Top Layer Networks

IDS Balancer^{TM} Version 2.2 Appliance

(IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0)

Security Target V2.3

August 31, 2004

TABLE OF CONTENTS

SECTION **PAGE**

Figures and Tables

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification:	Top Layer IDS Balancer™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0)
ST Title:	Top Layer IDS Balancer™ Version 2.2 Appliance Security Target
ST Version:	Version 2.3
ST Authors:	Top Layer Networks
ST Date:	August 31, 2004
Assurance level:	EAL2
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408
Keywords:	Network Security, Load Balancing, Intrusion Detection System (IDS), Information Flow Control, Security Target

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Top Layer IDS Balancer™ Version 2.2 Appliance. The scope of the evaluation includes three models: IDSB3531-CCV1.0, IDSB3532-CCV1.0, and IDSB4508-CCV1.0. The models only differ in the number of ports that they support. The IDS Balancer examines packets on a network, determines their types, and directs them to the appropriate IDS sensor for further analysis. The IDS Balancer also executes load balancing algorithms to distribute packets among multiple IDS sensors that were set up to process that specific type of packet.

1.3 Statement of Conformance

The Target of Evaluation (TOE) is Part 2 extended, Part 3 conformant, and Evaluation Assurance Level 2 (EAL2) conformant.

1.4 Interpretations

This Security Target incorporates the International Common Criteria (CC) Interpretations that were in effect as of 26 September 2003 and that were determined to be applicable to the TOE.

1.5 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, Protection Profile Claims, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and the threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5 specifies the TOE Security Requirements.   The TOE security requirements are made up of TOE Security Functional Requirements, TOE Security Assurance Requirements, Requirements for the IT Environment, and the Strength of Function claim.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures that meet the IT Security Requirements specified in Section 5.

Section 7, Protection Profile (PP) Claims, is not applicable. This product does not claim conformance to any PP.

Section 8, Rationale presents evidence that the ST is a complete and cohesive set of requirements. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Section 9 contains Acronyms and Terminology.

Section 10 contains document references.

2 TOE DESCRIPTION

2.1 Product Type

Top Layer Networks is a developer of a series of appliances that aid consumers in deploying a defense-in-depth security architecture providing intrusion detection and prevention. Top Layer's appliance offerings include secure edge controllers, intrusion prevention systems (IPS), and intrusion detection system (IDS) load balancing and optimizers.

The TOE is the Top Layer IDS Balancer™ Version 2.2 Appliance, henceforth referred to as the "Balancer". The Balancer is a passive, non-inline network appliance that sends copies of data traffic to multiple IDS sensors, henceforth referred to as the "IDS" for different kinds of examination and balances this traffic over one or more IDS for maximum efficiency of resources.

The scope of the evaluation includes three models of the TOE: IDSB3531-CCV1.0, IDSB3532-CCV1.0, and IDSB4508-CCV1.0., which run on the following ASIC-based platforms (AS3531, AS3532, and TL4508, respectively). Each platform runs the same custom developed proprietary set of software and each platform was evaluated and tested. As described in Section 2.2.1, the platforms differ only by the number of ports that they support.

The Balancer is a stateful inspection device. This means that the Balancer copies packets from the network, examines them, maintains a state table for traffic exchanges, and is configured by the Administrator to either drop its copy of a packet or deliver the copy of the packet to attached IDS for detailed analysis. Packets are not changed as they pass through the Balancer.

The copied traffic is generated by computing systems (clients, servers) communicating with each other over the consumer's network. Communication is based on establishing a logical connection between cooperating systems which is called a *session*. A session, based on transport protocols such as TCP or UDP, consists of two unidirectional streams of related data packets passing between the systems, e.g., client to server; server to client. A single unidirectional stream of related data packets is called a *flow.*

The Balancer's main function utilizes a Top Layer technique known as *flow mirroring. Flow Mirroring* directs all copied packets for a flow to a specified IDS for inspection. Being a stateful inspection device, the Balancer ensures that copies of both flows of a session are sent or *mirrored* to the same IDS to provide full context.

To achieve this, a Balancer connects to one or more network segments and mirrors traffic from these segments to one or more IDSs. Multiple input ports, each connected at a different point on the network, may be organized into *input groups* that direct specific sources of traffic to specific *monitor groups,* that is, monitor ports organized into one or more groups. There are two types of input groups:

- Port-based Input Groups: Aggregate traffic from multiple input ports. The Balancer mirrors this traffic based on administrator-defined relationships and destinations.
- Address-based Input Groups: Aggregate traffic based on the source IP address of the traffic. The Balancer identifies traffic by its source IP address and mirrors it to administrator-defined destinations.

