet
- Disable SSHv1
- Enable SSHv2
- Disable SNMPv1, v2, and v3
- Disable SSL AO
- Disable FTP
- Disable Virtualization
- Disable Device Automated Activation
- Enable disk encryption on all Data Center and branch devices
- Enable strong password policy
- Enable Secure Store to enforce strong encryption algorithm
- Configure cipher list for SSL management service to exclude weak cipher suites
- Disable local Print Services
- Disable centralized (CIFS) print services
- Disable CM print drivers Repository
- Remove all print admin privileges from defined users in CM

Only authorized user[s] can manage the TOE through a Central Management (CM) GUI, a Device Manager GUI or a Command Line Interface (CLI).

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 2, dated: September 2007.
The TOE and ST are EAL4 Augmented with ALC_FLR.1 Part 3 conformant.
The TOE and ST are CC Part 2 extended

2.2 Protection Profile Conformance

This ST does not claim compliance to any Common Criteria validated Protection Profiles.

3 Security Problem Definition

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Policies are identified as P.policy with "policy" specifying a unique name.

3.1 Threats

The table below lists the threats addressed by the TOE and the IT Environment. For the threats below, attackers are assumed to be of low attack potential.

Table 9: Applicable Threats

Threats	Descriptions
T.DEVICECOMPROMISE	An unauthorized user may gain access to a TOE device he/she is not permitted to access, view, or modify the configurations of the device.
T.EXCEEDPRIV	An authorized user of the TOE may exceed his/her assigned security privileges resulting in the illegal modification of the TOE configuration.
T.LOWEXP	An attacker with low attack potential may attempt to bypass the TSF and gain access to the TOE or the assets it protects.
T.NODETECT	An unauthorized user, host or device may attempt to mount an attack against the TOE security functions without detection.
T.ZONECOMPROMISE	An unauthorized device within a network may gain access to a WAAS solution they are not a member of, and interfere with the file caching services of the WAAS solution.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The table below identifies the organizational security policies applicable to the TOE.

Table 10: Organizational Security Policies

OSPs	Descriptions	References
P.PASSWORD	The organization shall have in place policies and enforcement mechanisms to ensure the use of strong passwords when creating or modifying user passwords in the TOE.	Not Specified
P.PERSONNEL	The organization shall have in place policies, training programs, and reporting and enforcement mechanisms such that personnel know their security responsibilities (and role) when using the TOE.	Not Specified

3.3 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 11: Assumptions

Assumptions	Descriptions
A.MANAGMENTLAN	The Management LAN is trusted. All services such as optional external AAA servers, or NTP servers are provided by the management LAN, and all devices attached to the management LAN are trusted to perform in a secure manner.
A.NOEVIL	Administrators of the TOE are assumed to be non-hostile, trusted to perform their duties in a secure manner, and expected to follow all security policies and procedures applicable to their deployment.
A.PHYSICAL	All TOE components are assumed to be in a physically secure environment.
A.TIMESOURCE	Clock sources external to the TOE are configured accurately so as to provide a trusted clock source to the TOE's internal clock.
A.ZONECONNECT	Interconnected switches and routers, which are part of the IT Environment, that communicate with the TOE components that make up the WAAS solution are assumed to have protection against unauthorized access.

4 Security Objectives

4.1 TOE Security Objectives

The table below identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 12: TOE Security Objectives

Security Objective	Description
O.AUDIT	The TOE shall record the necessary events to ensure that all users of the TOE are held accountable for their actions.
O.EAL	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PRIVILEGE	The TOE shall ensure that authorized users do not exceed their assigned privileges/roles.
O.SECFUN	The TOE must provide functionality that enables and authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.SECUREOPERATE	The TOE shall prevent unauthorized modification to its security functions and configuration data.
O.WAASPROTECT	The TOE shall prevent unauthorized disclosure of management traffic dealing with the configuration and viewing of TOE devices for those TOE devices that are part of a WAAS solution.
O.WAASSOLUTION	The TOE shall ensure that only those authorized entities that are part of a WAAS solution are granted access to WAAS services as defined by the authorized user.

4.2 Security Objectives for the Environment

The assumptions identified above are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. The table below identifies the security objectives for the environment.

Table 13: Objectives for the Environment

Security Objective	Description
OE.AUTHENTICATIONSERVER	The TOE environment may optionally provide trusted authentication and authorization services for use with the TOE. The protocols that may be used for these services are restricted to RADIUS, TACACS+ or Windows Authentication Server (NTLMv1, NTLMv2 and Kerberos).
OE.MANAGEMENTLAN	The environment provides the TOE with a trusted management network that includes optional NTP and AAA services.
OE.PERSONNEL	Those responsible for the TOE will ensure that administrators, operators and maintainers have been trained sufficiently to configure, operate, and maintain the TOE in a secure and trusted manner in accordance with the guidance documentation.
OE.SECUREMANAGE	Those responsible for the operation of the TOE and interconnected switches and routers shall ensure that the TOE environment is physically secure, and management and configuration of the security functions of the TOE are:

Security Objective	Description
	a) Initiated from a management station connected to a trusted network, b) Undertaken by trusted staff trained in the secure operation of the TOE, c) Performed securely through the creation of strong passwords in accordance with industry best practices, and d) Configured to interface only to trusted clock sources.

4.3 Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat, assumption, or policy is addressed by a security objective. The following tables provide the mapping and rationale for the security objectives identified in Chapter 4 and the assumptions, threats and policies identified in Chapter 3.

Table 14: Threats, Assumptions, and Policies to Security Objectives Mapping

	O.AUDIT	O.IDAUTH	O.PRIVILEGE	O.SECFUN	O.SECUREOPERATE	O.WAASPROTECT	O.WAASSOLUTION	O.EAL	OE.AUTHENTICATIONSERVER	OE.MANAGEMENTLAN	OE.PERSONNEL	OE.SECUREMANAGE
T.DEVICECOMPROMISE		X			X	X	X					
T.EXCEEDPRIV	X		X	X	X							
T.LOWEXP								X				
T.NODETECT	X			X								
T.ZONECOMPROMISE					X		X					
P.PASSWORD		X		X					X			X
P.PERSONNEL			X								X	X
A.MANAGMENTLAN										X		
A.NOEVIL												X
A.PHYSICAL												X
A.TIMESOURCE												X
A.ZONECONNECT												X

Table 15: Threats, Assumptions and Policies to TOE Security Objectives Rationale

Threat or Policy	Rationale	Objectives
T.EXCEEDPRIV T.NODETECT	The TOE shall record the necessary events to ensure that all users of the TOE are held accountable for their actions. The TOE reduces the threat of as user exceeding assigned privileges by auditing applicable operations and therefore the user may be caught.	O.AUDIT
T.LOWEXP	The TOE must be structurally tested and shown to be resistant to obvious vulnerabilities. The TOE counters the threat [T.LOWEXP] as it resists penetration attacks performed by an attacker possessing minimal attack potential. The TOE is tested and vulnerabilities which would be exploitable by attacker with low attack potential have been eliminated.	O.EAL
P.PASSWORD T.DEVICECOMPROMISE	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The Security Objective [O.IDAUTH] is upheld (and the TOE counters the threat) by the TOE requiring authentication of user accounts prior to any TOE function access. The policy is used to establish passwords that help the TOE effectively guard against attack.	O.IDAUTH
P.PERSONNEL T.EXCEEDPRIV	The TOE shall ensure that authorized users do not exceed their assigned privileges/roles. The Security Objective [O.PRIVILEGE] is upheld (and the threat is reduced) by the TOE assigning privileges to users such as the administrator versus a user and verify the privilege level whenever a user attempts to access TSF functionality. The policy ensures that the users of the TOE understand their privileges and responsibilities.	O.PRIVILEGE
T.EXCEEDPRIV T.NODETECT P.PASSWORD	The TOE must be able to identify and authenticate users and administrators prior to allowing access to TOE Security functions and data. The Security Objective [O.SECFUN] is upheld by the TOE's strong password policy, assignment of privileges to users such as the administrator; and audit of applicable operations so that a user may be caught. The TOE reduces each of the threats by requiring any entity accessing the TSF to be authenticated and verifying the privilege level of the entity after authentication and prior to allowing access. The policy ensures that the authentication credentials used in the authentication process are strong and provide the appropriate security strength.	O.SECFUN
T.DEVICECOMPROMISE T.EXCEEDPRIV T.ZONECOMPROMISE	The TOE shall prevent unauthorized modification to its security functions and configuration data. The Security Objective [O.SECUREOPERATION] is upheld by the TOE will be correctly configured in accordance with a security policy which will prevent bypass of the TSF; and the TOE Security Policy can only be altered by an authorized administrator. The TOE reduces each of the threats by requiring any entity accessing the TSF to be authenticated and verifying the privilege level of the entity after authentication and prior to allowing access. Only after the entity has been	O.SECUREOPERATE

Threat or Policy	Rationale	Objectives
	authenticated and privileges verified can it access/modify the configuration data.	
T.DEVICECOMPROMISE	The TOE shall prevent unauthorized disclosure of management traffic dealing with the configuration and viewing of TOE devices for those TOE devices that are part of a WAAS solution. The TOE reduces this threat by using encryption to protect communications to and from TOE components (thus reducing the possibility of an unauthorized entity view data).	O.WAASPROTECT
T.DEVICECOMPROMISE T.ZONECOMPROMISE	The TOE shall ensure that only those authorized entities that are part of a WAAS solution are granted access to WAAS services as defined by the authorized user. The TOE reduces these threats by verifying that entities attempting to access TOE resources are actually allowed access to the requested resources.	O.WAASSOLUTION

