SECODE
An NTT Communications Group Company

SECURITY TARGET

FOR

A10 NETWORKS THUNDER 5430S AND 6430S APPLICATIONS DELIVERY CONTROLLERS

EAL2
AUGMENTED WITH
ALC_FLR.1

Version: 1.2

November 20, 2013

DENMARK • FINLAND • NORWAY • SWEDEN • THE NETHERLANDS
www.secode.no • info@secode.com • Secode Norge AS, Postboks 721 Stoa, N-4808 Arendal, Norway • Tel +47 37 05 81 00

TABLE OF CONTENTS

ABBREVIATIONS

Abbreviation	Description
ACL	Access Control List
ACOS	Advanced Core Operating System
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command-line interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
DES	Data Encryption Standard
DNS	Domain Name System
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
IP	Internet Protocol
IT	Information Technology
NAT	Network Address Translation
OS	Operating System
PUBS	Publications
RSA	Rivest, Shamir and Adleman
SF	Security Function
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SLB	Server Load Balancing
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
VE	Virtual Ethernet
VIP	Virtual IP

1. ST INTRODUCTION (ASE_INT)

1.1. ST AND TOE REFERENCES

ST title: Security Target for A10 Networks Thunder 5430S and 6430S Application Delivery Controllers, Version 1.2

CC Version: 3.1 Revision 4

Assurance level: EAL2 augmented with ALC_FLR.1

PP Identification: None

TOE name: Thunder 5430S and 6430S Application Delivery Controllers

TOE version:
- Hardware versions: 5430S and 6430S
- Firmware version: 2.7.1-P2

1.2. TOE OVERVIEW

A10 Networks' Thunder is an application delivery controller designed to help enterprises and ISPs with application availability through a Web Application Delivery Platform. The Thunder Advanced Core Operating System (ACOS) architecture includes a multi-CPU architecture built from the ground up, for load balancing performance, scalability and reliability. The relevant Thunder application delivery controllers include the platform models 5430S and 6430S. These application delivery controllers are integrated 64-bit models, with both 64-bit ACOS and 64-bit hardware.

No non-TOE hardware/software/firmware is required by the TOE for operation.

1.3. TOE DESCRIPTION

The TOE is a hardware device. The hardware and firmware components of the TOE are enclosed in a metal enclosure which is the physical boundary of the TOE. The removable panels of the enclosure are protected by tamper-evident labels. The enclosure is opaque within the visible spectrum.

1.3.1. THUNDER APPLICATION DELIVERY CONTROLLERS FEATURES

The Thunder Application Delivery Controller is designed to meet the growing demands of Web sites, carriers and enterprises. The Thunder offers intelligent Layer 4-7 application processing capabilities with performance and scalability to meet critical business requirements. The Thunder's standard redundant components design can ensure organizations non-stop service availability for all types of applications.

High Availability feature is outside of the scope of the evaluation.

Key features of the Thunder are described in the following.

1. Application Delivery Features
   - Comprehensive IPv4/IPv6 Support
     - Transparent (Layer 2) and gateway (Layer 3) mode support for easy deployment into existing infrastructures

    - Network Address Translation (NAT) – IPv4-IPv4, IPv4-IPv6, IPv6-IPv4, IPv6-IPv6, ALG support for PPTP, Large-Scale NAT (LSN)
    - OSPFv2 for IPv4, OSPFv3 for IPv6
    - IS-IS and BGP for IPv4 and IPv6
    - IPv4/IPv6 static routes
    - DHCP relay
  - Advanced Layer 4/Layer 7 Server Load Balancing
    - Fast TCP, fast UDP, fast HTTP, and full HTTP Proxy
    - Comprehensive protocol support: HTTP, HTTPS, FTP, TCP, UDP, SSL, SIP, SMTP, and others
    - Comprehensive load-balancing methods – weight-based, connection-based, and response-based methods, as well as simple round robin
  - Protocol translation – support for mixed IPv4/IPv6 environments
  - Advanced health monitoring
  - Customizable configuration templates
  - RAM caching of web content
  - Firewall Load Balancing (FWLB)
  - Global Server Load Balancing (GSLB)
  - Transparent Cache Switching (TCS)

2. Acceleration and Security
   - SSL acceleration and offload
   - Traffic security
   - Management access security – Local admin database and support for optional remote RADIUS or TACACS+ AAA
   - Spam filter support (Policy-Based SLB) – High-speed application of very large black/white lists that filter based on source or destination IP host or subnet address
   - DoS attack detection and prevention
   - Access Control Lists (ACLs)

3. DNS Application Firewall – Solution consisting of the following:
   - Traffic validation – Drop or redirect malformed DNS queries
   - Dynamic traffic flow regulation:
     - High performance surge protection (connection and rate limiting)
     - Source-IP based connection rate limiting
     - Policy-Based SLB (black/white lists)

4. System Management
   - Dedicated management interface
   - Multiple access methods – SSH, HTTPS
   - Web-based Graphical User Interface (GUI) with language localization
   - Industry-standard Command Line Interface (CLI) support
   - On-demand backup of configuration files, logs, and system files
   - SNMP, syslog, alerting
   - Thunder Virtual Chassis System (aVCS), for managing multiple Thunder devices as a single device
   - Virtualized Management, provided by Role-Based Administration (RBA)

5. Troubleshooting tools
   - Port mirroring
   - Debug subsystem for packet capture

1.3.2. ACOS ARCHITECTURE

Thunder devices use embedded Advanced Core Operating System (ACOS) architecture. ACOS is built on top of a set of Symmetric Multi-Processing CPUs and uses shared memory architecture to maximize application data delivery.

ACOS is designed to handle high-volume application data with integrated Layer 2 / Layer 3 processing and integrated SSL acceleration built into the system.

ACOS inspects packets at Layers 2, 3, 4, and 7 and uses hardware-assisted forwarding. Packets are processed and forwarded based on ACOS configuration.

The Thunder device can be deployed into the network in transparent mode or gateway (route) mode.

- Transparent mode – The Thunder device has a single IP interface. For multinetted environments, the multiple Virtual LANs (VLANs) can be configured.
- Route mode – Each Thunder interface is in a separate IP subnet. Open Shortest Path First (OSPF) is supported.

In either type of deployment, ACOS performs Layer 4-7 switching based on the SLB configuration settings.

1.3.3. SECURE CLIENT-SERVER TRAFFIC

Commonly, clients and servers use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to secure traffic. Hardware acceleration is used for TLS encryption of data. For example, a client that is using a shopping application on a server will encrypt data before sending it to the server. The server will decrypt the client's data, and then send an encrypted reply to the client. The client will decrypt the server reply, and so on. (The Thunder device supports TLS version 1.0. For simplicity in this Security Target, the term "SSL" means both SSL version 3.1 and TLS version 1.0.)

SSL works using certificates and keys. Typically, a client will begin a secure session by sending an HTTPS request to a virtual IP (VIP) address. The request begins an SSL handshake. The Thunder device will respond with a digital certificate. From the client's perspective, this certificate comes from the server. Once the SSL handshake is complete, the client begins an encrypted client-server session with the Thunder device.

Figure 1 shows a simplified example of an SSL handshake. In this example, the A Thunder device is acting as an SSL proxy for backend servers.