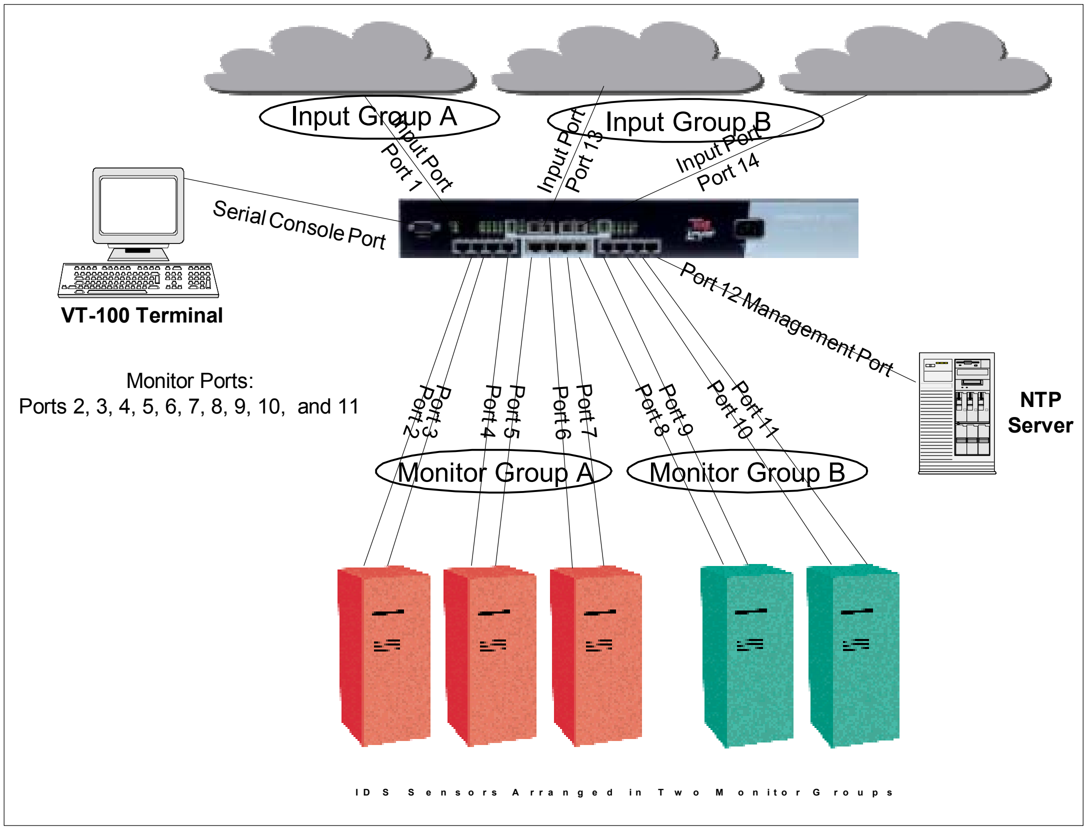
The Balancer balances incoming network traffic loads among the monitor ports in a given monitor group. This grouping feature allows the Balancer to separate network traffic for the delivery to different kinds of security devices, for example, protocol analyzers or sniffers. Monitor groups also allow for the inspection of network traffic from certain input ports, from specific IP address ranges, or from a set of defined traffic types based on network protocol information: IP versus non-IP; TCP, UDP, or other IP protocol; and TCP or UDP Port. Figure 2.1 depicts the Balancer with its input ports organized into multiple input groups, mirroring network traffic to its monitor ports which are organized into multiple monitor groups.

2.2 TSF Boundary and Scope of the Evaluation

The Balancer TOE consists of both a proprietary hardware platform and proprietary software.

The physical boundary of the Balancer is the hardware platform itself. The TOE includes the network ports as well as the local console port that is used for system administration. Network ports are either input, monitor or management ports. Input ports are connected to the network being monitored. Monitor ports are connected to the IDSs. Network traffic is mirrored from input ports to monitor ports. The management port is connected to a trusted management network which includes a Network Time Protocol (NTP) server. A VT-100 terminal is connected to the local console port. The VT-100 terminal is not part of the TOE.

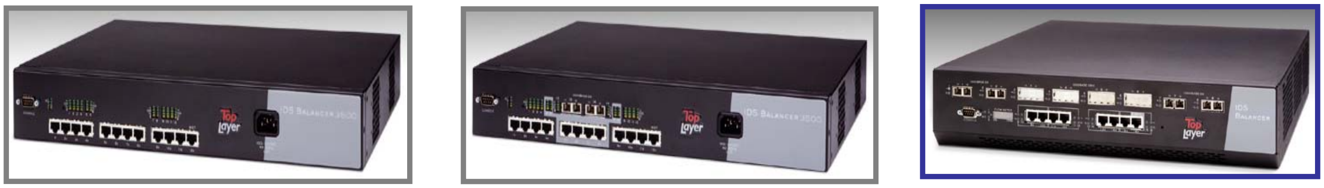
Figure 2.1 –Balancer Model AS3532 in a Network – Sample Configuration



2.2.1 Hardware

Figure 2.2 – IDS Balancer depicts the three hardware models that were evaluated: The Balancer 3500-Series (AS3531, AS3532) and the 4500-Series (TL4508). A Balancer hardware platform consists of the following components: multiple ASICs, memory, input, monitor, and management network ports, a local console port, the SanDisk and the enclosure. All three hardware platforms run the same software.

Figure 2.2 – IDS Balancer Models



The 3500-series has two models, the AS3531 and the AS3532. The AS3531 has 11 10/100 ports in addition to the management port for a total of 12 network ports. The AS3532 has two Gigabit Ports and 11 10/100 ports in addition to the management port for a total of 14 network ports. The TL4508 has eight Gigabit Ports and seven 10/100 Ports in addition to the management port for a total of 16 ports. This is shown in Table 2.1 (Models and Ports).