Table 16: Threats/Assumptions/Policies to Environment Security Objectives Rationale

Security Objectives for the Environment	Rationale	Threat, Policy, or Assumption
OE.AUTHENTICATIONSERVER	The objective [OE. AUTHENTICATIONSERVER] upholds the following Policy: [P.PASSWORD] with the TOE environment optionally providing trusted authentication and authorization services for use with the TOE; protocols used for these services are restricted to either RADIUS, TACACS+ or Windows Authentication Server. These servers provide the ability to set strong password requirements and enforce this policy.	P.PASSWORD
OE.MANAGEMENTLAN	The objective [OE.MANAGEMENTLAN} upholds the following Assumption: [A.MANAGEMENTLAN] as the environment provides the TOE with a trusted management network that includes optional NTP and AAA services. The objective provides the trusted management LAN described in the assumption.	A.MANAGMENTLAN
OE.PERSONNEL	The objective [OE.PERSONNEL] upholds the following Policy: [P.PERSONNEL] as those responsible for the TOE will ensure that administrators, operators and maintainers have been trained sufficiently to configure, operate, and maintain the TOE in a secure and trusted manner in accordance with the guidance documentation. The objective provides that the personnel are trained per the policy.	P.PERSONNEL
OE.SECUREMANAGE	The objective [OE.SECUREMANGE] upholds the following Assumptions [A] and Policies [P]: [A.NO-EVIL] as the objective ensures that those responsible for the operation of the TOE and interconnected switches and routers management and configuration of the security functions of the	A.NOEVIL A.PHYSICAL A.TIMESOURCE A.ZONECONNECT P.PASSWORD P.PERSONNEL

Security Objectives for the Environment	Rationale	Threat, Policy, or Assumption
	TOE are undertaken by trusted staff that are non-hostile and follow all administrator guidance. [A.PHYSICAL] the TOE will be maintained in a physically secure environment. The objective ensures that the users verify that the environment is secure. [A.TIMESOURCE] TOE will be configured to interface only to trusted clock sources. The objective ensures that administrators only configure the use of a trusted clock source. [A.ZONECONNECT] the TOE will be initiated from a management station connected to a trusted network. The object ensures that management traffic only originates from the trusted network. [P.PASSWORD] the TOE and any actions will be performed securely through the creation of strong passwords in accordance with industry best practices. The objective ensures that the password policy that is enforced in the environment. [P.PERSONNEL] must ensure management and configuration of the security functions of the TOE are undertaken by trusted staff trained in the secure operation of the TOE. The objective ensures that the required training is provided.	

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE.

5.1 Conventions

Common Criteria (CC) defines operation on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignments: indicated by [bracketed text].
- Refinements: indicated by **bold text** and denoted by ~~striking through the removed text~~ as required
- Selections: indicated by *underlined and italicized text.*

Explicitly stated SFRs are identified by having a label '(EXP)' after the requirement name for the TOE SFRs.

5.2 TOE Security Functional Requirements

The security functional requirements for this Security Target consist of the following components from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1 with the following exceptions

A. FCS_CKM.5: used to accurately specify SSLv3.1/TLSv1 key establishment
B. FCS_CKM.6: used to accurately specify SSHv2.0 key establishment

Table 17: TOE Security Functional Requirements

Requirement Class	Requirement Components
FAU: Security Audit Class	
FAU_GEN.1	Audit Data Generation
FAU_SAR.1	Audit Review
FCS: Cryptographic Support	
FCS_CKM.1	Cryptographic key generation (Disk)
FCS_CKM.5	SSL v3.0, and TLS v1.0 Symmetric Cryptographic Key Establishment
FCS_CKM.6	SSH Symmetric Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1(1)	Cryptographic Operation (SSL/TLS – Encryption/Decryption)
FCS_COP.1(2)	Cryptographic Operation (SSH – Encryption/Decryption)
FCS_COP.1(3)	Cryptographic Operation (Disk Encryption)
FCS_COP.1(4)	Cryptographic Operation (Disk Encryption)
FDP: User Data Protection Class	
FDP_ACC.1(1)	Subset Access Control
FDP_ACC.1(2)	Subset Access Control
FDP_ACF.1(1)	Security Attribute Based Access Control
FDP_ACF.1(2)	Security Attribute Based Access Control
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Simple Security Attributes

Requirement Class	Requirement Components
FIA: Identification and Authentication Class	
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Verification Of Secrets
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.5	Multiple Authentication Mechanisms
FIA_UID.2	User Identification Before Any Action
FMT: Security Management Class	
FMT_MOF.1	Management of Security Functions Behaviour
FMT_MSA.1(1)	Management of Security Attributes
FMT_MSA.1(2)	Management of Security Attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1(1)	Management of TSF data
FMT_MTD.1(2)	Management of TSF data
FMT_MTD.1(3)	Management of TSF data
FMT_MTD.1(4)	Management of TSF data
FMT_MTD.1(5)	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT: Protection of the TSF Class	
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_STM.1	Reliable Time Stamps
FTA: TOE access Class	
FTA_SSL.3	TSF-Initiated Termination
FTA_TSE.1	TOE Session Establishment
FTP: Trusted path/channels Class	
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1	Trusted Path

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) [User login and logout events on the CM GUI, user login on the TOE CLI interface, AAA events from optional external authentication servers, security relevant commands executed by administrator, or authorized administrator defined user, traffic denied because of an IP ACL policy].

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

Event	Information
User login and logout events on the CM GUI	**Date and time, type of event, the identity of the administrator, the IP address from where the action took place**
User login on the TOE CLI interface	**Date and time, type of event, the identity of the administrator**
AAA events from optional external authentication servers	**Date and time, type of event, the TOE component on which the event took place, the outcome of the event**
Security relevant commands	**Date and time, shell from which the command was**

executed by administrator or authorized administrator defined user	**issued, the command that completed**
Traffic denied because of an IP ACL policy	**Date and time, the TOE component on which the event took place, the type of event, the IP address from which the traffic was generated, the IP address for which the traffic was destined**

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the **ST**, [no other audit relevant information].

Dependencies: FPT_STM.1

FAU_SAR.1 Audit Review

Hierarchical to: No other Components.

FAU_SAR.1.1 The TSF shall provide [

- WAAS GUI Administrator (Admin),
- WAAS GUI Administrator (custom defined privilege),
- WAAS CLI Administrator (privileged),
- WAAS CLI Administrator (custom defined privilege) - if the role is defined with authorization to create role assignments and definitions]

with the capability to read [all audit information for which the role is authorized to access] 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

FCS_CKM.1 Cryptographic key generation (WAE Disk and Secure Store Encryption Keys)

Hierarchical to: No other Components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [strong random number generation algorithm (SecureRandom SHA1PRNG implementation by Sun Microsystems)] and specified cryptographic key sizes [256 bits] that meet the following: [FIPS 140-2 Statistically RNG (minimal) and RFC1750].

Dependencies: [FCS_CKM.2 or FCS_COP.1]
FCS_CKM.4
FMT_MSA.2

FCS_CKM.5 SSL v3.0, and TLS v1.0 Symmetric Cryptographic Key Establishment

Hierarchical to: No other Components.

FCS_CKM.5.1 The TSF shall provide the following cryptographic key establishment in accordance with [SSL version 3.0 key establishment, and TLS version 1.0 key establishment] that meets the following: [N/A (SSL v3.0), RFC 2246 (TLS v1.0)].

A. The ciphersuites used in conforming to the key establishment schemes are as follows:[
   a. DHE-RSA-WITH-3DES-EDE-CBC-SHA
   b. DHE-RSA-WITH-AES-128-CBC-SHA
   c. DHE-RSA-WITH-AES-256-CBC-SHA
   d. RSA-WITH-3DES-EDE-CBC-SHA
   e. RSA-WITH-AES-128-CBC-SHA
   f. RSA-WITH-AES-256-CBC-SHA

Dependencies: FCS_COP.1
FCS_CKM.4

Extended Requirements Rationale – FCS_CKM.5:

A. Class – The FCS class of SFRs identifies cryptographic functionality provided by the TOE. FCS_CKM.5 describes the cryptographic functionality associated with the SSL/TLS session establishment provided by the TOE. This is cryptographic functionality and consistent with the FCS class of SFRs.

B. Family – This SFR family addresses cryptographic key management. This SFR addresses the establishment of cryptographic sessions for TLS/SSL. This is consistent with the SFR family definition.

C. Component – This is the fifth component in the family. This is why the component is identified as "5."

FCS_CKM.6 SSH Symmetric Cryptographic Key Establishment

Hierarchical to: No other Components.

FCS_CKM.6 The TSF shall provide the following cryptographic key establishment in accordance with [SSH version 2.0 key establishment] that meets the following: [RFC 4253].