These documents are included on the documentation CD shipped with the Thunder system, and also are available on the A10 Networks support site:

- Thunder Installation Guide
- Thunder Configuration Guide
- Thunder GUI Reference guide
- Thunder CLI Reference Guide
- Thunder aFleX Reference Guide
- Thunder MIB Reference
- Thunder aXAPI Reference

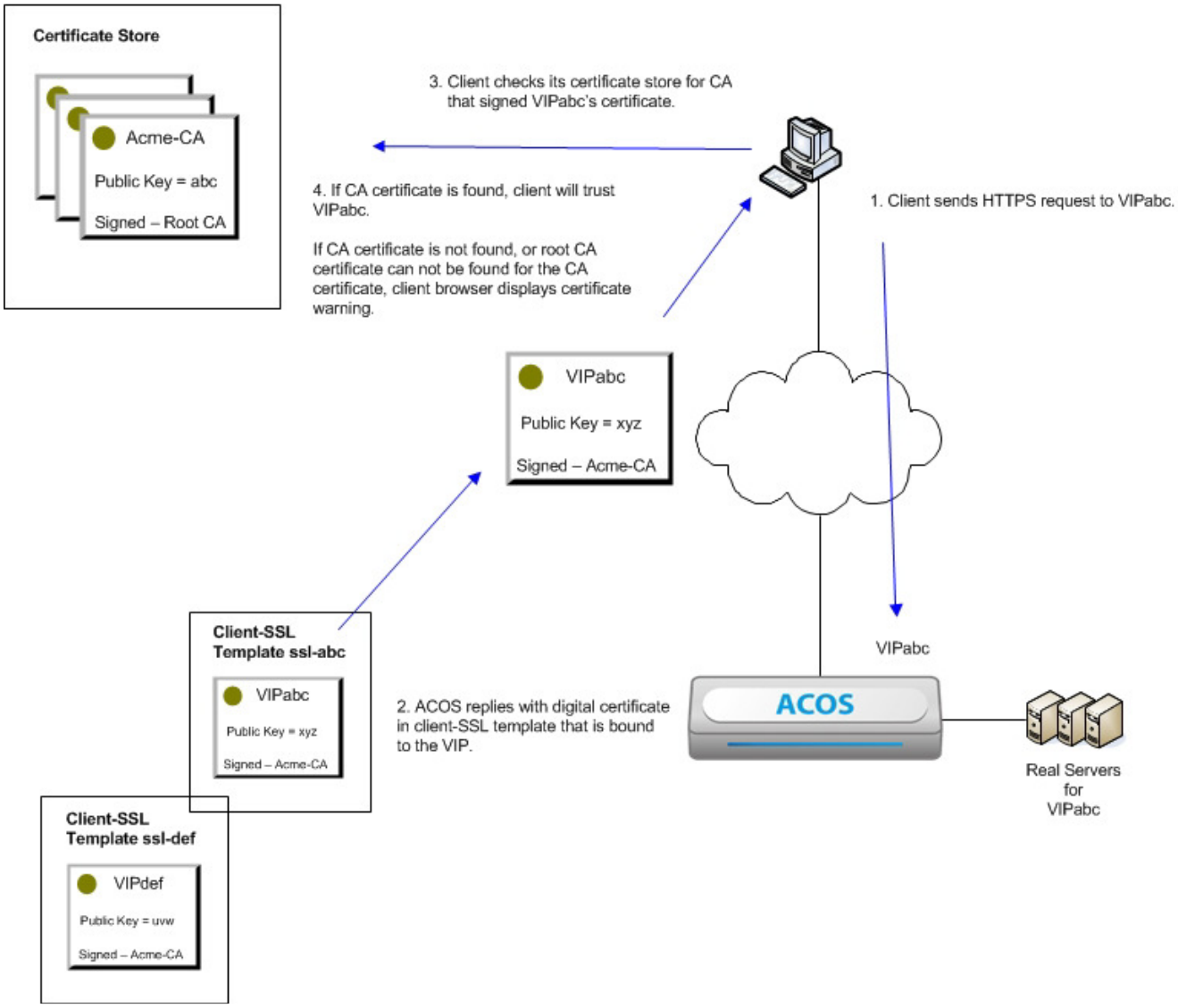

Figure 1; Typical SSL Handshake (simplified)

1.3.4. FIREWALL PROTECTION

The ACL pages on the Thunder Application Delivery Controllers can be used to configure and apply Access Control Lists (ACLs). ACLs can be used for the following tasks:
• Permit or block through traffic.

Table 1 lists the relevant ACL parameters.

Parameter	Description and Syntax
Action	Specifies the action to perform on traffic that matches the ACL: • Deny – Drops the traffic. • Permit – Allows the traffic.
Source Address	Specifies the source address on which to match.
Source Port	Specifies the source protocol port(s) on which to match.
Destination Address	Specifies the destination address on which to match.
Destination Port	Specifies the destination protocol port(s) on which to match.

Table 1; ACL parameters

The ACLs can be used to permit or deny packets based on address and protocol information in the packets. Thunder devices support the following types of ACLs:

- Standard IPv4 ACL – Standard IPv4 ACLs filter based on source IPv4 address.
- Extended IPv4 ACL – Extended IPv4 ACLs filter based on source and destination IPv4 addresses, IP protocol, and TCP/UDP port numbers.
- Extended IPv6 ACL – Extended IPv6 ACLs filter based on source and destination IPv6 addresses, IP protocol, and TCP/UDP port numbers.

Configuring of Standard IPv4 ACL, Extended IPv4 ACL and Extended IPv6 ACL can be done by means of a methods using GUI or CLI.

The ACLs can be used for the following tasks:

- Permit or block through traffic.
- Permit or block management access.
- Specify the internal host or subnet addresses to which to provide Network Address Translation (NAT).

An ACL can contain multiple rules. Each rule contains a single permit or denies statement. Rules are added to the ACL in the order they are configured. The first rule added appears at the top of the ACL.

Rules are applied to the traffic in the order they appear in the ACL (from the top, which is the first rule, downward). The first rule that matches traffic is used to permit or deny that traffic. After the first rule match, no additional rules are compared against the traffic.

Access lists do not take effect until they are applied.

- To permit or block through traffic on an interface, apply the ACL to the interface, using the GUI or the CLI.
- To permit or block through traffic on a virtual server port, apply the ACL to the virtual port. An ACL applied to a virtual server port permits or denies traffic just as an ACL applied to a physical port or Virtual Ethernet (VE) interface does. This can be done using the GUI or the CLI.
- To permit or block management access, use the ACL with the enable-management command. By default, certain types of management access through the Thunder device's Ethernet interfaces are blocked. The management access can be enabled or disabled, for individual access types and interfaces. An ACL can also be used to permit or deny management access through the interface by specific hosts or subnets. This can be done using the GUI or the CLI.
- To specify the internal host or subnet addresses to which to provide NAT, use the ACL when configuring the pool. The Thunder device uses NAT to perform SLB. The Thunder device also supports traditional Layer 3 NAT, which can be configured if required by the network.

A transparent session is a non-SLB Layer 2 or Layer 3 session that the Thunder device sets up for traffic that is transiting through the Thunder device, but is not initiated or terminated on the device.

To configure session filtering for transparent IPv6 sessions on an interface:

1. Configure an IPv6 ACL that uses the log transparent-session-only option.
2. Apply the ACL to the interface that receives incoming traffic for the sessions.

1.3.5. SERVER LOAD BALANCING

Server Load Balancing (SLB) is a suite of resource management features with the intention to make server farms more reliable and efficient. The TOE supports SSH and HTTPS management interfaces.

Server farms can easily be grown in response to changing traffic flow, while protecting the servers behind a common virtual IP address. From the perspective of a client who accesses services, requests go to and arrive from a single IP address. The client is unaware that the server is in fact multiple servers managed by a Thunder device.

There is no need to wait for DNS entries to propagate for new servers. A new server can be added to the Thunder configuration for the virtual server, and the new real server should then become accessible immediately.