Table 2.1 – Models and Ports

Model	Type of Port	Number of Ports
AS3531	10BASE – T / 100BASE – TX	12
AS3532	10BASE – T / 100BASE – TX	12
	1000BASE – SX	2
TL4508	10BASE – T / 100BASE – TX	8
	1000BASE – SX	4
	1000BASE – LX or 1000BASE – TX	4

2.2.2 Software

The Balancer uses custom developed proprietary software that controls the entire system. The software consists of the balancer-specific software preloaded on a Compact Flash™ Card (also referred to as a SanDisk).

There is no general-purpose operating system, untrusted software, or programming capabilities on the hardware platform. The command line interface is the only management interface included in the evaluated configuration. Administrators access the command line interface via a VT-100 terminal attached to the serial console port.

The administrator can enable and disable access to the Balancer's management services. The configuration under evaluation only includes management of the Balancer using the serial console port. The following services are disabled in the evaluated configuration and were disabled during testing:

- TopView: Web Management Interface used to configure and manage the Balancer.
- Telnet: Telnet access to the Balancer's Command Line Interface.
- SNMP: Simple Network Management Protocol interface to the Balancer.
- TopFlow: SecureWatch collector's ability to request traffic reports from the Balancer.
- TopViewSecure: Web Management Interface using Secure Socket Layer access (HTTPS).
- OpenSSH: A form of Secure Shell used for Telnet sessions.

The above services are disabled using the Command Line Interface.

2.3 TOE Functionality

The Balancer provides the following security functions:

- Information Flow Control
- Identification and Authentication
- Security Audit
- TOE Access
- Security Management
- Protection of TOE Security Functions

2.3.1 Information Flow Control

The Balancer monitors traffic *flows* from multiple network segments and distributes copies of these flows across one or more groups of attached IDSs. The decision criteria for copying a specific flow are configured by the administrator using the command line interface. All traffic from any specific session is copied to the same output or *monitor port* to the downstream attached IDS. The Balancer also provides the capability to forward TCP Reset packets received from a monitor port to the associated input port.

2.3.2 Identification and Authentication

The Balancer authenticates administrators. Only local (not remote) identification and authentication are included in the evaluated configuration, as administrators access the TOE through the Serial Console Port and the Command Line Interface.

Passwords are used for administrator authentication. The password is any combination of alphabetic and numeric characters that must meet a minimum length of eight characters. The administrator is able to re-set the minimum password length to eight or more characters, but cannot change it to seven or less characters.

A management session is created when an administrator logs in by supplying a valid combination of user name and password. If this information is correct, the administrator is successfully authenticated, and may proceed to issue management commands to the Balancer. If the login attempt is rejected, no management access is granted, and a management session is unable to be established. When the authentication is successful, the management session ends when the administrator logs off.

2.3.3 Security Audit

The Balancer generates event logs that are copied to the SanDisk located on the Balancer and can be viewed by the administrator using the Command Line Interface in the evaluated configuration. The Balancer records auditable events to the event log file to the Balancer's SanDisk. This file is persistent across management sessions unless the system administrator performs a clear-event-log CLI command. This command removes the Balancer's event log file. When the next event occurs, a new event log file is created.

The Balancer audits the following auditable events:

- Start-up of the audit event.
- Port link state changes.
- Management session start up and completion.
- Configuration backup.
- System reboot notification.

The following security relevant information is included in the audit record: date, time, and type of event.

2.3.4 TOE Access

The Balancer provides two features—Console Session Timeout and Banner—that serve to protect against unauthorized access. The Balancer has the capability to terminate the console session after an administrator-defined time period of inactivity. This timeout security function prevents unauthorized access to the Balancer should the administrator move away from the Balancer without logging off from an open management session. The Balancer also allows an administrator to create a customizable banner that is capable of displaying an advisory warning about unauthorized use.

2.3.5 Security Management

There are two trusted user roles: administrator and monitor. Trusted users with the administrator role can set configuration and management options, whereas those with the monitor role can only view them. There are no untrusted Balancer users. The TOE is managed through the Command Line Interface, which provides the necessary functionality to configure and manage the TOE.

2.3.6 Protection of TOE Security Functions

The software and hardware subsystems work together to implement the following security functionality related to Protection of the TSF:

- Non-Bypassability
- Domain separation
- Reliable time stamps

The Balancer ensures that security protection enforcement functions are invoked and succeed before each function within the Balancer's scope of control is allowed to proceed. All management operations are conducted in the context of an associated management session. This management session is allocated *only* after successful authentication. Management operations are checked for conformance to the granted level of access and rejected if not conformant. The management session is destroyed when the corresponding administrator logs out of that session.

The Balancer maintains a security domain to track network traffic flow to determine on which input port traffic arrives and to which monitor port traffic is copied. Traffic flow is based on the information flow policy. Separation is maintained between data from different input ports.

The Balancer also maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

The Balancer's protected domain includes the preloaded software residing on the Balancer's SanDisk that is provided to the customer. The Balancer's software is compiled and built as a single, monolithic entity and is then loaded onto the Balancer's SanDisk. The Balancer has no means for installing, uninstalling, or activating additional applications or components such as libraries or single files below the level of decomposition of this single monolithic entity. The software can only be modified by physically removing the SanDisk, overwriting the appropriate executable file, and replacing the SanDisk and rebooting.