A. The encryption cipher used in negotiating the SSH key establishment scheme are as follows:[
   a. 3des-cbc
   b. Blowfish-cbc
   c. Twofish256-cbc
   d. Twofish-cbc

   e. Twofish192-cbc
   f. Twofish128-cbc
   g. Aes256-cbc
   h. Aes192-cbc
   i. Aes128-cbc
   j. Serpent256-cbc
   k. Serpent192-cbc
   l. Serpent128-cbc
   m. Idea-cbc]

B. The MACs used in negotiating the SSH key establishment scheme are as follows:[
   a. Hmac-sha1
   b. Hmac-sha1-96
   c. Hmac-md5
   d. Hmac-md5-96
   e. None]

C. The key exchange methods used in negotiating the SSH key establishment scheme are as follows:[
   a. Diffie-hellman-group1-sha1
   b. Diffie-hellman-group14-sha1]

D. The public key and/or certificate formats used in negotiating the SSH key establishment scheme are as follows:[
   a. Ssh-dss
   b. Ssh-rsa
   c. Pgp-sign-rsa
   d. Pgp-sign-dss]

Dependencies: FCS_COP.1
FCS_CKM.4

Extended Requirements Rationale – FCS_CKM.6:

D. Class – The FCS class of SFRs identifies cryptographic functionality provided by the TOE. FCS_CKM.6 describes the cryptographic functionality associated with the SSH session establishment provided by the TOE. This is cryptographic functionality and consistent with the FCS class of SFRs.

E. Family – This SFR family addresses cryptographic key management. This SFR addresses the establishment of cryptographic sessions for SSH. This is consistent with the SFR family definition.

A. Component – This is the sixth component in the family. This is why the component is identified as “6.”

FCS_CKM.4 Cryptographic Key Destruction

Hierarchical to: No other Components.

FCS_CKM.4 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [FIPS 140-2].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]
FMT_MSA.2

FCS_ COP.1(1): Cryptographic Operation (SSL/TLS – Encryption/Decryption)

Hierarchical to: No other Components.

FCS_COP.1(1) The TSF shall perform [encryption and decryption] in accordance with **the following** ~~a~~ specified cryptographic algorithm**s** [AES and Triple-DES] and cryptographic key sizes [128, 168, 192, and 256] that meet the following: [

a. FIPS 197 (AES)
b. FIPS 46-3 (Triple-DES)].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1],
FCS_CKM.4,
FMT_MSA.2

FCS_COP.1(2) Cryptographic Operation (SSH – Encryption/Decryption)

Hierarchical to: No other Components.

FCS_COP.1(2) The TSF shall perform [encryption and decryption] in accordance with **the following** ~~a~~ specified cryptographic algorithm**s** [Triple-DES (CBC mode), blowfish (CBC mode), twofish (CBC mode), AES (CBC mode), serpent (CBC mode), and IDEA (CBC mode)] and cryptographic key sizes [128, 192, and 256 bits] that meet the following: [

a. N/A (Blowfish)
b. N/A (Twofish)
c. N/A (IDEA)
d. FIPS 46-3 (Triple-DES)
e. FIPS 197 (AES)
f. N/A (Serpent)].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]
FCS_CKM.4
FMT_MSA.2

FCS_ COP.1(3): Cryptographic Operation (Disk - Encryption)

Hierarchical to: No other Components.

FCS_COP.1(3) The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES-CBC] and cryptographic key sizes [256 bits] that meet the following: [FIPS PUB 197].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1],
FCS_CKM.4,
FMT_MSA.2

FCS_ COP.1(4): Cryptographic Operation (Hash)

Hierarchical to: No other Components.

FCS_COP.1(4) The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [N/A] that meet the following: [FIPS PUB 180-2].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1],
FCS_CKM.4,
FMT_MSA.2

FDP_ACC.1(1) Subset Access Control (Administrative RBAC)

Hierarchical to: No other Components.

FDP_ACC.1(1).1 The TSF shall enforce the [Role Based Access Control Policy] on [

- Subject: Processes acting on behalf of authenticated user;
- Objects: GUI elements, CLI commands;
- Operations: Exercise GUI Elements/CLI Elements].

Dependencies: FDP_ACF.1

FDP_ACC.1(2) Subset Access Control (Discretionary Access Control)

Hierarchical to: No other Components.

FDP_ACC.1(2).1 The TSF shall enforce the [Discretionary Access Control Policy] on [

- Subject: Processes acting on behalf of file users;
- Objects: Cached named files;
- Operations: Read and/or write].

Dependencies: FDP_ACF.1

FDP_ACF.1(1) Security Attribute Based Access Control (Administrative RBAC)

Hierarchical to: No other Components.

FDP_ACF.1(1) The TSF shall enforce the [Role Based Access Control Policy] to objects based on the following: [

- Processes acting on behalf of authenticated user (Subject)
  - User identity (GUI and CLI users)
  - Role assignment (GUI user)
  - Domain assignment (GUI users)
  - Privilege (CLI user)
- GUI elements (Object)
  - Role assignment
  - Domain assignment
- CLI commands (Object)
  - Privilege].

FDP_ACF.1(1).2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- An administrator is able to exercise GUI elements if the role definition for the role assignment of the authenticated user explicitly grants access (create, modify, query, initialize, change-default, disable, enable, and determine the behavior of) to the GUI element and the domain assignment of the User and GUI element match or
- When not using TACACS+ per command authorizations an administrator is able to exercise CLI elements if the role assignment of the authenticated user explicitly grants access to the CLI command or
- When using TACACS+ per command authorizations an administrator is able to exercise CLI elements when an explicit allow response is received from an IT environment remote TACAS+ server].

FDP_ACF.1(1).3 The TSF shall explicitly authorise access of subjects to objects based on the [none].

FDP_ACF.1(1).4 The TSF shall explicitly deny access of subjects to objects based on the following rules: [none].

Dependencies: FDP_ACC.1,
FMT_MSA.3

FDP_ACF.1(2) Security Attribute Based Access Control (Discretionary Access Control)

Hierarchical to: No other Components.

FDP_ACF.1(2).1 The TSF shall enforce the [Discretionary Access Control Policy] to objects based on the following: [

- Processes acting on behalf of users (subjects)
  - User identity,
- Cached named files (objects)
  - File server on which the original copy of the file is resident].

FDP_ACF.1(2).2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- The TOE enforces the decision of the file server on which the original copy of a cached file is resident to allow or disallow read and/or write access to a cached file].

FDP_ACF.1(2).3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1(2).4 The TSF shall explicitly deny access of subjects to objects based on the following: [

- The TOE is operating in offline mode].

Dependencies: FDP_ACC.1,
FMT_MSA.3

FDP_IFC.1 Subset Information Flow Control

Hierarchical to: No other Components.

FDP_IFC.1.1 The TSF shall enforce the [Device Information Flow Control Policy] on [

- Subject: external IT entities that send information destined for the TOE;
- Information: traffic destined for the TOE;
- Operations: permit or deny].

Dependencies: FDP_IFF.1

FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other Components.

FDP_IFF.1.1 The TSF shall enforce the [Device Information Flow Control Policy] based on the following types of subject and information security attributes: [

- external IT entity (subject):
  - Presumed address;
- traffic (information):
  - TOE interface on which the traffic is received,
  - Presumed address of source subject,
  - IP address of destination subject,
  - Transport layer protocol
  - Source Port
  - Destination Port
  - ICMP Message Type].

FDP_IFF.1.2 The TSF shall permit or deny an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- Traffic destined for a TOE interface for which an IP ACL is applied with security attributes that match an administratively configured permit policy rule is permitted, or,
- Traffic destined for a TOE interface for which an IP ACL is applied with security attributes that match an administratively configured deny policy rule is denied. Traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or,
- Traffic destined for a TOE interface for which an IP ACL is applied with security attributes that match an administratively configured deny-and-log policy rule is denied and a copy of the traffic is logged by the TOE

The permit/deny polices for traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of permit/deny policies include: presumed address. The information attributes that are available for the creation of permit/deny include: Source IP address, Destination IP address, Protocol, Source Port, Destination Port, ICMP Message type].

FDP_IFF.1.3 The TSF shall enforce the [no additional rules].

FDP_IFF.1.4 The TSF shall provide the following [no additional capabilities].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [no additional capabilities].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [if an IP ACL is applied to a TOE interface and traffic destined for a TOE interface does not match an administratively configured IP ACL permit rule, the traffic flow is denied].

Dependencies: FDP_IFC.1,
FMT_MSA.3

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 **TOE Administrative** users: [

- Authentication credentials,
- User identifiers,
- Role assignments,
- Domain].

Dependencies: No dependencies.

FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

- At least 8 characters long
- Cannot contain all of the same characters (e.g., 99999999)
- Cannot contain all consecutive characters (e.g., 12345678)].

Dependencies: No dependencies

FIA_UAU.2 User Authentication Before Any Action

Hierarchical to: FIA_UAU.1

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

FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other Components.

FIA_UAU.5.1 The TSF shall provide [a local authentication mechanism and a remote authentication mechanism] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following rules:

- For local authentication: username and password;
- For remote CLI authentication: username and password;
- For remote web authentication: username and password; and
- Optionally, for local and remote username and password authentication, use of an external authentication server].

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 identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other Components.

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, and modify the behaviour of the functions [of remote management protocols and authentication server configuration] to [

- WAAS GUI Administrator (Admin),
- WAAS GUI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to manage remote protocol and authentication server configuration
- WAAS CLI Administrator (Privileged),
- WAAS CLI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to create role assignments and definitions].

Dependencies: FMT_SMR.1,
FMT_SMF.1

FMT_MSA.1(1) Management of Security Attributes

Hierarchical to: No other Components.

FMT_MSA.1(1).1 The TSF shall enforce the [Role Based Access Control Policy] to restrict the ability to query, modify, and [create] the security attributes [role assignments and role definitions] to [

- WAAS GUI Administrator (Admin),
- WAAS CLI Administrator (Privileged),
- WAAS CLI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to create role assignments and definitions].