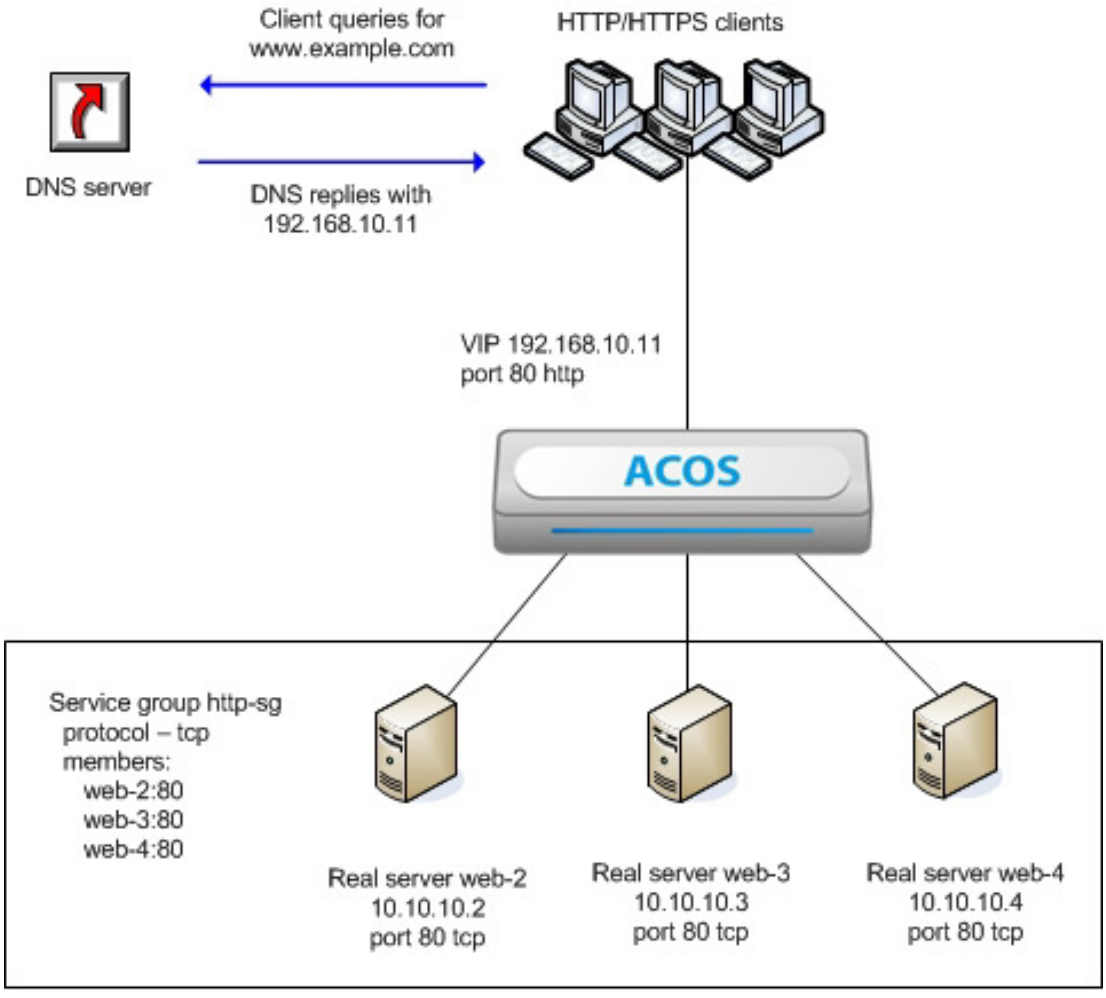

Figure 2; SLB Example

The services managed by the Thunder device are controlled by service groups. A service group is a set of real servers. The Thunder device selects a real server for a client's request based on a set of tuneable criteria including server health, server response time,

and server load. These criteria can be tuned for individual servers and even individual service ports.

TOE administrators are identified to the TOE by usernames. The TOE uses password-based authentication for administrator authentication.

The following load balancing algorithms are supported by the TOE:

- Round Robin
- Active Server, based on number of active servers
- Weighted Preference, based on administrative weights
- Connection Load, based on number of connections that are on the servers.

1.4. NOTATIONS AND FORMATTING

The notations and formatting used in this ST are consistent with version 3.1 Revision 4 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text in square brackets, [*Selection value*].

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value with bold face in square brackets, [Assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threat agents are given names beginning with "TA." – e.g., TA.User. Threats to the TOE are given names beginning with "TT." – e.g., TT.Filter_Fails. TOE security environment threats are given names beginning with "TE."-- e.g., TE.Crypto_Fails.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter-msg and OE.Clearance.

2. CC CONFORMANCE CLAIM (ASE_CCL)

This TOE and ST are conformant with the following specifications:
CC Part 2: Security functional components, September 2012, Version 3.1, Revision 4, extended.
CC Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, conformant, EAL2 augmented with ALC_FLR.1.

There are no Protection Profile claims.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1. THREATS TO SECURITY

3.1.1. ASSETS

AS.Servers_Inside: The servers behind the SLB need protection, together with the information passed through the TOE and stored on the servers.

3.1.2. THREAT AGENTS

TA.Admin: The administrator may unintentionally perform actions jeopardizing the security of the TOE.

TA.Client: Clients may unintentionally perform unauthorized actions.

TA.Hacker: Personnel with no authorized access to the TOE environment. These threat agents may try to access information and may have "unlimited" resources supporting them.

TA.SLB_Failure: The SLB may fail due to configuration/system errors.

3.1.3. IDENTIFICATION OF THREATS

3.1.3.1. THREATS TO THE TOE

TT.Masquerade: A hacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

TT.Tampering: A hacker may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.

TT.Access_TOE: A user may gain unauthorized access to security data on the TOE due to SLB failure.

TT.Access_Int: A user may gain unauthorized access to server resources on protected/internal network.

TT.Mod_Conf: A hacker may modify the TOE configuration to gain unauthorized access to server resources on protected/internal network.

3.2. ORGANIZATIONAL SECURITY POLICIES

P.Cryptography: The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

P.Cryptography_Validated: Only FIPS 140-1/2 compliant cryptography (methods and implementations) are acceptable for key management (i.e., generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

P.Manage: The TOE shall only be managed by authorized users.

P.Access: All data collected and produced by the TOE shall only be used for authorized purposes.

P.Integrity: Data collected and produced by the TOE shall be protected from modification.

3.3. ASSUMPTIONS

A.Install: The TOE has been installed and configured according to the appropriate installation guides, and all traffic between clients and servers flows through it.

A.Manage: There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it contains.

A.No_Evil: The administrators of the TOE are non-hostile, appropriately trained, and follow all guidance.

A.Locate: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1. TOE SECURITY OBJECTIVES

O.Load_Balancing: The TOE must provide encrypted SSL connections for load balanced servers with basic firewall protection.

O.Cryptography: The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted outside the TOE.

O.Cryptography_Validated: The TOE will use CMVP FIPS 140-1/2 compliant crypto modules for cryptographic services implementing CMVP -approved security functions and random number generation services used by cryptographic functions.

O.Protect: The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data, and preserve correct operations during specified failure events.

O.Admin: The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators, may exercise such control.

O.Authenticate: The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.

O.Audit: The TOE must record the actions taken by administrators, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.

O.Time: The TOE must provide reliable timestamps for its own use.

O.Access_Int: The TOE must allow access to server resources on protected/internal network only as defined by the Information Flow Control SFP.

O.Integrity: The TOE must ensure the integrity of all audit and system data.

4.2. OPERATIONAL ENVIRONMENT SECURITY OBJECTIVES

OE.External: The TOE environment must ensure any authentication data in the environment are protected and maintained.

OE.Manage: Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.

OE.Connect: The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.

OE.Power: The TOE environment must provide the electricity necessary to the TOE to function. The power to the TOE must be reliable and protected from surges and disconnects.

OE.AC: The TOE environment must regulate the temperature of the facility where the TOE is located so no damage is caused by heat or cold.

OE.Physical: The physical environment must be suitable for supporting a computing device in a secure setting.

OE.Install: Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.

4.3. SECURITY OBJECTIVES RATIONALE

The table below shows that all threats, assumptions, and security policies of the TOE are met by one or more TOE or environment security objective. In the next sections a rationale is given for each of these tracings.

Threats, Policies, Assumptions / Objectives	TT.Masquerade	TT.Tampering	TT.Access_TOE	TT.Access_Int	TT.Mod_Conf	P.Cryptography	P.Cryptography_Validated	P.Manage	P.Access	P.Integrity	A.Install	A.Manage	A.No_Evil	A.Locate
O.Load_Balancing					X					X				
O.Cryptography						X	X							
O.Cryptography_Validated							X							
O.Protect		X			X			X	X					
O.Admin			X					X						
O.Authenticate	X		X		X			X	X					
O.Audit	X		X		X									
O.Time			X	X										
O.Access_Int				X				X	X					
O.Integrity										X				
OE.External			X		X									X
OE.Manage			X	X	X						X	X	X	
OE.Connect		X												X
OE.Power		X												X
OE.AC		X												X
OE.Physical		X												X
OE.Install			X	X				X			X	X	X	
OE.Person								X						

Table 2; Tracing of objectives to threats, policies, and assumptions

4.4. THREATS

4.4.1. TT.MASQUERADE

The threat **TT.Masquerade** is met by the objectives **O.Authenticate** and **O.Audit**. The **O.Authenticate** objective ensures that Administrators supply login credentials before being granted management access to the TOE. The **O.Audit** objective ensures that events of security relevance are audited.

4.4.2. TT.TAMPERING

The threat **TT.Tampering** is met by the objectives **O.Protect**, **OE.Connect**, **OE.Power**, **OE.AC** and **OE.Physical**. **O.Protect** ensures that the protection mechanisms of the TOE designed to prevent tampering with TOE IT assets are in place and functioning properly, and that these mechanisms cannot be bypassed. **OE.Connect** ensures that the TOE has a reliable network connection. **OE.Power** ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to the TOE. **OE.AC** ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature. **OE.Physical** ensures that the environment will protect the TOE from physical tampering.