In addition to the Balancer-specific software, other software files that are also stored and dynamically accessed on the SanDisk include the configuration files and log file. These files can only be modified by either violating the physical security of the Balancer and pulling out the SanDisk memory card and accessing those files, or using the appropriate Administrator-level CLI commands to modify the Balancer configuration, save the current Balancer configuration into the configuration file, or clear the event log file.

Either one of these file modification methods requires physical access to the Balancer itself. The underlying assumption regarding the operation of the Balancer is that it is maintained in a physically secure environment. Should a breach in physical security occur, the Balancer is also protected by a tamper-proof seal that makes any physical tampering of the unit evident to the administrator.

The Balancer maintains reliable time stamps for its own use. It is a Network Time Protocol (NTP) client. The NTP client accesses an NTP Server in the IT environment to obtain the time. The Balancer maintains a real-time clock in its hardware, which is equipped with a battery backup power source. The Balancer uses Network Time Protocol (NTP as documented in RFC 1305) to configure its time settings. Synchronization with the NTP server enables time-specific events, such as system logs, to be correlated. The NTP server uses Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).

When the Balancer receives NTP broadcasts, it determines the system time by querying an NTP server at the administrator-defined query interval. The Balancer then updates the system clock.

2.4 IT Environment

The IT environment includes a trusted management network, a VT100 terminal, and an NTP Server. The Balancer relies upon an NTP Server in the IT environment to provide reliable time. The NTP Client and NTP Server communicate using the Network Time Protocol as documented in RFC 1305. The NTP Server is the only platform and service on the trusted management network in the evaluated configuration.

2.5 Operational Environment

The TOE is intended to be used in cases where there is a low level of risk, such as processing unclassified and classified data in a non-hostile environment. Furthermore, the nature of the TOE is to function as a pass-through device within a highly protected physical environment. Packets are not changed as they pass through the Balancer. The TOE is intended to protect itself against attackers with an attack potential of low and the EAL2 Assurance Requirements are consistent with such an environment.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

A.CONNECT The following TOE connectivity requirements are satisfied. The Management Port of the TOE is connected to the Trusted Management Network. The only system on the Trusted Management Network is the Network Time Protocol (NTP) Server. Those responsible for the TOE ensure that the NTP Server is properly configured and adequately protected, for example by a firewall, if it obtains the time from a reliable source over the internet. A VT100 terminal is connected to the local console port for system administration.

A.NO_EVIL Administrators are non-hostile, appropriately trained and follow all administrative guidance.

A.PHYSICAL The IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.TIME The IT environment provides a Network Time Protocol (NTP) Server.

A.TRUSTED_USERS The only users of the TOE are trusted administrators.

3.2 Threats

This Security Target requires that the TOE protect against attackers with an attack potential of low. Attackers are assumed to have a low level of expertise, resources, and motivation.

T.EXAUTH Administrators may be granted more authority than they need to perform their jobs due to the TOE implementing only one trusted role. This increases the risk that they will make security relevant errors in the configuration of the TOE.

T.GUESS An attacker may try to guess administrator authentication data in order to use this information to launch attacks on the TOE.

T.NOAUTH An attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

T.NOBANNER Necessary information about acceptable usage and warnings may not be communicated to the administrator at login increasing the risk of the administrator selecting insecure configuration options.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data resulting in an insecure configuration of the TOE.

T.UNATTENDED An administrator may leave the console unattended resulting in an unauthorized user gaining access to the TOE and making insecure changes to the configuration.

T.UNBALANCE Too much network traffic may be directed to a single IDS so that it is unable to detect the intrusions that it was designed to detect.

T.UNDETECT Security relevant events may go undetected and uncorrected due to their not being recorded, stored, or viewed.

T.USAGE The TOE may be inadvertently configured, used, or administered in an insecure manner by either authorized or unauthorized persons.

4 Security Objectives

This section contains the following:

- Security Objectives for the TOE,
- Security Objectives for the IT Environment, and
- Security Objectives for the Non-IT Environment.

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

O.AUDREC The TOE must provide a means to record, store, and view a readable audit trail of the specified events relating to security management with accurate dates and times.

O.BALANCE The TOE must provide a means of controlling the flow of network traffic from the network being monitored to a specific IDS or groups of IDSs.

O.BANNER The TOE must provide the capability of displaying an advisory warning about unauthorized use of the TOE at login.

O.IDAUTH The TOE must uniquely identify and authenticate all trusted users, before granting such users access to TOE functions.

O.NONBYPASS The TOE must ensure that the security functions of the TOE cannot be bypassed.

O.PWDLEN The TOE must enforce a minimum password length.

O.ROLES The TOE must support two administrative roles, only one of which is granted read access.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.SECSTA The TOE must provide default values for security attributes, so that the TOE does not compromise its resources upon initial startup.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.TIMEOUT The TOE must provide the capability for the administrator to set a time limit on console inactivity before the console session times out.

4.2 Security Objectives for the IT Environment

There is one security objective for the IT environment:

OE.TIME The IT environment must provide an RFC-1305-compliant Network Time Protocol (NTP) Server.

4.3 Security Objectives for the Non-IT Environment

These objectives do not levy any IT requirements, but are satisfied by procedural or administrative measures. The Non-IT security objectives are as follows:

ON.ADMTRA Authorized administrators must be trained in the establishment and maintenance of security policies and practices.