Dependencies: [FDP_ACC.1 or FDP_IFC.1],
FMT_SMR.1,
FMT_SMF.1

FMT_MSA.1(2) Management of security attributes

Hierarchical to: No other Components.

FMT_MSA.1(2).1 The TSF shall enforce the [Device Information Flow Policy] to restrict the ability to *query, modify, and* [create] the security attributes [found in permit/deny policies, including, subject attributes: presumed address and information attributes: Source IP address, Destination IP address and Protocol] to [

- WAAS GUI Administrator (Admin),
- WAAS CLI Administrator (Privileged),
- WAAS CLI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to create role assignments and definitions].

Dependencies: [FDP_ACC.1 or FDP_IFC.1],
FMT_SMR.1,
FMT_SMF.1.

FMT_MSA.3 Static Attribute Initialisation

Hierarchical to: No other Components.

FMT_MSA.3.1 The TSF shall enforce the [Device Information Flow Policy] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [no role] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1,
FMT_SMR.1

FMT_MTD.1(1) Management of TSF Data

Hierarchical to: No other Components.

FMT_MTD.1(1).1 The TSF shall restrict the ability to *query, and clear* the [audit trail] to [

- WAAS GUI Administrator (Admin),
- WAAS GUI Administrator (Custom Defined Privilege)
- WAAS CLI Administrator (Privileged) (clear only),
- WAAS CLI Administrator (Custom Defined Privilege) (clear only) - if the role is defined with authorizations to create role assignments and definitions].

Dependencies: FMT_SMR.1,
FMT_SMF.1

FMT_MTD.1(2) Management of TSF Data

Hierarchical to: No other Components.

FMT_MTD.1(2).1 The TSF shall restrict the ability to *modify* and [initialize] the [user security attributes (other than authentication data), roles, definitions, and IP ACLs] to [

- WAAS GUI Administrator (Admin),
- WAAS CLI Administrator (Privileged),
- WAAS CLI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to create role assignments and definitions)].

Dependencies: FMT_SMR.1,
FMT_SMF.1

FMT_MTD.1(3) Management of TSF Data

Hierarchical to: No other Components.

FMT_MTD.1(3).1 The TSF shall restrict the ability to *modify* and [initialize] the [user authentication credentials] to [

- WAAS GUI Administrator (Admin),
- WAAS GUI Administrator (Custom Defined Privilege) (Modify only) - if the role is defined with authorizations to create role assignments and definitions),
- WAAS CLI Administrator (Privileged),
- WAAS CLI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to create role assignments and definitions)].

Dependencies: FMT_SMR.1,
FMT_SMF.1

FMT_MTD.1(4) Management of TSF Data

Hierarchical to: No other Components.

FMT_MTD.1(4).1 The TSF shall restrict the ability to *change_default*, [modify] the [user inactivity threshold for an established CLI or CM GUI web session] to [

- WAAS GUI Administrator (Admin) (both CLI or CM GUI inactivity period),
- WAAS GUI Administrator (Custom Defined Privilege) (both CLI or CM GUI inactivity period) - if the role is defined with authorizations to create role assignments and definitions)
- WAAS CLI Administrator (Privileged) (CLI inactivity period only),
- WAAS CLI Administrator (Custom Defined Privilege) (CLI inactivity period only) - if the role is defined with authorizations to create role assignments and definitions)].

Dependencies: FMT_SMR.1,
FMT_SMF.1

FMT_MTD.1(5) Management of TSF Data

Hierarchical to: No other Components.

FMT_MTD.1(5).1 The TSF shall restrict the ability to [modify] the [TOE clock] to [

- WAAS GUI Administrator (Admin),
- WAAS GUI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to create role assignments and definitions)
- WAAS CLI Administrator (Privileged),
- WAAS CLI Administrator (Custom Defined Privilege) - if the role is defined with authorizations to create role assignments and definitions)].

Dependencies: FMT_SMR.1,
FMT_SMF.1

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 security management functions: [

- Read audit information; query, modify, and create role assignments and role definitions; query, modify, and create IP ACLs;
- Query and clear the audit trail initialize and modify user security attributes, role definitions and IP ACLs;
- Initialize user authentication credentials;
- Change default and modify inactivity threshold parameter; and
- Modify clock].

Dependencies: No dependencies.

FMT_SMR.1 Security Roles

Hierarchical to: No other Components.

FMT_SMR.1.1 The TSF shall maintain the roles [

- WAAS GUI Administrator,
- WAAS CLI Administrator (Privileged),
- WAAS GUI or CLI user with custom role assignments and privileges].

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

Dependencies: FIA_UID.1 Timing of identification.

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other Components.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE.

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 for its own use.

Dependencies: No dependencies.

FTA_SSL.3 TSF-Initiated Termination

Hierarchical to: No other Components.

FTA_SSL.3.1 The TSF shall terminate ~~an~~ **CLI** ~~interactive~~ **or CM GUI web administrative** session after ~~a~~ **an** [an administratively configured period of inactivity].

Dependencies: No dependencies.

FTA_TSE.1 TOE Session Establishment

Hierarchical to: No other Components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [a configured IP ACL deny policy].

Dependencies: No dependencies.

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other Components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit *the TSF* to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall use a trusted channel for the following functions: [optional AAA services].

Dependencies: No dependencies.

FTP_TRP.1 Remote Administration Trusted Channel

Hierarchical to: No other Components.

FTP_TRP.1.1 FTP_TRP.1.1 — The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*.
FTP_TRP.1.2 FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.
FTP_TRP.1.3 FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial user authentication* [and remote administration]

Dependencies: No dependencies.

Application note: Secure remote administration is provided by SSL or SSH

5.3 Functional Requirement Dependency Rationale

This section of the Security Target demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate dependent SFRs. The following table lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale.

Not applicable in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 18: SFR Dependency Rationale

TOE SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Satisfied
FAU_SAR.1	FAU_GEN.1	Satisfied
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	Satisfied by FCS_COP.1(3)
	FCS_CKM.4	Satisfied
	FMT_MSA.2	N/A since the keys are automatically generated by the TOE.
FCS_CKM.5	FCS_COP.1	Satisfied by FCS_COP.1(1)
	FCS_CKM.4	Satisfied
FCS_CKM.6	FCS_COP.1	Satisfied by FCS_COP.1(2)
	FCS_CKM.4	Satisfied
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Satisfied by FCS_CKM.1, FCS_CKM.5, FCS_CKM.6
	FMT_MSA.2	N/A since the keys are automatically generated by the TOE.
FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Satisfied by explicitly stated SFR FCS_CKM.5
	FCS_CKM.4	Satisfied
	FMT_MSA.2	N/A since the keys are automatically established by the TOE per TLSv1.0.
FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Satisfied by explicitly stated SFR FCS_CKM.6
	FCS_CKM.4	Satisfied
	FMT_MSA.2	N/A since the keys are automatically established by the TOE per SSHv2.
FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Satisfied by FCS_CKM.1
	FCS_CKM.4	Satisfied
	FMT_MSA.2	Not required since the keys are automatically established by the TOE.
FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Not required since hashing does not use keys.
	FCS_CKM.4	Not required since hashing does not use keys.

TOE SFR	Dependency	Rationale
	FMT_MSA.2	Not required since hashing does not use keys.
FDP_ACC.1(1)	FDP_ACF.1	Satisfied
FDP_ACC.1(2)	FDP_ACF.1	Satisfied
FDP_ACF.1(1)	FDP_ACC.1	Satisfied
	FMT_MSA.3	N/A since the set of objects associated with the access control SFR is fixed
FDP_ACF.1(2)	FDP_ACC.1	Satisfied
	FMT_MSA.3	The security attributes of the CIFS files on which this policy is applied is controlled by the originating file servers in the IT environment. The TOE does not maintain or control the attributes. Therefore, this is not required.
FDP_IFC.1	FDP_IFF.1	Satisfied
FDP_IFF.1	FDP_IFC.1	Satisfied
	FMT_MSA.3	Satisfied
FIA_ATD.1	No dependencies.	Not applicable.
FIA_SOS.1	No dependencies.	Not applicable.
FIA_UAU.2	FIA_UID.1	Satisfied
FIA_UAU.5	No dependencies.	Not applicable.
FIA_UID.2	No dependencies.	Not applicable.
FMT_MOF.1	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1],	Satisfied by FDP_ACC.1(1)
	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1],	Satisfied by FDP_IFC.1
	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MSA.3	FMT_MSA.1	Satisfied
	FMT_SMR.1	Satisfied
FMT_MTD.1(1)	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MTD.1(2)	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MTD.1(3)	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MTD.1(4)	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MTD.1(5)	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_SMF.1	No dependencies.	Not applicable.
FMT_SMR.1	FIA_UID.1	Satisfied
FPT_ITT.1	No dependencies.	Not applicable.
FPT_STM.1	No dependencies.	Not applicable.
FTA_SSL.3	No dependencies.	Not applicable.
FTA_TSE.1	No dependencies.	Not applicable.
FTP_ITC.1	No dependencies.	Not applicable.
FTP_TRP.1	No dependencies.	Not applicable.

5.3.1 Assurance Requirement Dependency Rationale

All assurance requirement dependencies are satisfied.

5.4 TOE Security Requirements Rationale

The purpose of this section is to present the functional and assurance requirements in this ST effectively support the other, and their combination meets the stated security objectives. The following tables show that each security requirement (and SFRs in particular) is *necessary*, that is, each security objective is addressed by at least one security requirement, and vice versa.