4.4.3. TT.ACCESS_TOE

The threat **TT.Access_TOE** is met by the objectives **O.Admin, O.Authenticate, O.Audit, O.Time, OE.External, OE.Manage** and **OE.Install**. **O.Admin** ensures that only Administrators can access the management functions for the TOE. **O.Authenticate** ensures that Administrators identify and authenticate themselves before they are given access. **O.Audit** ensures that events of security relevance are audited. **O.Time** ensures that the TOE has the correct time when recording audit records. **OE.External** ensures that authentication data is stored securely outside of the TOE. **OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the TOE and who will periodically check the accuracy of the TOE's timestamps. **OE.Install** ensures that the TOE will be installed correctly and configured securely.

4.4.4. TT.ACCESS_INT

The threat **TT.Access_Int** is met by the objectives **O.Time**, **O.Access_Int**, **OE.Manage** and **OE.Install**. **O.Time** ensures that the TOE maintains the correct time to be used when the date and time are determining factors for access. **O.Access_Int** ensures that the TOE limits access to internal network resources to the authorized users. **OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the TOE and who will periodically check the accuracy of the TOE's timestamps. **OE.Install** ensures that the TOE will be installed correctly and configured securely. All traffic between the internal and external networks will flow through the TOE.

4.4.5. TT.MOD_CONF

The threat **TT.Mod_Conf** is met by the objectives **O.Load_Balancing**, **O.Protect**, **O.Authenticate**, **O.Audit**, **OE.External** and **OE.Manage. O.Load_Balancing** ensures that the TOE has basic firewall protection**. O.Protect** ensures that the TOE protects configuration data from unauthorized modifications. **O.Authenticate** ensures that Administrators identify and authenticate themselves before they are given access to configuration data. **O.Audit** ensures that events of security relevance are audited. **OE.External** ensures that that authentication data is stored securely outside of the TOE. **OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data.

4.5. POLICIES

4.5.1. P.CRYPTOGRAPHY

The policy **P.Cryptography** is met by the objective **O.Cryptography** which will require the TOE to implement cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit outside the TOE.

4.5.2. P.CRYPTOGRAPHY_VALIDATED

The policy **P.Cryptography_Validated** is met by the objectives **O.Cryptography** and **O.Cryptography_Validated. O.Cryptography** satisfies this policy by requiring the TOE to implement cryptographic services. These services will provide confidentiality and integrity protection of the data while in transit outside the TOE. **O.Cryptography_Validated** satisfies this policy by requiring that all crypto modules for cryptographic services be CMVP FIPS 140-1/2 compliant. This will provide assurance that the CMVP approved security functions and random number generation will be in accordance with CMVP and comply with the FIPS 140-1/2.

4.5.3. P.MANAGE

The policy **P.Manage** is met by the objectives **O.Protect**, **O.Admin**, **O.Authenticate**, **O.Access_Int**, **OE.Install** and **OE.Person**. The **O.Admin** objective ensures there is a set of functions for administrators to use. The **OE.Install** objective supports the **OE.Person** objective by ensuring administrator follow all provided documentation and maintain the security policy. The **O.Authenticate** objective provides for authentication of users prior to any TOE function accesses. The **O.Protect** objective provides for TOE self-protection. The **O.Access_Int** ensures that the TOE limits access to internal network resources to the authorized users.

4.5.4. P.ACCESS

The policy **P.Access** is met by the objectives **O.Protect**, **O.Authenticate** and **O.Access_Int**. The **O.Authenticate** objective provides for authentication of users prior to any TOE function accesses. The **O.Protect** objective provides for TOE self-protection. The **O.Access_Int** ensures that the TOE limits access to internal network resources to the authorized users.

4.5.5. P.INTEGRITY

The policy **P.Integrity** is met by the objectives **O.Load_Balancing** and **O.Integrity**. **O.Load_Balancing** provides encrypted SSL connections for load balanced servers. **O.Integrity** ensures the protection of data from modification.

4.6. ASSUMPTIONS

4.6.1. A.INSTALL

The assumption **A.Install** is met by the objectives **OE.Manage** and **OE.Install. OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data. **OE.Install** ensures that the TOE will be installed correctly and configured securely. All traffic between the internal and external networks will flow through the TOE.

4.6.2. A.MANAGE

The assumption **A.Manage** is met by the objectives **OE.Manage** and **OE.Install. OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data and who will periodically check the accuracy of the TOE's timestamps. **OE.Install** ensures that the TOE will be installed correctly and configured securely.

4.6.3. A.NO_EVIL

The assumption **A.No_Evil** is met by the objectives **OE.Manage** and **OE.Install. OE.Manage** ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data and who will periodically check the accuracy of the TOE's timestamps. **OE.Install** ensures that the TOE will be installed correctly and configured securely.

4.6.4. A.LOCATE

The assumption **A.Locate** is met by the objectives **OE.External**, **OE.Connect**, **OE.Power**, **OE.AC** and **OE.Physical**. **OE.External** ensures that that authentication data is stored securely outside of the TOE. **OE.Connect** ensures that the TOE has a reliable network connection. **OE.Power** ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to the TOE. **OE.AC** ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature. **OE.Physical** ensures that the TOE's environment is suitable for securely supporting the TOE.

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

The following explicit components have been included in this Security Target because the Common Criteria components were found to be insufficient as stated.

5.1. EXPLICIT FUNCTIONAL COMPONENTS

Explicit Component	Identifier	Rationale
FLB_SCO_EXP.1	Secure communication	This explicit component is necessary since it describes the core functionality, consisting of client/TOE/server communication, firewall protection and load balancing.
FCS_BCM_EXP.1	Baseline cryptographic module	This explicit component is necessary since it provides for the specification of the required FIPS compliance based on the implementation baseline.
FCS_COP_EXP.1	Random number generation	This explicit component is necessary since the CC cryptographic operation components are focused on specific algorithm types and operations requiring specific key sizes.
FCS_COP_EXP.2	Cryptographic Operation	This explicit component is necessary because it describes requirements for a FIPS 140-1 or 140-2 compliant crypto module rather than the entire TSF.
FIA_UAU_EXP.1	Timing of authentication – User	This explicit requirement is necessary to clearly specify the user authentication mechanism.

Table 3; Rationale for Explicit Functional Components

6. SECURITY REQUIREMENTS (ASE_REQ)

6.1. SECURITY FUNCTIONAL REQUIREMENTS (SFRS)

Functional Class	Functional Components
FLB	FLB_SCO_EXP.1
FAU	FAU_GEN.1, FAU_GEN.2, FAU.SAR.1, FAU.SAR.3, FAU.STG.1, FAU.STG.4
FCS	FCS_BCM_EXP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2
FDP	FDP_ACC.1a, FDP_ACC.1b, FDP_ACF.1a, FDP_ACF.1b, FDP_IFC.1, FDP_IFF.1
FIA	FIA_ATD.1.1, FIA_UAU.1a, FIA_UAU_EXP.1, FIA_UAU.5, FIA_UID.1
FMT	FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3a, FMT_MSA.3b, FMT_MSA.3c, FMT_SMF.1, FMT_SMR.1
FPT	FPT_FLS.1, FPT_ITC.1, FPT_ITT.1, FPT_STM.1

Table 4; **Functional requirements for the TOE**

6.1.1. LOAD BALANCING REQUIREMENTS (FLB)

6.1.1.1. FLB_SCO_EXP.1 SECURE COMMUNICATION

Dependences: None.

FLB_SCO_EXP.1.1 The TSF provides SSL proxy services between clients located on unprotected network and servers located on protected network, where the connection between the TOE and the client is SSL encrypted, and the connection between the TOE and the server may be encrypted or plaintext. Once the SSL handshake between the client and the TOE is complete, the client begins an encrypted session with the TOE. If encryption is used between the TOE and the server, once the SSL handshake between the TOE and the server is complete, the TOE begins an encrypted session with the server.

FLB_SCO_EXP.1.2 The TSF shall provide firewall protection by means of Access Control Lists (ACLs), used to permit or block through traffic.

FLB_SCO_EXP.1.3 The TSF shall provide Server Load Balancing (SLB) on network servers when a client opens a connection from outside. The following load balancing algorithms are supported by the TOE: Round Robin, Active Server, Weighted Preference, Connection Load.