ON.CONNECT The following TOE connectivity requirements are satisfied. The Management Port of the TOE must be connected to the Trusted Management Network. The only system on the Trusted Management Network must be the Network Time Protocol (NTP) Server. Those responsible for the TOE must ensure that the NTP Server is properly configured and adequately protected, for example by a firewall, if it obtains the time from a reliable source over the internet. A VT100 terminal must be connected to the local console port for system administration.

ON.GUIDANCE The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

ON.PHYSICAL Sufficient physical security must be provided for the TOE platform.

ON.TRUSTED_USERS The administrator must ensure that no untrusted users are granted access to the TOE.

5 IT Security Requirements

The conventions for indicating the completions of the operations in the security functional requirements in Sections 5.1 and 5.3 are as follows:

- Selection: Text is bold and enclosed in brackets. An example is “FMT_MOF.1.1 The TSF shall restrict the ability to [**determine the behaviour of**] the functions …”
- Assignment: Text is bolded italics and enclosed in brackets. An example is “FDP_IFC.1.1 The TSF shall enforce the [***Information Flow Control SFP***] on …”
- Refinements: Text is italicized and underlined. An example is FPT_STM.1;2 where “The TSF shall” is replaced by “The *IT environment* shall” in Section 5.3
- Iterations: The component ID is followed by a semicolon followed by an iteration number. An identifying phrase follows the component title in brackets. An example is “**FPT_STM.1;2 Reliable Time Stamps [IT Environment]”**
- Application notes – Introduced by “Application Note:”

5.1 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5.1. They are all taken from Part 2 of the Common Criteria, except for FAU_GEN_LOG.1, which is explicitly stated.

Table 5.1 – Functional Components

No.	Component	Component Name
1	FAU_GEN_LOG.1	Audit log generation
2	FAU_SAR.1	Audit review
3	FAU_STG.1	Protected audit trail storage
4	FDP_IFC.1	Subset information flow control
5	FDP_IFF.1	Simple security attributes
6	FIA_ATD.1	User attribute definition
7	FIA_SOS.1	Verification of Secrets
8	FIA_UAU.2	User authentication before any action
9	FIA_UID.2	User identification before any action
10	FMT_MOF.1	Management of security functions behaviour
11	FMT_MSA.1	Management of security attributes
12	FMT_MSA.3	Static attribute initialization
13	FMT_SMF.1	Specification of management functions
14	FMT_SMR.1	Security roles
15	FPT_RVM.1	Non-bypassability of the TSP
16	FPT_SEP.1	TSF domain separation
17	FPT_STM.1;1	Reliable time stamps [TOE]
18	FTA_SSL.3	TSF-initiated termination
19	FTA_TAB.1	Default TOE access banners

5.1.1 Class FAU: Security Audit

5.1.1.1 FAU_GEN_LOG.1 Audit log generation

Hierarchical to: No other components.

FAU_GEN_LOG.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- ***Start up of audit***
- ***Port link state change***
- ***Management session startup and completion***
- ***Configuration backup***
- ***System reboot notification***

FAU_GEN_LOG.1.2 The TSF shall record within each audit record at least the following information: date, time, and type of event,

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: A port link state change occurs when a port link changes state from valid to down or from down to valid.

5.1.1.2 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [***administrator and monitor***] with the capability to read [***date, time, and type of event***] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.3 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

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

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

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 Class FDP: User Data Protection

5.1.2.1 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the [***Information Flow Control SFP***] on: [

Subjects: External IT Entities

Information: Packet;

Operations:

- ***Copy packet to monitor port***
- ***Drop the packet,***
- ***Forward TCP reset packets]***

Dependencies: FDP_IFF.1 Simple security attributes

5.1.2.2 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

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

Packet Attributes

- ***Input Port: port on which the Balancer receives the packet***
- ***Source IP address: Source IP address in packet,***
- ***Destination IP address: Destination IP address in packet, ,***
- ***Multicast or Unicast: Attribute of packet.***
- ***Application: Determined by network protocol information associated with the network packet: IP versus non-IP; TCP, UDP or other IP protocol, and TCP or UDP Port.***
- ***Network Session: Balancer handles complete flow of traffic for both the forward flow from source to destination and reverse flow from destination to source.***
- ***MAC address: MAC address of devices connected to the Balancer's input ports.***

Input Port Characteristics

- ***Input group membership***
- ***Input group type (port-based or address-based)***
- ***Source IP address range***
- ***MAC address:***

Monitor Port Characteristics

- ***Monitor group membership***
- ***Destination IP address range***
- ***Application. Determined by network protocol information: IP versus non-IP; TCP, UDP or other IP protocol, and TCP or UDP Port.***
- ***Application Flow Timeout:. Time after which information about a flow may not be retained in the flow table when traffic is heavy***
- ***Application priority: Determines which traffic is forwarded during heavy traffic conditions***
- ***Load balancing algorithm (either round robin or weighted round robin)***
- ***Load balancing weight (used in weighted round robin algorithm)]***

Input and Monitor Port Characteristics

- ***Input or monitor Port***
- ***Input port group / monitor port group associations***
- ***Flooding controls matrix; Specifies whether or not multicast traffic is allowed between a specific Input port and a specific Monitor 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: ***[***

1. Input Port to Monitor Port

The TSF shall either copy a packet to a monitor port or drop a packet based on:

- ***Packet attributes,***
- ***Input port characteristics,***
- ***Monitor port characteristics***
- ***Information flow control algorithm.***

Note: The Balancer is a passive device on the network that it is monitoring. Packets are copied from the input port into the Balancer for analysis and processing. When processing is completed, the packet may be copied to one or more monitor ports or dropped. At intermediate steps during the processing of a packet, the packet can be tentatively assigned to a monitor group, but it will not actually be copied to a monitor port at this time.