Table 19: Security Requirements Rationale

Objective	Requirement	Rationale
O.AUDIT	FAU_GEN.1	Requires the capability to generate records of security-relevant events, including security relevant commands executed by the user in order to be able to hold a user accountable for their actions.
	FAU_SAR.1	Requires that authorized users will have the capability to read and interpret data stored in the audit logs such that security breaches can be detected.
	FMT_MTD.1(1)	Supports this objective because it restricts the ability to access the audit trail to the administrator so that the integrity of the audit trail is controlled by an authorized user.
	FMT_MTD.1(5)	Supports this objective because it restricts the ability to modify the TOE clock to the administrator so that the integrity of audit timestamps are controlled by an authorized user.
	FMT_SMF.1	Provides the function for reading the audit trail and to query, and clear the audit trail.
	FPT_STM.1	Requires the provision of reliable time stamps that can be associated with security-relevant events.
O.EAL	ADV_ARC.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ADV_TDS.3	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ADV_FSP.4	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ADV_IMP.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	AGD_OPE.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	AGD_PRE.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ALC_CMC.4	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ALC_LCD.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ALC_TAT.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested

Objective	Requirement	Rationale
		and resistant to a penetration from an attacker with low attack potential.
	ALC_CMS.4	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ALC_DEL.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ALC_DVS.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ASE_CCL.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ASE_REQ.2	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ASE_ECD.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ASE_INT.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ASE_OBJ.2	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ASE_SPD.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ASE_TSS.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ATE_COV.2	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ATE_IND.2	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ATE_DPT.2	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	ATE_FUN.1	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
	AVA_VAN.3	All the Security Assurance Requirements together satisfy this objective. The EAL4 requirements provide the evidence the TOE is structurally tested and resistant to a penetration from an attacker with low attack potential.
O.IDAUTH	FIA_UAU.2	Supports the authentication of a user's identity prior to allowing access to TOE functions and data.
	FIA_UAU.5	Specifies the authentication mechanism that can be used to authenticate a user prior to being allowed access to any mediated functions on the TOE.
	FIA_UID.2	Specifies the user must identify themselves prior to being allowed access to any mediated functions of the TOE.

Objective	Requirement	Rationale
	FIA_SOS.1	Supports the authentication mechanism by enforcing the minimum complexity of administrative passwords.
	FMT_MTD.1(3)	FMT_MTD.1(3) supports the authentication mechanism by allowing the administrator to set up accounts and initialize the authentication credentials.
	FTP_ITC.1	Allows authentication to be performed by an external authentication server. The results of which are protected and enforced by the TOE.
O.PRIVILEGE	FDP_ACC.1(1)	Requires that all user actions resulting in the access to TOE security functions and configuration data are controlled by roles.
	FDP_ACF.1(1)	Supports FDP_ACC.1 (1) by ensuring that access to TOE security functions and configuration data is based on the assigned user role.
	FIA_ATD.1	Associates the user security role with their user identity which then determines the user's set of privileges.
	FMT_MSA.1(1)	Specifies that only users with a privileged role can access the TOE security functions and related configuration data.
	FMT_MTD.1(2)	Restricts the ability to modify and initialize role definitions to administrators.
	FMT_SMF.1	Details the security management functions relevant to the TOE, including the configuration of user roles (which determine the user privileges).
	FMT_SMR.1	Ensures that the TOE maintains the administrator role as well as other administrator defined roles.
O.SECUREOPER	FDP_ACC.1(1)	Requires that all user actions resulting in the access to TOE security functions and configuration data are controlled by roles to prevent unauthorized activity.
	FDP_ACF.1(1)	Supports FDP_ACC.1(1) by ensuring that access to TOE security functions and configuration data is done so in accordance with the role definition.
	FDP_IFC.1	Requires that all IP packets that flow to the TOE (This includes management session data) are subject to inspection prior to being processed if a IP ACL exists.
	FDP_IFF.1	Supports FDP_IFC.1 by ensuring that IP packets flowing to the TOE (This includes management session data.) do so in accordance with the rules of the information flow control policy.
	FMT_MOF.1	Requires that the ability to manage the security functions and access the remote management and authentication server configuration is restricted to users with a privileged role.
	FMT_MSA.1(1)	Specifies that only users with a privileged role can manage the TOE security functions and related configuration data.
	FMT_MSA.1(2)	Supports the Device Information Flow Policy to restrict who can configure the security attributes of the policy which protects the TOE from unauthorized modifications.
	FMT_MSA.3	Ensures that the default values of security attributes are restrictive in nature as to enforce the access control and information flow control security policies for the TOE.
	FMT_MTD.1(2)	Supports the initialization of IP ACLs to control authorized access to the TOE.
	FMT_MTD.1(4)	Limits the inactivity period for interactive session so that unauthorized access can be thwarted from trying to take advantage of an unattended session.
	FMT_SMF.1	Specifies the management capabilities of the TSF to include security functions that can disable, enable, modify the behavior of security function and configuration of the TOE.
	FTA_SSL.3	Ensures the termination of an interactive CLI or web session in order to mitigate session hijacking of a user terminal left unattended.

Objective	Requirement	Rationale
	FTA_TSE.1	Allows the TOE to deny session establishment for all users and devices based on pre-defined conditions.
O.WAASPROTE(	FDP_IFC.1	Establishes the policy to control access of external entities (devices) to the TOE by the use of IP ACLs. This policy enforces which TOE components the TOE will communicate for the TOE solution.
	FDP_IFF.1	Establishes the policy to control access of external entities (devices) to the TOE by the use of IP ACLs. This policy enforces which TOE components the TOE will communicate for the TOE solution.
	FPT_ITT.1	Provides for the protected communication among WAAS solution devices. This ensures that only WAAS solution devices can communicate with each other.
	FCS_CKM.1	Provides cryptographic support for the generation of keys for Disk encryption.
	FCS_CKM.5	Provides cryptographic support f or generation of keys for TLS.
	FCS_CKM.6	Provides cryptographic support for the generation of keys for SSH.
	FCS_CKM.4	Provides key destruction cryptographic support.
	FCS_COP.1(1)	Provides TLS encryption support.
	FCS_COP.1(2)	Provides SSH encryption support.
	FCS_COP.1(3)	Provides Disk encryption support.
	FCS-COP.1(4)	Provides SHA hash support.
	FTP_TRP.1	Provides secure remote administrative and optional monitoring communication.
O.WAASSOLUTI	FDP_ACC.1(2)	Establishes the policy to only allow authorized file access to cached files.
	FDP_ACF.1(2)	Establishes the policy to only allow authorized file access to cached files.
	FDP_IFC.1	Establishes the policy to control access of external entities (devices) to the TOE by the use of IP ACLs.
	FDP_IFF.1	Establishes the policy to control access of external entities (devices) to the TOE by the use of IP ACLs.
	FMT_MSA.1(2)	Supports the Device Information Flow Policy to restrict who can configure the security attributes of the policy.
	FMT_MSA.3	Supports the Device Information Flow Policy to establish the default values of the security attributes for network access to the TOE.
	FMT_MTD.1(2)	Supports the modifying and initializing the IP ACLs to support the Device Information Flow Policy to restrict access to the TOE to authorized entities.
	FMT_SMF.1	Specifies the management capabilities of the TSF to include security functions that can create, modify and delete the configuration data (which includes managing the access parameters to other devices in a specific WAAS solution that is the TOE).
	FPT_ITT.1	Provides for the protected communication among WAAS solution devices. This ensures that only WAAS solution devices can communicate with each other.

5.5 TOE Security Assurance Requirements

The security assurance requirement for the TOE is the EAL4 augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 20: EAL4 Augmented with ALC_FLR.1 Components

Assurance Class	Assurance components
CC EAL4 Assurance Requirements	
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_TDS.3 Basic modular design
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_REQ.2 Derived security requirements
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_IND.2 Independent testing - sample
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis
Augmented Assurance Requirements	
ALC: Life-Cycle Support	ALC_FLR.1 Basic flaw remediation

5.5.1 Assurance Requirements Rationale

The ST is written with EAL4 augmented with ALC_FLR.1.

EAL4 was chosen because it permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 provides the developers and users a moderate to high level of independently assured security in conventional commercial TOEs.

EAL 4 is augmented by ALC_FLR.1 to help ensure that the customers can report the flaws and the flaws can be systematically corrected.

5.6 Subjects, Objects, Operations, Security Attributes, and External Entities

The following are used in the previous SFRs.

Users	**Authorized user:** These are administrative users of the TOE. These users access the TOE through either the TOE CLI or administrative GUI. **Pre-position user:** This user is configured and resident on an IT environment

	file server. This user account is assumed by the TOE to cache files from IT environment file servers prior to first access by a file user through the TOE. **Branch WAE devices that uses user name and password to retrieve preposition from the file server via Data Center WAE device:** The Branch WAE assumes the preposition user on a file server and caches files resident on the file server prior to first access by a file user through the TOE. The credentials used for prepositioning are configured by the TOE administrator.
Subject	**RBAC SFP subjects:** Processes acting on behalf of authenticated user **DAC SFP Subjects:** Processes acting on behalf of users. **Device Information Flow Control Policy SFP subjects:** External IT entities that send and receive information through the TOE.
Object/Information	**Objects controlled by the RBAC SFP:** GUI elements, CLI commands **Objects controlled by the DAC SFP:** cached named files **Information controlled by the Device Information Flow Control Policy SFP:** traffic sent to or through the TOE
Operations	**RBAC SFP operations:** Allow access, not allow access **DAC SFP operations:** Read/write operations **Device Information Flow Control Policy SFP operations:** Permit/deny **Other operations (found in FMT_*** requirements):** **Create:** Role assignments, and role definitions, IP ACLs **Modify:** Fle permissions associated with the cached files **Query, clear:** The audit trail **Initialize:** User authentication credentials **Change:** Default, modify – user inactivity threshold **Disable/enable, determine/modify the behavior of:** Remote management protocols and authentication server configuration. **Modify:** Clock
External Entities	**External entities found in Device Information Flow Control Policy SFP:** Any external IT entity attempting to send network traffic through the TOE. There is no limitation of the type of IT entity these devices may be.