6.1.2. SECURITY AUDIT (FAU)

6.1.2.1. FAU_GEN.1 AUDIT DATA GENERATION

Dependences: FPT_STM.1 Reliable time stamps

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) [**Login and logoff, network packet processing logging, system upgrade, system restart, CPU usage, alarms**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**None**].

6.1.2.2. FAU_GEN.2 User identity association

Dependences: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2.3. FAU_SAR.1 Audit review

Dependences: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**the authorized user**] with the capability to read [**all information]** 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.

6.1.2.4. FAU_SAR.3 Selectable audit review

Dependences: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**read only support through the CLI**] of audit data based on [**user name, IP address, login module, date/time**].

6.1.2.5. FAU_STG.1 Protected audit trail storage

Dependences: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

6.1.2.6. FAU_STG.4 Prevention of audit data loss

Dependences: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [*overwrite the oldest stored audit records*] and [**no other actions**] if the audit trail is full.

6.1.3. CRYPTOGRAPHIC SUPPORT (FCS)

6.1.3.1. FCS_BCM_EXP.1 BASELINE CRYPTOGRAPHIC MODULE

Dependences: None.

FCS_BCM_EXP.1.1 All cryptographic modules shall comply with FIPS 140-1/2 when performing FIPS approved cryptographic functions in FIPS approved cryptographic modes of operation.

FCS_BCM_EXP.1.2 The cryptographic module implemented shall comply with a minimum overall rating of Level 1.

FCS_BCM_EXP.1.3 The FIPS validation testing of the TOE cryptographic module(s) shall be in conformance with FIPS 140-1, 140-2, or the most recently approved FIPS 140 standard for which CMVP is accepting validation reports from Cryptographic Modules Testing laboratories.

6.1.3.2. FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION

Dependences: FCS_CKM.2 Cryptographic key distribution
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[listed in Table 5: Cryptographic Operation]** and specified cryptographic key sizes **[listed in Table 5: Cryptographic Operation]** that meet the following: **[listed in Table 5: Cryptographic Operation]**.

6.1.3.3. FCS_CKM.2 CRYPTOGRAPHIC KEY DISTRIBUTION

Dependences: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[cryptographic key distribution method]** that meets the following: **[listed in Table 5: Cryptographic Operation]**.

6.1.3.4. FCS_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION

Dependences: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[cryptographic key zeroization method]** that meets the following: **[The Key Zeroization Requirements in FIPS PUB 140-1/2 Key Management Security Level 1; Zeroization of all private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters shall be immediate and complete]**.

6.1.3.5. FCS_COP_EXP.1 RANDOM NUMBER GENERATION

Dependences: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP_EXP.1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-compliant crypto module running in a FIPS-approved mode.

6.1.3.6. FCS_COP_EXP.2 Cryptographic Operation

Dependences: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP_EXP.2.1 A crypto module shall perform encryption and decryption using the FIPS-140-1/2 Approved [**AES**] algorithm and operating in [**CBC mode**] and supporting FIPS approved key sizes of [**listed in Table 5: Cryptographic Operation**].

FCS_COP_EXP.2.2 A crypto module shall perform encryption and decryption using the FIPS-140-1/2 Approved [**Triple DES**] algorithm and operating in [**CBC mode**] and supporting FIPS approved key sizes of **[listed in Table 5: Cryptographic Operation]**.

Cryptographic operations	Cryptographic algorithm	Key sizes (bits)	Standards
Hashing	SHS	Not Applicable	FIPS PUB 180-3
Message Authentication Code	HMAC	128	FIPS PUB 198
Encryption/decryption	AES	128, 192, 256	FIPS PUB 197
Encryption/decryption of the traffic	Triple DES	112, 168	FIPS PUB 46-3
Public key encryption/decryption and signature generation/verification	RSA	1024, 1536, 2048, 3072, 4096	FIPS PUB 186-2
Cryptographic key generation	PRNG	112, 128, 192, 256	ANSI X9.31

Table 5; Cryptographic Operation

6.1.4. User Data Protection (FDP)

6.1.4.1. FDP_ACC.1a Subset access control – Administrator Access Control

Dependences: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**Administrator Access Control SFP**] on [subjects: **administrators**, objects: **commands**, operations: **execute**].

6.1.4.2. FDP_ACC.1b Subset access control – SSL Access Control

Dependences: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**SSL Access Control SFP**] on [subjects: **SSL clients**, objects: **SSL connections**, operations: **establish, disconnect**].

6.1.4.3. FDP_ACF.1a Security attribute based access control – Administrator Access Control

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

FDP_ACF.1.1 The TSF shall enforce the [**Administrator Access Control SFP**] to objects based on the following: [subjects: **administrators**, subject attributes: **administrator roles**, object: **commands**, object attributes: **none**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Admin Privilege Levels**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

6.1.4.4. FDP_ACF.1B SECURITY ATTRIBUTE BASED ACCESS CONTROL – SSL ACCESS CONTROL

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

FDP_ACF.1.1 The TSF shall enforce the [**SSL Access Control SFP**] to objects based on the following: [subjects: **SSL clients**, subject attributes: **SSL client certificate attributes, source IP, destination IP, source port, destination port**, object: **SSL connections**, object attributes: **none**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Access Control Lists (ACLs)**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

6.1.4.5. FDP_IFC.1 SUBSET INFORMATION FLOW CONTROL

Dependences: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the **[SSL information flow control SFP]** on subjects: **SSL clients**, information: **protected/internal server resources**, operations: **access**].

6.1.4.6. FDP_IFF.1 SIMPLE SECURITY ATTRIBUTES

Dependences: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the **[SSL information flow control SFP]** based on the following types of subject and information security attributes: [subjects: **SSL clients**, subject attributes: **none**, information: **protected/internal server resources**, information attributes: **server address, server port**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**the client has been granted access to the server resource by the Thunder device**].

FDP_IFF.1.3 The TSF shall enforce the [**no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional information flow control SFP rules**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**no additional information flow control SFP rules**].

6.1.5. IDENTIFICATION AND AUTHENTICATION (FIA)

6.1.5.1. FIA_ATD.1 USER ATTRIBUTE DEFINITION

Dependences: None.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [SSL client certificate attributes: **Common Name, Not valid before date/time, Not valid after date/time, Key length, Certification authority signed or self-signed**].

6.1.5.2. FIA_UAU.1A TIMING OF AUTHENTICATION - ADMINISTRATOR

Dependences: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **[identification, SSL/SSH connection establishment]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.3. FIA_UAU_EXP.1 TIMING OF AUTHENTICATION - USER

Dependences: FIA_UID.1 Timing of identification

When the administrator has enabled SSL proxy with client certificate authentication, the TSF shall:

- allow SSL connection with client certificate authentication and SSL connection establishment on behalf of the user to be performed before the user is authenticated;
- require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.5.4. FIA_UAU.5 MULTIPLE AUTHENTICATION MECHANISMS

Dependences: None

FIA_UAU.5.1 The TSF shall provide **[password and certificate based authentication mechanisms]** to support user authentication.

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

a) **authentication of administrators with username and password at the GUI or the CLI, or authentication of administrators with public key at the SSH CLI, such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;**

b) **when the administrator has enabled SSL proxy with client certificate authentication, certificate based authentication mechanism, with client and server certificates, shall be used for users sending information to or receiving information from TOE using HTTPS, such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user].**

6.1.5.5. FIA_UID.1 TIMING OF IDENTIFICATION

Dependences: None.

FIA_UID.1.1 The TSF shall allow **[SSL connection establishment]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

6.1.6. SECURITY MANAGEMENT (FMT)

6.1.6.1. FMT_MOF.1 MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

Dependences: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of*] the functions **[configuration of other admin accounts, change the passwords of other administrators]** to **[Root Admin and Super Admin]**.

6.1.6.2. FMT_MSA.1 MANAGEMENT OF SECURITY ATTRIBUTES

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**Administrator Access Control SFP**] to restrict the ability to [*modify, delete or add*] the security attributes [**admin resources**] to [**Root Admin, Super Admin**].

6.1.6.3. FMT_MSA.2 SECURE SECURITY ATTRIBUTES

Dependences: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [**admin resources**].