The TSF shall copy a packet to a monitor port or drop a packet based on the following information flow control algorithm.

Step 1:

If the packet is a multicast packet and the Flooding Controls Matrix specifies a monitor port for the input port, then copy the packet to the specified monitor port and stop, else drop the packet and stop.

Note: the Flooding Controls Matrix specifies whether multicast/broadcast packet arriving at a given Input Port is allowed to be copied to a given Monitor Port. The Flooding Controls Matrix controls flooding of broadcast/multicast traffic on a port-to-port level of granularity.

Note: No other processing is performed on a multicast packet.

Step 2:

If the input port is a member of a port-based input group, then assign the packet to the port-based input group and go to Step 3, else assign the packet to an address-based input group based on source IP address range and go to Step 4 below.

Step 3:

Assign packet to the monitor group(s) associated with the input group and go to Step 5.

Note: Traffic can be assigned to up to four different monitor groups. Steps 5-8 are repeated for each monitor group to which the network traffic is assigned. The packet may be dropped for some monitor groups and copied to a monitor port for others.

Step 4:

If the source IP address falls into an IP address range, then assign the traffic to that IP address range's Address-Based Input Group, else if the source IP address doesn't fall in ANY of the IP address Ranges associated with ANY of the Address-Based Input Groups, the traffic is assigned to the All Hosts Input Group. Then assign the traffic to the monitor group(s) associated with the previously assigned input group and go to Step 5.

Note: Traffic can be assigned to up to four different monitor groups. Steps 5-8 are repeated for each monitor group to which the network traffic is assigned. The packet may be dropped for some monitor groups and copied to a monitor port for others.

Step 5:

If the protocol(s) of the network traffic match an application associated with the input group/monitor group pair(s), then go to Step 6, Else drop traffic and stop.

Step 6:

If the destination address of the network traffic is within the specified destination address range for the application, then go to step 7, else drop the traffic and stop

Step 7:

If traffic conditions allow and the application priority is high enough, then go to step 8 to continue processing, else drop the traffic and stop.

Step 8:

If the packet is the first packet of a session, Then use the Load Balancing algorithm associated with the Monitor Group to copy the first packet of each session to a specific Monitor Port and stop; else copy the packet to the same monitor port as the first packet was copied to and stop

The exception to the rule in Step 8 is occurs if the time limit for application flow timeout is reached before another packet is received for the session. The packet may be handled as the first packet of a new session. In other words, if the time limit for application flow timeout is reached, later packets in a session may not be sent to the same Monitor Port as the first packet.

Note: A session can consist of a flow pair, or the two halves of a bidirectional exchange/conversation. Both halves of the connection are correlated, so that they are assigned by the Load Balancing algorithm to the same Monitor Port (so an IDS won't see just one half of the connection's traffic).

2. Monitor Port to Input Port

If an Input Port is set for the MAC address in the packet, the TSF shall forward TCP reset packets received from a Monitor Port to an Input Port.]

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

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules***: [None]***

Dependencies:

FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

5.1.3 Class FIA: Identification and Authentication

5.1.3.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- ***User Name***
- ***User Role***
- ***Password].***

5.1.3.2 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 [***minimum password length set by the administrator***].

Dependencies: No dependencies

Application Note: The administrator guidance directs the administrator to set a minimum password length of eight characters.

5.1.3.3 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 Timing of identification

5.1.3.4 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

5.1.4 Class FMT: Security Management

5.1.4.1 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**] the functions [***listed in Table 5.2***] to [***the authorised roles identified in Table 5.2***].

Dependencies: FMT_SMR.1 Security roles

Table 5.2 – Management of TSF Data

Security Function	Operation	Authorized Role	Notes
Audit	Clear audit log	Administrator	

Audit	Show audit log	Administrator, Monitor	
Identification and Authentication	Set minimum password length	Administrator	
Identification and Authentication	Show minimum password length	Administrator, Monitor	
Identification and Authentication	Set password	Administrator	
Identification and Authentication	Show user	Administrator or Monitor	
Identification and Authentication	Set user name	Administrator	
Identification and Authentication	Delete user	Administrator	
Identification and Authentication	Connect	Administrator, Monitor	Starts management session
Security Management	Show session	Administrator, Monitor	Shows open management session. There will be only one in the evaluated configuration.
Security Management	Quit	Administrator, Monitor	Ends management session. Unsaved configuration changes are lost.
Security Management	Set user role	Administrator	
Security Management	Reset	Administrator	Equivalent to turning balancer off and on. Unsaved configuration changes are lost.
Security Management	Reset to Factory	Administrator	Resets configuration options to defaults except for IP address, subnet mask, default route, date, and time.
Security Management	Save configuration	Administrator	Saves configuration changes in file on SanDisk.
Security Management	Set management access	Administrator	Used to put the Balancer in the evaluated configuration by denying access to all management interfaces except the CLI interface.
Security Management	Show management access	Administrator, Monitor	Can be used to check with management interfaces are enabled to verify that the Balancer is in the evaluated configuration.
Security Management	Set device name, IP address, and default route	Administrator	