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 21: How TOE SFRs Measures

<table>
<tr><th>SFRs</th><th>Rationale</th></tr>
<tr><td>FAU_GEN.1</td><td>The TOE generates an audit record that is stored internally within the TOE whenever an auditable event occurs. The types of events that cause audit records to be generated include,
<ul>
<li>User login and logout events on the CM GUI;</li>
<li>User login events on the TOE CLI interface</li>
<li>AAA events from external authentication servers;</li>
<li>traffic denied because of an IP ACL policy</li>
<li>Security relevant commands executed by administrator or authorized administrator defined user; including commands related to the following:
+ Management of roles,
+ Management of IP ACLs,
+ Management of I&A ,
+ Clock management,
+ Management of inactivity threshold.</li>
</ul>
Each of the events generated by the TOE contains the information specified in the SFR, as follows:
<table>
<tr><th>Event</th><th>Information</th></tr>
<tr><td>User login and logout events on the CM GUI</td><td>Date and time, type of event, the identity of the administrator, the IP address from where the action took place</td></tr>
<tr><td>User login on the TOE CLI interface</td><td>Date and time, type of event, the identity of the administrator</td></tr>
<tr><td>AAA events from optional external authentication servers</td><td>Date and time, type of event, the TOE component on which the event took place, the outcome of the event</td></tr>
<tr><td>Security relevant commands executed by administrator or authorized administrator defined user</td><td>Date and time, shell from which the command was issued, the command that completed</td></tr>
<tr><td>Traffic denied because of an IP ACL policy</td><td>Date and time, the TOE component on which the event took place, the type of event, the IP address from which the traffic was generated, the IP address for which the traffic was destined</td></tr>
</table>
Additionally, the startup and shutdown of the audit functionality is audited.</td></tr>
<tr><td>FAU_SAR.1</td><td>The TOE provides the ability for the administrators of the TOE to view all audit events stored within the TOE. The TOE provides a GUI interface that allows an administrative user to display the audit event to the management workstation..</td></tr>
</table>

SFRs	Rationale
	The WAAS Central Manager GUI, which is only available to those TOE devices that are configured as CMs, audits the creation and modification of TOE devices that occurs thru the interface along with those activities dealing with system configuration changes, modifications, and creations. The WAAS Central Manager GUI provides a capability to view the system audit logs generated by using the CM and the WAAS Central Manager GUI. Administrative access to audit logs is only granted to users whose role is authorized to access the audit records. The TOE verifies if the user's assigned role is authorized to access the audit records before granting access. The WAE Device Manager GUI, which is specific to and local to a TOE device, performs auditing and allows viewing of audit information for the CIFS File Cache functionality that is local to that TOE device. The audit records are stored on the hard disk as a combination of syslog and errlog files on a TOE device. The TOE records the start-up and shutdown of the audit functions, user actions and all security relevant commands executed by the user. The TOE records the date and time of each event, the type of event, the involved subject identity and the outcome of the event, where an outcome exists. The audit trail is log files stored on TOE devices that may be reviewed at any time. Audit review through the TOE CLI is facilitated using one of two commands, as follows: • #type-tail • #type These commands are only available to privileged WAAS CLI Administrators and custom WAAS CLI Administrators whose authorizations include the commands. The integrity of the audit logs is maintained by restricting access to the audit log to only authorized administrators. There are no interfaces other then interfaces controlled by the TOE that allows access to the audit logs. There is no way to modify the TOE audit records without proper authorization.
FCS_CKM.1	The data stored within the TOE is encrypted using AES-256 encryption. The encryption key used to encrypt the data is created using the SecureRandom SHA1PRNG provided by the TOE.
FCS_CKM.5	The TOE provides protected communication between the CM and application accelerator WAE devices using TLSv1. SSL/TLS protects the management communication between these TOE components. The TOE uses HTTPS for the Web GUIs available on the TOE devices. Using HTTPS protects the confidentiality and integrity of the TOE management that is carried out over this interface. In support of these operations, the TOE provides TLSv1/SSLv3 session establishment methods. The specific ciphersuites used for session establishment include, • DHE-RSA-WITH-3DES-EDE-CBC-SHA; • DHE-RSA-WITH-AES-128-CBC-SHA; • DHE-RSA-WITH-AES-256-CBC-SHA; • RSA-WITH-3DES-EDE-CBC-SHA; • RSA-WITH-AES-128-CBC-SHA; • RSA-WITH-AES-256-CBC-SHA.
FCS_CKM.6	The TOE protects remote CLI management and configuration sessions with SSH version 2.

SFRs	Rationale
	In support of these operations, the TOE provides SSHv2 session establishment methods. The specific cipher options used for session establishment are specified in the text of the SFR.
FCS_CKM.4	The TOE zeroizes all of the cryptographic keys used within the TOE after the key is no longer of use to the TOE.
FCS_COP.1(1)	The TOE provides protected communication between the CM and application accelerator WAE devices using TLSv1. SSL/TLS protects the management communication between these TOE components. The TOE uses HTTPS for the Web GUIs available on the TOE devices. Using HTTPS protects the confidentiality and integrity of the TOE management that is carried out over this interface. In support of these operations, the TOE provides the following symmetric encryption methods, RC2, Triple-DES, and AES.
FCS_COP.1(2)	The TOE protects remote CLI management and configuration sessions with SSH version 2. In support of these operations, the TOE provides the following symmetric encryption methods, Triple-DES (CBC mode), blowfish (CBC mode), twofish (CBC mode), AES (CBC mode), serpent (CBC mode), IDEA (CBC mode), and cast (CBC mode).
FCS_COP.1(3)	The data stored within the TOE is encrypted using AES-256 encryption.
FCS_COP.1(4)	The TOE provides SHS hashing in support of SSH and SSL/TLS.
FDP_ACC.1(1)	The TOE enforces role-based access restrictions on administrative access and authorization. Access to the administrative functionality of the TOE is permitted based on the role assigned to the user attempting to access the functionality. The decision to allow a user access to specific administrative functionality is based on the administratively configured permission assigned to the role(s) for which the user is associated. Authorized administrators connect to the TOE via a management workstation. Upon connection to the TOE, the administrator is prompted to provide credentials. After the presented credentials are verified, the user is allowed the access associated with the presented credentials.
FDP_ACC.1(2)	This SFR defines how the TOE provides access to cached files. The original copies of these files are created on file server in the IT environment. The goal of this SFP is to provide accelerated access to copies of the files cached within the TOE. Whenever a user attempts to access a file cached on the TOE, the TOE checks the file server. The file server responses to the TOE with an allow or deny access decision. The TOE enforces the decision provided by the file server.
FDP_ACF.1(1)	For security management via the WAAS Central Management GUI administrator defined roles are used. The TOE does not support the dynamic creation of new CLI or GUI elements. The TOE only allows authorized administrators the ability to define roles with custom permissions that defined access to the CLI/GUI elements. Whenever a user is created, the WAAS administrator assigns each user a role. The assigned role defines the GUI elements for which the user has access. Additionally, each administrator and GUI element is also assigned to a domain. These domains represent a collection of devices within the WAAS network. If the domain assigned to an administrator does not match the domain assigned to the GUI element, the administrator is not grant access.

SFRs	Rationale
	The TOE verifies the user's privileges prior to allowing access to any TOE administrative functionality. The TOE has two default roles of administrator for the WAAS Central Management GUI, WAAS GUI Administrator (admin) and "print". Only the "admin" role has the ability to do everything through using the GUI (it is a super user account). Only the "admin" role and the custom roles defined by the administrator are considered security relevant. The "print" administrator does not have any controls over any security functionality of the TOE. The "print" role is non-security relevant. For the GUI custom defined administrator, read or write access can be defined for any of the sections and subsections of the GUI. These sections include the following; Devices - Allows the administrator to go to the Dashboard and Alerts displays for your entire WAAS network and allows the administrator to choose a specific device or device group for which to configure WAAS services and general settings. The administrator can also view detailed device information and messages, and manage locations Monitor - Allows the administrator to see network traffic and other charts and reports to monitor the health and performance of your WAAS network. Report - Allows the administrator to manage and schedule reports for your WAAS network. Jobs - Allows the administrator to manage software update jobs. Configure - Allows the administrator to configure the main WAAS services (file, print, and application acceleration) and other settings. Admin - Allows the administrator to manage user accounts, passwords, licenses, and virtual blades, and view the system log. Locally authorized CLI administration has two access levels for CLI administrators, privileged and user. When a CLI administrator is created locally on the WAAS, the administrator is defined as a privileged administrator. Privileged CLI administrators are able to access every administrative command and capability available through the WAAS CLI. This allows the administrator to configure (create, modify, delete) the security features of the TOE device. A non-privileged CLI administrator is operating as a regular user with the only privileges of being able to view the settings and configurations of the TOE. Users assigned this role cannot perform security relevant operations. Actions carried out through the CLI of a TOE device are localized to that TOE device. The TOE additionally supports the definition of custom CLI administrators via TACACS+ per command authorization. In this case, a user account defined on an IT environment TACACS+ server can be associated with a user role defined as a list of TOE CLI commands the given user is authorized to execute (This list is comprised of existing CLI commands. There is not capability on the TOE to create new CLI commands.). Whenever a CLI command is received by the TOE for a custom defined administrator, the TOE sends a request to the TACACS+ server. The TACACS+ server then verifies whether the requested command is allowed for the user and sends an allowed or non-allowed response. The TOE then enforces the access decision issued by