6.1.6.4. FMT_MSA.3A STATIC ATTRIBUTE INITIALISATION – ADMINISTRATOR ACCESS CONTROL SFP

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

FMT_MSA.3.1 The TSF shall enforce the [**Administrator Access Control SFP**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Root Admin, Super Admin**] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.5. FMT_MSA.3B STATIC ATTRIBUTE INITIALISATION – SSL ACCESS CONTROL SFP

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

FMT_MSA.3.1 The TSF shall enforce the [**SSL Access Control SFP**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Thunder device**] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.6. FMT_MSA.3C STATIC ATTRIBUTE INITIALISATION – SSL INFORMATION FLOW CONTROL SFP

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

FMT_MSA.3.1 The TSF shall enforce the [**SSL Information flow Control SFP**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Thunder device**] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.7. FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

Dependencies: None.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**admin account configuration**].

6.1.6.8. FMT_SMR.1 SECURITY ROLES

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **[Root Admin, Super Admin, Read Only Admin, Partition Write Admin, Partition Read Admin, Partition RS Operator]**.

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

6.1.7. PROTECTION OF THE TSF (FPT)

6.1.7.1. FPT_FLS.1 FAIL SECURE

Dependencies: None.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**the real servers for the URL requested by the client are unavailable, fan and power supply failures**].

6.1.7.2. FPT_ITC.1 INTER-TSF CONFIDENTIALITY DURING TRANSMISSION

Dependencies: None.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

6.1.7.3. FPT_ITT.1 Basic internal TSF data transfer protection

Dependencies: None.

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

6.1.7.4. FPT_STM.1 Reliable time stamps

Dependencies: None.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2. Security Assurance Requirements (SARs)

Assurance Class	Assurance Components
ADV	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1
AGD	AGD_OPE.1, AGD_PRE.1
ALC	ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1
ATE	ATE_COV.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_VAN.2

Table 6; Assurance requirements: EAL2 Augmented with ALC_FLR.1

For the detailed requirements refer to section 8.

6.3. SECURITY REQUIREMENTS RATIONALE

6.3.1. RELATION BETWEEN SFRS AND SECURITY OBJECTIVES

Objectives / Requirement	FLB_SCO_EXP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.3	FAU_STG.1	FAU_STG.4	FCS_BCM_EXP.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP_EXP.1	FCS_COP_EXP.2	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FDP_IFC.1	FDP_IFF.1	FIA_ATD.1	FIA_UAU.1a	FIA_UAU_EXP.1	FIA_UAU.5	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3a	FMT_MSA.3b	FMT_MSA.3c	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_ITC.1	FPT_ITT.1	FPT_STM.1
O.Load_ Balancing	X																																			
O.Crypto-graphy								X	X	X	X	X	X																							
O.Crypto-graphy_ Validated								X	X	X	X	X	X																							
O.Protect						X																			X						X		X			
O.Admin					X									X		X									X	X	X	X			X	X				
O.Authent-icate																				X	X		X	X	X						X					
O.Audit			X	X	X	X	X	X																												
O.Time																																				X
O.Access_ Int															X		X	X	X			X	X	X					X	X						
O.Integrity						X																									X			X	X	

Table 7; Tracing of functional requirements to objectives

6.3.1.1. O.LOAD_BALANCING

The TOE must provide encrypted SSL connections for load balanced servers with basic firewall protection. **FLB_SCO_EXP.1** provides SSL handshake between clients and servers, firewall protection by means of Access Control Lists and Server Load Balancing on network servers.

6.3.1.2. O.CRYPTOGRAPHY

The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted outside the TOE. **FCS_BCM_EXP.1** is an explicit requirement that specifies the CMVP FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensively the module is tested. **FCS_CKM.1** ensures that, if necessary, the TOE is capable of generating cryptographic keys. **FCS_CKM.2** ensures that, if necessary, the TOE is capable of distribution cryptographic keys. **FCS_CKM.4** mandates the standards (FIPS 140-1/2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. **FCS_COP_EXP.1** performs all Random Number Generation used by the cryptographic functionality. **FCS_COP_EXP.2** requires for data decryption and encryption that CMVP approved algorithms are used, and that the algorithms meet the FIPS PUB 140-1/2 standard.

6.3.1.3. O.CRYPTOGRAPHY_VALIDATED

The TOE will use CMVP FIPS 140-1/2 compliant crypto modules for cryptographic services implementing CMVP approved security functions and random number generation services used by cryptographic functions. **FCS_BCM_EXP.1** is an explicit requirement that specifies the CMVP FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensively the module is tested. **FCS_CKM.1** ensures that, if necessary, the TOE is capable of generating cryptographic keys. **FCS_CKM.2** ensures that, if necessary, the

TOE is capable of distribution of cryptographic keys. **FCS_CKM.4** mandates the standards (FIPS 140-1/2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. **FCS_COP_EXP.1** performs all Random Number Generation used by the cryptographic functionality. **FCS_COP_EXP.2** requires for data decryption and encryption that a CMVP approved algorithms are used, and that the algorithms meet the FIPS PUB 140-1/2 standard.

6.3.1.4. O.PROTECT

The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data. **FAU_STG.1** requires that the TOE prevent unauthorized modifications to the audit data. **FMT_MOF.1** requires that the TOE provide the ability to restrict managing the behaviour of functions of the TOE to authorized users of the TOE. **FMT_SMF.1** supports this objective by identifying the corresponding management functions. **FPT_FLS.1** preserves a secure state when a set of failures occur.

6.3.1.5. O.ADMIN

The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control. **FAU.SAR.1** provides the TOE the ability to review the audit trail of the System. **FDP_ACC.1a** requires the TOE to enforce the Administrator Access Control SFP. **FDP_ACF.1a** specifies the attributes used to enforce the Administrator Access Control SFP. **FMT_MOF.1** restricts access to TOE management functions. **FMT_MSA.1** specifies which roles can access security attributes. **FMT_MSA.2** ensures that only secure values are accepted. **FMT_MSA.3a** defines static attribute initialization for the Administrator Access Control SFP and who can modify the default values. **FMT_SMF.1** specifies the management functions the TOE must provide. **FMT_SMR.1** requires the TOE to maintain separate Administrator roles.

6.3.1.6. O.AUTHENTICATE

The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data. **FIA_ATD.1.1** defines security attributes of subjects used to enforce the authentication policy of the TOE. **FIA_UAU.1a** requires Administrators to be authenticated before they are able to perform any other actions. **FIA_UAU.5** provides multiple authenticated mechanisms to support user authentication. **FIA_UID.1** requires Administrators to be identified before they are able to perform any other actions. **FMT_MOF.1** requires the TOE provide the ability to restrict managing the behaviour of functions of the TOE to authorized users of the TOE. **FMT_SMF.1** supports this objective by identifying the corresponding management functions.

6.3.1.7. O.AUDIT

The TOE must record the actions taken by administrators, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail. **FAU_GEN.1** requires that the TOE records all commands entered by an Administrator. **FAU_GEN.2** requires that the TOE associates events with users. **FAU.SAR.1** requires that the TOE provides the authorized administrators with the ability to read the audit records. **FAU.SAR.3** restricts access to audit records. **FAU.STG.1** requires that the TOE protect the audit records it holds. **FAU.STG.4** requires that the TOE overwrites the oldest audit records if audit trail is full.

6.3.1.8. O.TIME

The TOE must provide reliable timestamps for its own use. **FPT_STM.1** requires that the TOE provides reliable timestamps for its own use.

6.3.1.9. O.ACCESS_INT

The TOE must allow access to server resources on protected/internal network only as defined by the Information Flow Control SFP. **FDP_ACC.1b** requires the TOE to enforce the SSL Access Control SFP. **FDP_ACF.1b** specifies the attributes used to enforce the SSL Access Control SFP. **FDP_IFC.1** requires the TOE to enforce the Information Flow Control SFP. **FDP_IFF.1** specifies the attributes used to enforce the Information Flow Control SFP. **FIA_UAU_EXP.1** requires users to be authenticated before they are able to perform any other actions. **FIA_UAU.5** provides multiple authenticated mechanisms to support user authentication. **FIA_UID.1** requires users to be identified before they are able to perform any other actions. **FMT_MSA.3b** defines static attribute initialization for the SSL Access Control SFP and who can modify the default values. **FMT_MSA.3c** defines static attribute initialization for the SSL Information Control SFP and who can modify the default values.

6.3.1.10. O.INTEGRITY

The TOE must ensure the integrity of all audit and system data. **FAU.STG.1** requires the TOE to protect the stored audit records from unauthorized deletion. **FMT_SMF.1** supports this objective by identifying the corresponding management functions. **FPT_ITC.1** requires the TOE to protect the collected data from disclosure and ensure its integrity when the data is transmitted to another IT product. **FPT_ITT.1** requires the TOE to protect the collected data from disclosure and ensure its integrity when the data is transmitted to a separate part of the TOE.