Security Management	Show device name, IP address, default route	Administrator, Monitor	
Security Management	Shutdown	Administrator	Ends management session and shuts down Balancer.
Time	Set IP address of NTP Server	Administrator	
Time	Set NTP client query interval	Administrator	
Time	Show NTP	Administrator, Monitor	
TOE Access	Set banner	Administrator	
TOE Access	Set session timeout value	Administrator	
TOE Access,	Show session timeout value	Administrator, Monitor	

5.1.4.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [***Information Flow Control SFP***] to restrict the ability to ***[Perform operations as specified in Table 5.3 on***] the security attributes [***security attributes as specified in Table 5.3***] to [***the authorized identified roles as specified in Table 5.3].***

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

Table 5.3 – Management of Security Attributes

Attribute(s)	**Operation**	**Authorized Role**
Application, Destination IP address	Create application and associate application with destination IP address	Administrator
Application	Delete application	Administrator
Application	Show application	Administrator or Monitor
Application Flow Timeout	Associate application with an Application Flow Timeout value	Administrator
Application Priority	Set application priority	Administrator
Application Priority	Show application priority	Administrator or Monitor
Application, Input Group, Monitor Group	Associate application/input group with monitor group	Administrator
Application, Input Group, Monitor Group	Remove association between application/input group and monitor group	Administrator
Flooding Controls	Set flooding controls	Administrator
Flooding Controls	Show flooding controls	Administrator or Monitor

Input Group Type	Create input group and specify to be address-based or port-based	Administrator
Input Group	Delete input group	Administrator
Input Group	Show input group	Administrator or Monitor
Input Group Membership	Assign port to port-based input group	Administrator
Monitor Group, Load Balancing Algorithm	Set load balancing algorithm for monitor group	Administrator
Monitor Group, Load Balancing Algorithm	Show monitor group and load balancing algorithm for monitor group	Administrator or Monitor
Monitor Port, Load Balancing Weight	Set load balancing weight for port	Administrator
Port, Load Balancing Weight	Show load balancing weight for port	Administrator or Monitor
Monitor Group	Delete Monitor Group	Administrator
Port Monitor Group Membership	Assign port to monitor group	Administrator
Port Role	Set port to be input port or monitor port	Administrator
Port Role	Show port group	Administrator or Monitor
Source IP address range	Set source IP address range for address-based input group	Administrator
Source IP address range	Delete source IP range for address-based input group	Administrator
Source IP address Range	Show source IP address range	Administrator or Monitor
MAC address	Set MAC address for input port	Administrator
TCP Reset Packet Forwarding	Delete MAC address for input port	Administrator
TCP Reset Packet Forwarding	Show MAC address	Administrator or Monitor

5.1.4.3 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [***Information Flow Control SFP***] to provide [***as specified in Tables 5.4 and 5.5]*** default values for security attributes that are used to enforce the *SF*P.

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

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

Table 5.4 – Default Port Roles

Model	Port Role	Default Ports

TL4508	Input Port	1, 2, 9
TL4508	Monitor Port	7, 8, 10, 11, 12, 13, 14, 15 Assigned to default monitor group
TL4508	Management Port	16
TL4508	Monitor Port if in use; None otherwise.	3, 4, 5, 6
AS3531 and AS3532	Input Port	1
AS3531 and AS3532	Monitor Port	2, 3, 4, 5, 6, 7, 8, 9, 10, 11 Assigned to default monitor group
AS3531 and AS3532	Management Port	12
AS3532 only	Monitor Port if in use; None otherwise	13, 14

Table 5.5 – Default Values of Security Attributes

Attribute	**Default Values**
Input Group	All Hosts
Monitor Group	Default, TopFlow
Port Based or Address Based	Address Based
Source Address Range	0.0.0.0 to 255.255.255.255
Input Group/Monitor Group Association	All Hosts to Default
Applications	As defined in application library
Application Destination Address	0.0.0.0 to 255.255.255.255
Application Priority	Medium
Load Balancing Algorithm	Round Robin
Load Balancing Weight	1
Flooding Configuration Matrix	Enabled for flooding from all input ports to all monitor ports.
TCP Reset Forwarding Configuration Matrix	Disabled. No MAC addresses set for input ports.
User Roles	A users role is set to either administrator or monitor at the time that the user is created.
User Password	toplayer (case sensitive)

5.1.4.4 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 [***as specified in Tables 5.2 and 5.3***]

Dependencies: No Dependencies

5.1.4.5 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [

- ***Administrator, and***
- ***Monitor]***

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

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of the TSF

5.1.5.1 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

5.1.5.2 FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.5.3 FPT_STM.1;1 Reliable time stamps [TOE]

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to *implement an NTP client based on RFC 1305 and* provide reliable time stamps for its own use *based on the time received from the NTP server*.

Dependencies: No dependencies

5.1.6 Class FTA: TOE Access

5.1.6.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1 The TSF shall terminate an interactive session after [***the time interval of user inactivity specified by the administrator***].