SFRs	Rationale
	the TACACS+ server. When this option is used, the TOE only enforces the decision from TACACS+ server. The TOE does not actively decide access. Any commercially available AAA server that supports TACAC+ may be used. Note: That per command authorization is not available when using RADIUS or Window Authentication because it is not supported by the protocols.
FDP_ACF.1(2)	This SFR defines how the TOE provides access to cached files. The original copies of these files are created on file server in the IT environment. The goal of this SFR is to provide accelerated access to copies of the files cached within the TOE. Whenever a user attempts to access a file cached on the TOE, the TOE passes the user request to the originating file server. The originating file server then compares the requesting file user's permissions against the minimum file permissions associated with the original file resident on the file server. The file returns an allow or deny access decision to the TOE. The TOE then consequently either allow or deny access to the cached file based on the decision returned by the file server. Whenever a file request is made, the TOE asks the originating file server if the file should be served. If the file server says yes, then the file is served from the cache. If the file server says no, the file is not served. The TOE enforces the decision made by the file server. When the TOE is offline/disconnected it does not serve the file at all.
FDP_IFC.1	The TOE allows a privileged user to create and maintain IP-based, network based, access control lists for TOE management traffic traveling over Ethernet. The TOE has the ability to reject session establishment based on the port of network traffic defined by an IP ACL policy. The TOE has the ability to reject session establishment for interconnected TOE devices based on the IP ACL policies configured into specific TOE devices.
FDP_IFF.1	The TOE implements access control policies that are designed as protection for access to the TOE itself and not meant to filter traffic passed through the TOE. When traffic that meets an administratively configured IP ACL policy is passed to the TOE, the TOE makes an information flow decision to permit or deny the traffic. Traffic is permitted or denied, as follows, ▪ Traffic destined for a TOE interface for which an IP ACL is applied with security attributes that match an administratively configured permit policy rule is allowed to flow, or, ▪ Traffic destined for a TOE interface for which an IP ACL is applied with security attributes that match an administratively configured deny policy rule is denied. Traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or, ▪ Traffic destined for a TOE interface for which an IP ACL is applied with security attributes that match an administratively configured deny-and-log policy rule is denied and a copy of the traffic is logged by the TOE. The permit/deny polices for traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of permit/deny policies include: presumed address. The information attributes that are available for the creation of permit/deny include: Source IP address, Destination IP address, Protocol, Source Port,Destination Port and ICMP message type.

SFRs	Rationale
	Additionally, packets received on a TOE interface for which an IP ACL is applied will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to permit the traffic). Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. IP ACL policy names must be unique within the TOE device they are created for. IP ACL policy names are limited to 30 characters and contain no white space or special characters. A CM TOE Device can manage up to 50 IP ACLs and a total of 500 conditions per TOE device. When the IP ACL policy name is numeric, numbers 1 through 99 denote standard IP ACL policies and numbers 100 through 199 denote extended IP ACL policies. IP ACL policy names that begin with a number cannot contain nonnumeric characters.
FIA_ATD.1	In support of TOE administration, the TOE maintains several attributes associated with each of the TOE administrators. The attributes include: ▪ Authentication Credentials ▪ User ID ▪ User Role ▪ Domain The TOE uses the attributes to ensure secure management of the TOE.
FIA_SOS.1	The TOE enforces minimum complexity of administrative passwords configured on the TOE. Passwords must at minimum: ▪ Be at least 8 characters long ▪ Not contain all of the same characters (e.g., 99999999) ▪ Not contain all consecutive characters (e.g., 12345678)
FIA_UAU.2	The TOE allows for users to be authenticated by the remote AAA service or Windows server. It also requires users to be identified and authenticated prior to allowing any TSF mediated actions to be performed. The TOE ensures that each user must be successfully authenticated prior to accessing the TSF mediated functions of the TOE. Users with management access must successfully authenticate themselves using a unique user name and password combination prior to performing any actions on the TOE. If local authentication is used, the TOE maintains/stores the user name and password locally within the WAAS Appliance. There is no access to locally stored authentication credentials except through administrative interfaces protected by authentication. There is no unauthorized/unauthenticated interface available to access locally store authentication credentials. The TOE verifies the authenticated user's authorizations prior to allowing access to any locally stored authentication credentials.
FIA_UAU.5	The TOE allows for users to be authenticated by the remote AAA service or Windows server if configured by the administrator. The TOE provides the local authentication mechanism for each user based on the username and password combination. Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE.

SFRs	Rationale
	To support external authentication, the administrator must explicitly configure the TOE to support additional authentication methods. The TOE administrator can configure the types of authentication supported and order in which the authentication methods are applied.
FIA_UID.2	The TOE allows for users to be identified and authenticated prior to allowing any TSF mediated actions to be performed. It also ensures that each user must be successfully authenticated prior to accessing the TSF mediated functions of the TOE.
FMT_MOF.1	The TOE provides the authorized administrator the ability to manage how the TOE interacts with external AAA servers and remote management protocols. The TOE provides the authorized administrator the ability to determine which remote management protocols and AAA servers are available, the ability to enable/disable authentication provided by remote AAA servers, the ability to enable/disable remote management of protocols, the ability to modify the remote AAA servers used by the TOE, and the ability to modify the remote management protocols used by the TOE.
FMT_MSA.1(1)	The TOE implements role based access control based on user roles and provides the interface to manage the security attributes of the policy. The TOE ensures that only those users with privileged roles may access the security management functions of the TOE for role assignments and role definitions.
FMT_MSA.1(2)	The TOE uses the attribute settings for the security attributes set by the administrator for the Device Information Flow Policy to enforce the policy . The TOE ensures that only administrators are able to modify and create security attributes for IP ACLs.
FMT_MSA.3	The TOE uses the attribute settings for the security attributes set by the administrator for the Device Information Flow Policy to enforce the policy.
FMT_MTD.1(1)	The TOE ensures that only authorized administrators may query, and clear the audit trail. This is accomplished on the CM GUI through the following navigation: Admin > logs > Audit log.
FMT_MTD.1(2)	The TOE ensures that only authorized administrators may initialize and modify user security attributes (assigned roles/assigned domains), role definitions and IP ACLs. Roles are configured over the CM GUI through the following navigation: Admin > AAA > Roles. Domains are configured over the CM GUI through the following navigation: Admin > AAA > domains. IP ACLs are configured over the CM GUI through the following navigation: Configure>Network>TCP/IP Settings>IP ACL. IP ACLs are configured over the CM GUI using the following commands: - (config) ip access-list - (config-if) ip access-group - (config-std-nacl) delete - (config-std-nacl) deny - (config-std-nacl) exit - (config-std-nacl) list - (config-std-nacl) move - (config-std-nacl) permit - (config-ext-nacl) delete

SFRs	Rationale
	- (config-ext-nacl) deny - (config-ext-nacl) exit - (config-ext-nacl) list - (config-ext-nacl) permit - (config-ext-nacl) move - (config-ext-nacl) permit Note: Custom defined GUI administrators do not have the ability to manage role definitions and IP ACLs.
FMT_MTD.1(3)	The TOE ensures that only authorized administrators may initialize user authentication credentials. User Authentication Credentials are initialized over the CM GUI through the following navigation: Admin > AAA > Users. User Authentication Credentials are initialized over the CLI using the following command: - (config) username Note: Custom defined GUI administrators do not have the ability to initialize user authentication credentials. The TOE also ensures that only authorized administrators may modify configured passwords.
FMT_MTD.1(4)	The TOE ensures that only the authorized administrator has the ability to change default and modify the user inactivity threshold for established CLI or CM GUI web session. The inactivity threshold is configured over the CM GUI through the following navigation: Configure>System Properties. The inactivity threshold is configured over the CLI using the following command: - (config) exec-timeout Note: the CLI administrators cannot define the inactivity time period for GUI inactivity.
FMT_MTD.1(5)	The TOE ensures that only the authorized administrator has the ability to modify the TOE clock. The TOE clock is configured over the CM GUI through the following navigation: - Configure>Date/Time The TOE clock is configured over the CLI using the following command: - Clock - ntpdate
FMT_SMF.1	The TOE provides the functionality necessary to support the security management functions of the TOE. The TOE permits an authorized administrator to perform the following actions: • Determine the behavior of, disable, enable, modify the behavior of functions that control the security functions and configure the TOE • Read audit information • Query, modify, and create role assignments and role definitions • Query, modify, and create IP ACLs • Query, clear the audit trail • Initialize user authentication credentials and • Change default and modify inactivity threshold parameter