6.3.2. SFR DEPENDENCIES

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them.

Security functional requirement	Dependency	Rationale
FLB_SCO_EXP.1 Secure communication	None	
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCS_BCM_EXP.1 Baseline cryptographic module	None	

Security functional requirement	Dependency	Rationale
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution FCS_CKM.4 Cryptographic key destruction	Included
FCS_CKM.2 Cryptographic key distribution	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction	Included
FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 Cryptographic key generation	Included
FCS_COP_EXP.1 Random Number Generation	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction	Included
FCS_COP_EXP.2 Cryptographic Operation	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction	Included
FDP_ACC.1a Subset access control – Administrator Access Control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACC.1b Subset access control – SSL Access Control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1a Security attribute based access control - Administrator Access Control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Included
FDP_ACF.1b Security attribute based access control - SSL Access Control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Included
FDP_IFC.1 Subset information flow control	FDP_IFF.1 Simple security attributes	Included
FDP_IFF.1 Simple security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1a Timing of authentication - Administrator	FIA_UID.1 Timing of identification	Included
FIA_UAU_EXP.1 Timing of authentication – User	FIA_UID.1 Timing of identification	Included
FIA_UAU.5 Multiple authentication mechanisms	None	
FIA_UID.1 Timing of identification	None	
FMT_MOF.1 Management of security functions behaviour	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	Included

Security functional requirement	Dependency	Rationale
FMT_MSA.1 Management of security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included
FMT_MSA.2 Secure security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	Included
FMT_MSA.3a Static attribute initialisation - Administrator Access Control SFP	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_MSA.3b Static attribute initialisation - SSL Access Control SFP	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_MSA.3c Static attribute initialisation – Information Flow Control SFP	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_SMF.1 Specification of Management Functions	None	
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	Included
FPT_FLS.1 Fail secure	None	
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	

Table 8; Security functional requirements dependency rationale

6.3.3. SAR Rationale

This ST contains the assurance requirements from the CC EAL2 assurance package augmented with ALC_FLR.1. The SARs that were chosen are consistent with best industry practices for Common Criteria evaluation of similar products.

6.4. Rationale for Explicitly Stated Requirements

Explicit Requirement	Identifier	Rationale
FLB_SCO_EXP.1	Secure communication	This explicit component is necessary since it describes the core functionality, consisting of client/TOE/server communication, firewall protection and load balancing.
FCS_BCM_EXP.1	Baseline cryptographic module	This explicit requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.

Explicit Requirement	Identifier	Rationale
FCS_COP_EXP.1	Random Number Generation	This explicit requirement is necessary since the CC cryptographic operation components address only specific algorithm types and operations requiring specific key sizes. FCS_COP_EXP.1 requires FIPS approved random number generation to be used for all cryptographic functionalities, while FCS_CKM.1 is limited to cryptographic key generation.
FCS_COP_EXP.2	Cryptographic Operation	This explicit requirement is necessary because it describes requirements for a crypto module rather than the entire TSF.
FIA_UAU_EXP.1	Timing of authentication – User	This explicit requirement is necessary to clearly specify the user authentication mechanism.

Table 9; Explicitly stated SFR rationale

7. TOE Summary Specification (ASE_TSS)

7.1. TOE Security Functions Specification

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 6.1.

7.1.1. SF.Load_Balancing

Clients use encrypted SSL connections towards load balanced servers, which are protected by a basic firewall. Clients use SSL to establish secure connections to the TOE. The TOE then may or may not use SSL to establish connection to the servers on the protected network. The TOE, therefore, serves as a TLS proxy. The following load balancing algorithms are supported by the TOE: Round Robin, Active Server, Weighted Preference, and Connection Load.

7.1.2. SF.Security_Audit

The product supports audit records (system logs), related to TOE management and network-related events. The types of events audited are described in table 10. The TOE provides a capability to generate and view events based on the log level (ranges from 0 to 7). The TOE provides support in CLI for view only for user name and IP address, login module and date/time. If the internal audit storage is exhausted then the old records are overwritten, and no alerts are generated. The TOE never outputs sensitive information such as passwords or keys to the log records.

Event Type	Information specified in the log record
Logins and logoffs, authentication	User name, IP address , date/time
Network packet processing logging	IP addresses, date/time, protocol, ports
System upgrade, restart	Administrator name, time of upgrade/restart and upgrade version
CPU usage	shows cpu performance, date/time
Alarms	System log for alarms: fan, power supply, date/time

Table 10; Types of events audited

7.1.3. SF.CRYPTOGRAPHIC_SUPPORT

The SSL cryptographic processing uses a FIPS compliant cryptographic module. The TOE creates and deletes certificate keys at the SSL management configuration.

7.1.4. SF_USERDATA_PROTECTION

The TOE supports the access and flow control operations execute, establish, disconnect and access; with the subject attributes administrator roles, SSL client certificate attributes, source IP, destination IP, source port, destination port; and with the information attributes server address and server port. Server farms can easily be grown in response to changing traffic flow, while protecting the servers behind a common virtual IP address.

7.1.5. SF.IDENTIFICATION_AUTHENTICATION

Administrators can connect to the TOE through the SSL/HTTPS, and must be identified and authenticated before being given access to the TOE. The TOE is then accessed through the GUI in a Web browser by entering the IP address of the Thunder device, using https. Administrators can also access the CLI through a console connection, or an SSH session. Regardless of which connection method is used, access to the Thunder CLI is generally referred to as an EXEC session or simply a CLI session. Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access is password-protected to prevent unauthorized use. When the system administrator has set a password with the enable password global configuration command, users are prompted to enter it before being allowed access to privileged EXEC mode. The password is case sensitive. Client Certificates are used for user authentication. The module uses client certificates with at least 1024 bit RSA key. The TOE allows authentication of administrators using the public key method at the SSH CLI. Client certificate attributes are supported by the product internal database.

7.1.6. SF.SECURITY_MANAGEMENT

A default login IP address is the only restrictive default value when the Thunder TOE product is shipped. The TOE always requires authentication for management interfaces. Administrators can be locked out, meaning that the login possibility for an administrator is disabled for a certain period of time. The Root admin role is never locked out. The TOE has the following access levels; Root, Super Admin, Read Only Admin, Partition Write Admin, Partition Read Admin and Partition RS Operator. Table 10 gives a brief description of management functions available to these roles.

Administrator role	Description
Root	Allows access to all levels of the system. This account can configure other admin accounts. It cannot be deleted.
Super Admin	Allows access to all levels of the system. This account is not the "Root" account and it can be deleted. This account can configure other admin accounts.
Read Only Admin	Allows monitoring access to the system but not configuration access. In the CLI, this account can only access the User EXEC and Privileged EXEC levels, not the configuration levels. In the GUI, this account cannot modify configuration information.
Partition Write Admin	The admin has read-write privileges within the private partition to which the admin is assigned. The admin has read-only privileges for the shared partition.
Partition Read Admin	The admin has read-only privileges within the private partition to

	which the admin is assigned, and read-only privileges for the shared partition.
Partition RS Operator	The admin is assigned to a private partition but has permission only to view service port statistics for real servers in the partition, and to disable or re-enable the real servers and their service ports.

Table 11; Administrator role description

7.1.7. SF.TSF_PROTECTION

The TOE does not provide uncontrolled or unprotected interfaces. The remote management interfaces are encrypted and authenticated using FIPS 140-2-compliant cryptography. The TOE hardware provides timestamps for the TOE's use.

7.2. SECURITY FUNCTIONS RATIONALE

The table below shows that all TOE security requirements can be traced to at least one TOE security function.