SFRs	Rationale
	- Modify clock.
FMT_SMR.1	The TOE implements role based access control based on user roles. It also ensures that only users with privileged roles may access the security management functions of the TSF configuration, and associate users with their roles. The TOE supports one predefined security relevant role for GUI administrators (admin). The “admin” role has the ability to do everything through using the GUI (it is a super user account). The TOE supports one predefined security relevant role for CLI administrators (Privileged CLI administrator). Privileged CLI administrators are able to access every administrative command and capability available through the WAAS CLI. This allows the administrator to configure (create, modify, delete) the security features of the TOE device. Additionally, the TOE supports the definition of custom roles for both GUI and CLI administrators. TOE administrators with the appropriate access have the ability to define roles that allow customer access to TOE GUI and CLI elements. When a user is assigned a custom role, that user is granted the access defined by the role. For the custom defined GUI administrator, read or write access can be defined for any of the sections and subsections of the GUI. These sections include the following: Devices - Allows the administrator to go to the Dashboard and Alerts displays for your entire WAAS network and allows the administrator to choose a specific device or device group for which to configure WAAS services and general settings. The administrator can also view detailed device information and messages, and manage locations. Monitor - Allows the administrator to see network traffic and other charts and reports to monitor the health and performance of your WAAS network. Report - Allows the administrator to manage and schedule reports for your WAAS network. Jobs - Allows the administrator to manage software update jobs. Configure - Allows the administrator to configure the main WAAS services (file, print, and application acceleration) and other settings. Admin - Allows the administrator to manage user accounts, passwords, licenses, and virtual blades, and view the system log. For the CLI administrator, an IT environment TACACS+ server is used to define per command access to the CLI administrative interface. The user rights can be defined for any command supported by TOE. Regardless of the command the authorization procedure is the same. The TOE receives a request for a specific command by an administrator. The TOE then forwards the command to the TACACS+ server. The server then returns a specific allow or deny response. The TOE only allows the command to execute if a specific allow response is received by from the TACACS+ server.

SFRs	Rationale
FPT_ITT.1	The TOE provides protected communication between devices in the WAAS solution. This protected communication includes management traffic related to the association of Data Center, Branch and CM TOE components to form the WAAS solution. These communications are protected using TLSv1. When a TOE device is activated, a unique hash tag is associated with the device and exchanged with the device. This tag is used by the device to identify itself in all future communication with the CM. The TOE ensures that administrative interface and capabilities exist to allow an authorized user to associate TOE component devices to be part of the TOE Solution. Additionally, the TOE provides protected communication between its components using TLSv1 protocol. Management traffic between Central Managers and WAE devices is not subject to modification or disclosure. This includes TOE configuration information and network settings and updates.
FPT_STM.1	The TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. Optionally, the TOE time source may be synchronized with an external NTP server
FTA_SSL.3	The TOE enforces the shell and terminal session timeout values (default of 15 minutes for CLI and 10 minutes for CM GUI) so that when the time period of inactivity has elapsed the user terminal session or Web session is terminated. The TOE provides the administrator with the ability to configure the user inactivity threshold for session termination.
FTA_TSE.1	The TOE has the ability to deny connections based on configured IP ACL deny policy. If traffic received by the TOE matches an administratively configured IP ACL deny policy, the traffic is denied.
FTP_ITC.1	The TOE provides a trusted channel by which the TOE receives optional external authentication services such as RADIUS, TACACS+ and Windows Authentication. The optional RADIUS, TACACS+, and Window Server authentication services are supported by the TOE through an authentication client module which resides on the TOE devices. Through this client, security management can be centralized including the specification of the RADIUS, TACACS+, and Windows authentication server to include pre-shared key, server time-out interval, and the display of server details. When the RADIUS and TACACS+ services are used AAA event messages generated by the client are also recorded in the TOE audit log.
FTP_TRP.1	The TOE provides a protected channel by which an SSL/TLS or SSH host may initiate communication and manage the TOE.

6.1 TOE Bypass and interference/logical tampering Protection Measures

The TOE is a solution that is made up of any combination of hardware appliances and pluggable modules, as defined in the TOE Description, which are referred to as TOE devices. The TOE devices are hardware products containing software in which all operations in the TOE scope are protected from interference and tampering by untrusted subjects, with all administration and configuration operations performed within the physical boundary of the TOE. The TOE has been designed so that all locally maintained user data and WAAS solution data can only be manipulated via the CLI or the Web interfaces. This design, combined with the fact that only a user with a defined role on the TOE may access the TOE security functions, provides a distinct protected domain for the TSF.

Users operating in a role that includes access to the service involved with configuring TOE devices (i.e., the user has access to the Device tab of the WAAS Central Management GUI) can configure the CLI session timeout value for inactivity on a CLI session. When the time limit is exceeded for inactivity the TOE exits and closes the CLI session. The default is 15 minutes.

Users operating in a role that includes access to the services involved with configuring TOE system configurations (i.e., the user has access to the System tab of the WAAS Central Management GUI) can configure the WAAS Central Management GUI inactivity time out for users using this GUI. When the time limit is exceeded for inactivity the TOE exits and closes the GUI session. The default is 10 minutes.

The TOE provides protected communication between the CM and application accelerator WAE devices using TLSv1. SSL/TLS protects the management communication between these TOE components. This includes TOE configuration information, network settings and updates.

The TOE uses HTTPS for the Web GUIs available on the TOE devices. Using HTTPS protects the confidentiality and integrity of the TOE management that is carried out over this interface. An administrator enters the IP address of the TOE device and the port that the TOE listens on for HTTPS communications. After the web browser has established a communication channel with the TOE the administrator accepts the self signed certificate from the TOE device that is used to encrypt the session. The acceptance of the certificate must be done or else the TOE device will not provide the logon screen. Accepting the certificate also helps protect the initial identification and authentication that is done by an administrator. Once an administrator has accepted the certificate and inputted their I&A credentials the TOE establishes an HTTPS session that is used for the duration of the administrator session. All traffic flowing from the Web browser being used by the administrator and the TOE device is protected from disclosure and modification.

The Appliance (WAE/WAVE) and module (NME-WAE) TOE devices maintain real time using an internal hardware clock. The TOE solution can optionally be configured to interface with a Network Time Protocol (NTP) server to retrieve a time value.

All modules needing to securely protect sensitive data stored on the TOE will utilize the functions of another module called the Secure Store. Secure Store module is required for this evaluation to enforce strong encryption and decryption algorithms.

All Key Encryption Keys required by Central Manager and application accelerator TOE are retrieved and managed by Key Manager Module on the Central Manager. Key Manager provides keys derived based on Secure Random algorithm. Further, keys stored in Key Manager's repository are securely stored using the encryption functions provided by the Secure Store.

Secure Store when enabled on Central Manager TOE, provides user-inputted passphrase based AES 256 bit algorithm, to encrypt and decrypt sensitive data stored on the Central Manager.
Secure Store when enabled on the application accelerator TOE, uses Central Manager's Key Manager provided Secure Random Key Encryption Key to encrypt and decrypt sensitive data stored on the WAE. The Central Manager and application accelerator devices use Secure Store

for encrypting passwords and encryption keys on the TOE.

Additionally, application acceleration TOE provides encrypted storage for protection of the DRE generated “byte-cache” and CIFS file cache. The disk encryption feature includes two aspects: the actual data encryption on the application accelerator TOE’s disk and the encryption key storage and management. When you enable disk encryption, all user data in application accelerator TOE persistent storage will be encrypted. The encryption key for unlocking the encrypted data is stored in the Key Manager repository on Central Manager. When you reboot an application accelerator TOE after configuring disk encryption, the WAE retrieves the key from the Key Manager automatically, allowing normal access to the data that is stored in encrypted persistent storage.

Appendix A: Glossary

Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Security Target:

AAA	Authentication, Authorization, Accounting
ACL	Access control List
AO	Application Optimizer
CC	Common Criteria
CLI	Command Line Interface
CM	Central Manager
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IP	Internet Protocol
IPFC	IP over Fibre Channel
IT	Information Technology
KEK	Key Encryption Key
NM	Network Module. Same as NME-WAE
NME-WAE	WAE Network Module
NTP	Network Time Protocol
PP	Protection Profile
RADIUS	Remote Access Dial-In User Service
SF	Security Function
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SOF	Strength of Function
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WAAS	Wide Area Application Services
WAE	Wide Area Application Engine
WAVE	Wide Area Virtualization Engine
WCCP	WEB Cache Communication Protocol

Acronyms and Abbreviations

The following terms are used in this Security Target:

Application Accelerator Device — The server-side application accelerator device is placed between the servers at the data center and the WAN connecting the data center to branch offices. The client-side application-accelerator device serves client requests at branch offices or forwards requests to the data center application accelerator device.

SSH — Secure Shell is a network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote.

SSL — Protocol used for encrypting and security messages transmitted over the Internet. Predecessor of TLS.

TLS — Protocol used for encrypting and security messages transmitted over the Internet

Telnet	Protocol used for encrypting and security messages transmitted over the Internet
WCCPv2	The WCCP V2.0 protocol specifies interactions between one or more routers and one or more web-caches. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a group of routers. (http://www.wrec.org/Drafts/draft-wilson-wrec-wccp-v2-00.txt)

References

The following documentation was used to prepare this ST:

[CC_PART 1]	Common Criteria for Information Technology Security Evaluation – Part1: introduction and general model; dated August 2005, version 2.3, Revision 1, CCMB-22006-09-001
[CC_PART 2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated August 2005, version 2.3, Revision 2, CCMB-2007-09-002
[CC_PART 3]	Common Criteria for Information Technology Security Evaluation – part3: Security assurance components, dated August 2005, version 2.3, Revision 2, CCMB-2007-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated August 2005, version 2.3, Revision 2, CCMB-2007-09-004
Cisco WAAS solution text	Cisco WAAS Brochure: C45-41226-01; C02-419740-00