Security functions \ Requirement	FLB_SCO_EXP.1	FAU_GEN.1	FAU_GEN.2	FAU.SAR.1	FAU.SAR.3	FAU.STG.1	FAU.STG.4	FCS_BCM_EXP.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP_EXP.1	FCS_COP_EXP.2	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FDP_IFC.1	FDP_IFF.1	FIA_ATD.1	FIA_UAU.1a	FIA_UAU_EXP.1	FIA_UAU.5	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3a	FMT_MSA.3b	FMT_MSA.3c	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_ITC.1	FPT_ITT.1	FPT_STM.1
SF.Load_Balancing	X																																			
SF.Security_Audit		X	X	X	X	X	X																													
SF.Cryptographic_Support								X	X	X	X	X	X																								
SF_Userdata_Protection														X	X	X	X	X	X																		
SF.Identification_Authentication																				X	X	X	X	X													
SF.Security_Management																									X	X	X	X	X	X	X	X					
SF.TSF_Protection																																	X	X	X	X

Table 12; Tracing of security functions to requirements

7.2.1. SF.LOAD_BALANCING

The TOE security function SF.Load_Balancing, "Clients use encrypted SSL connections towards load balanced servers, which are protected by a basic firewall.", meets the load balancing requirements **FLB_SCO_EXP.1.1, FLB_SCO_EXP.1.2, FLB_SCO_EXP.1.3.**

7.2.2. SF.SECURITY_AUDIT

The TOE security function SF.Security_Audit, "The TOE provides a capability to generate and view events based on the log level (ranges from 0 to 7), together with a CLI view only support for user name and IP address, login module and date/time. If the internal audit storage is exhausted then the old records are overwritten, and no alerts are

generated.", meets the audit requirements **FAU_GEN.1, FAU_GEN.2, FAU.SAR.1, FAU.SAR.3, FAU.STG.1, FAU.STG.4.**

7.2.3. SF.CRYPTOGRAPHIC_SUPPORT

The TOE security function SF.Cryptographic_Support, "The SSL cryptographic processing uses a FIPS compliant cryptographic module. The TOE creates and deletes certificate keys at the SSL management configuration.", meets the cryptographic requirements **FCS_BCM_EXP.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP_EXP.1, FCS_COP_EXP.2.**

7.2.4. SF.USERDATA_PROTECTION

The TOE supports access and flow control operations with the attributes administrator roles, username, password, SSL client certificate attributes, source IP, destination IP, source port, destination port. It is possible to grow server farms in response to changing traffic flow, while protecting the servers behind a common virtual IP address.", meets the protection of user data requirements **FDP_ACC.1a, FDP_ACC.1b, FDP_ACF.1a, FDP_ACF.1b, FDP_IFC.1, FDP_IFF.1.**

7.2.5. SF.IDENTIFICATION_AUTHENTICATION

The TOE security function SF.Identification_Authentication, "Users access the TOE through the SSL, and must be identified and authenticated before being given access to the TOE. Client certificate attributes are supported by the product internal database.", meets the identification and authentication requirements **FIA_ATD.1.1, FIA_UAU.1a, FIA_UAU_EXP.1, FIA_UAU.5, FIA_UID.1.**

7.2.6. SF.SECURITY_MANAGEMENT

The TOE security function SF.Security_Management, "The TOE always requires authentication for management interfaces. Administrators can be locked out but the Root Admin is never locked out. The TOE has the access levels Root Admin, Super Admin, Read Only Admin, Partition Write Admin, Partition Read Admin and Partition OS Operator.", meets the management requirements **FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3a, FMT_MSA.3b, FMT_MSA.3c, FMT_SMF.1, FMT_SMR.1.**

7.2.7. SF.TSF_PROTECTION

SSL connections and failures are supported by the TOE. The TOE hardware provides timestamps for the TOE's use.", meets the protection of the TSF requirements **FPT_FLS.1, FPT_ITC.1, FPT_ITT.1, FPT_STM.1.**

8. ASSURANCE REQUIREMENTS

8.1. DEVELOPMENT (ADV)

8.1.1. SECURITY ARCHITECTURE DESCRIPTION (ADV_ARC.1)

The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document. ADV_ARC.1.1C

The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs. ADV_ARC.1.2C

The security architecture description shall describe how the TSF initialisation process is secure. ADV_ARC.1.3C

The security architecture description shall demonstrate that the TSF protects itself from tampering. ADV_ARC.1.4C

The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality. ADV_ARC.1.5C

8.1.2. SECURITY-ENFORCING FUNCTIONAL SPECIFICATION (ADV_FSP.2)

The functional specification shall completely represent the TSF. ADV_FSP.2.1C

The functional specification shall describe the purpose and method of use for all TSFI. ADV_FSP.2.2C

The functional specification shall identify and describe all parameters associated with each TSFI. ADV_FSP.2.3C

For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI. ADV_FSP.2.4C

For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions. ADV_FSP.2.5C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification. ADV_FSP.2.6C

8.1.3. BASIC DESIGN (ADV_TDS.1)

The design shall describe the structure of the TOE in terms of subsystems. ADV_TDS.1.1C

The design shall identify all subsystems of the TSF. ADV_TDS.1.2C

The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing. ADV_TDS.1.3C

The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems. ADV_TDS.1.4C

The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF. ADV_TDS.1.5C

The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke. ADV_TDS.1.6C

8.2. GUIDANCE DOCUMENTS (AGD)

8.2.1. OPERATIONAL USER GUIDANCE (AGD_OPE.1)

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner. AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate. AGD_OPE.1.3C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. AGD_OPE.1.4C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation. AGD_OPE.1.5C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST. AGD_OPE.1.6C

The operational user guidance shall be clear and reasonable. AGD_OPE.1.7C

8.2.2. PREPARATIVE PROCEDURES (AGD_PRE.1)

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures. AGD_PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST. AGD_PRE.1.2C

8.3. LIFE-CYCLE SUPPORT (ALC)

8.3.1. USE OF A CM SYSTEM (ALC_CMC.2)

The TOE shall be labelled with its unique reference. ALC_CMC.2.1C

The CM documentation shall describe the method used to uniquely identify the configuration items. ALC_CMC.2.2C

The CM system shall uniquely identify all configuration items. ALC_CMC.2.3C

8.3.2. Parts of the TOE CM coverage (ALC_CMS.2)

The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE. ALC_CMS.2.1C

The configuration list shall uniquely identify the configuration items. ALC_CMS.2.1C

For each TSF relevant configuration item, the configuration list shall indicate the developer of the item. ALC_CMS.2.3C

8.3.3. Delivery procedures (ALC_DEL.1)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer. ALC_DEL.1.1C

The developer shall use the delivery procedures. ALC_DEL.1.1C

8.3.4. Flaw remediation (ALC_FLR.1)

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE. ALC_FLR.1.1C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. ALC_FLR.1.2C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. ALC_FLR.1.3C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. ALC_FLR.1.4C

8.4. Tests (ATE)

8.4.1. Evidence of coverage (ATE_COV.1)

The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification. ATE_COV.1.1C

8.4.2. Functional testing (ATE_FUN.1)

The test documentation shall consist of test plans, expected test results and actual test results. ATE_FUN.1.1C

The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests. ATE_FUN.1.2C

The expected test results shall show the anticipated outputs from a successful execution of the tests. ATE_FUN.1.3C

The actual test results shall be consistent with the expected test results. ATE_FUN.1.4C

8.4.3. INDEPENDENT TESTING - SAMPLE (ATE_IND.2)

The TOE shall be suitable for testing. ATE_IND.2.1C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. ATE_IND.2.2C

8.5. VULNERABILITY ASSESSMENT (AVA)

8.5.1. VULNERABILITY ANALYSIS (AVA_VAN.2)

The TOE shall be suitable for testing. AVA_VAN.2.1C

9. ASSURANCE MEASURES

The table below lists the assurance components defined by the EAL2 package augmented with ALC_FLR.1, and the documentation submitted as assurance measures.

Assurance component	Component name	Assurance measures
ADV_ARC.1	Security architecture description	Security Design for the Thunder Series
ADV_FSP.2	Security-enforcing functional specification	Security Design for the Thunder Series
ADV_TDS.1	Basic design	Security Design for the Thunder Series
AGD_OPE.1	Operational user guidance	Operational user guidance for the Thunder Series
AGD_PRE.1	Preparative procedures	Preparative procedures for the Thunder Series
ALC_CMC.2	Use of a CM system	CM plan for the Thunder Series
ALC_CMS.2	Parts of the TOE CM coverage	CM plan for the Thunder Series
ALC_DEL.1	Delivery procedures	Delivery Procedures for the Thunder Series
ALC_FLR.1	Flaw remediation	Flaw remediation for the Thunder Series
ATE_COV.1	Evidence of coverage	Security Testing of the Thunder Series
ATE_FUN.1	Functional testing	Security Testing of the Thunder Series
ATE_IND.2	Independent testing – sample	EVIT Security Testing of the Thunder Series
AVA_VAN.2	Vulnerability analysis	Vulnerability analysis of the Thunder Series

Table 13; Assurance Measures