Dependencies: No dependencies

5.1.6.2 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Dependencies: No dependencies

5.2 Security Requirements for the IT Environment

There is only one security requirement for the IT environment. The TOE is a Network Time Protocol (NTP) client that accesses an NTP server in the IT environment to obtain the time.

5.2.1.1 FPT_STM.1;2 Reliable time stamps [IT Environment]

Hierarchical to: No other components.

FPT_STM.1.1 The *IT Environment* shall be able to provide reliable time stamps for *the NTP client of the TOE in accordance with RFC 1305.*

Dependencies: No dependencies

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components is refined. The assurance components are listed in Table 5.6.

Table 5.6 - EAL2 Assurance Components

Component	Component Title
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.4 Strength of Function

The minimum strength of function claim for the TOE security functional requirements is SOF-basic. The SOF claim applies to the FIA_UAU.2 User authentication before any action and the FIA_SOS.1 Verification of secrets security functional requirements.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 IFF-1 Information Flow Control

Subjects, Information, and Operations

The information flow control policy is based on the following subjects, information, and operations:

- Subjects: External IT Entities
- Information: Packet;
- Operations:
    - Copy packet to monitor port
    - Drop packet
    - Forward TCP reset packet

Input Port to Monitor Port

The rules to determine whether to copy a packet to a monitor port or to drop the packet are based on packet attributes, input port characteristics, and monitor port characteristics.

The packet attributes and port characteristics are as specified in Section 5.1.2.2 FDP_IFF.1 Simple security attributes under FDP_IFF.1.1.

The information flow control algorithm is specified in Section 5.1.2.2 FDP_IFF.1 Simple security attributes under FDP_IFF.1.2.

More detail about the impact of the application flow timeout attribute is provided here. The application flow timeout value is a feature for tuning the Balancer for a specific network so it does not run out of flows as fast as it would if this feature were not provided. The feature's intent is to speed up the harvesting of entries in the flow table so that the flow table doesn't fill up with flows that are expired. The feature does not result in the Balancer dropping traffic; it will continue to mirror traffic as a new flow. If a flow expires, the number of used entries in the flow table will be reduced by one, and when traffic starts again for the flow, a new entry will be created and the number of used flow entries will increase by one. Externally, the second half of the flow may or may not be mirrored to the same mirror group, depending on the results of following the information flow control algorithm. This feature increases the Balancer's ability to continue functioning during many well-known denial-of-service attacks.

Monitor Port to Input Port

The only information flow from the monitor port to an input port is TCP reset packet forwarding.

The Balancer can forward TCP reset packets received from a Monitor Port to an Input Port if the destination MAC address in the TCP reset packet matches the Static MAC address entry set for an Input Port. This is how the Balancer recognizes which Input Port(s) from which to forward a TCP reset packet. The same static MAC address can be configured to more than one Input Port. The result in this case is that the Balancer makes copies of the TCP reset packet and forwards the copies from all of these Input Ports.

6.1.2 Identification and Authentication

6.1.2.1 IA-1 User Identification

The TSF identifies users with the administrator or monitor role before they are able to access the TOE. Such users are identified by their user name.

6.1.2.2 IA-2 User Authentication

The TOE provides a password mechanism to authenticate administrators and monitors before they are able to access the TOE. If such a user enters an incorrect password, that user cannot log in and cannot issue commands. The SOF claim for this function is SOF-Basic.

6.1.2.3 IA-3 User Attributes

The TSF maintains the following attributes for the two administrator roles that it supports:

- User Name,
- User Role, and
- User Password.

6.1.2.4 IA-4 Minimum Password Length

The TSF is able to enforce a minimum password length of eight characters. The minimum password length can be set by the administrator.

6.1.3 Audit

6.1.3.1 AU-1 Event Log

The TSF is able to record auditable events in the event log. The event log is stored on the SanDisk on the Balancer. There is no interface to modify individual audit records. In addition, it is assumed that the TOE – and, therefore, the SanDisk on it -- is physically protected.

The Balancer records auditable events in the event.log file to the Balancer’s SanDisk. This file is persistent across management sessions unless the administrator performs a “clear-event-log” CLI command. This command removes the Balancer’s event log file until the next event occurs at which point a new event log file is created.

6.1.3.2 AU-2 Auditable Events

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

- Start up of audit
- Port link state change (i.e., a change of state from “valid” to “down” or vice versa)
- Management session startup and completion
- Configuration backup
- System reboot notification

6.1.3.3 AU-3 Audit Information

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

- Date
- Time

- Type of event

6.1.3.4 AU-4 Audit Review

The TSF provides the ability for both the administrator and monitor to view the audit records through the Command Line Interface.

6.1.4 Security Management

6.1.4.1 SM-1 Roles

The TOE maintains two trusted roles:

- Administrator
- Monitor

6.1.4.2 SM-2 Management of security attributes

The administrator can create, modify, and delete the security attributes as specified in Table 5.3 in Section 5.1.

6.1.4.3 SM-3 View Security Attributes

Both the monitor and the administrator can view the security attributes listed in Table 5.3 except for the user password, which neither role can see.

6.1.4.4 SM-4 Default Port Roles

Each model of the Balancer has a varying number of network interfaces (see Table 2.1 in Section 2.2.1). These interfaces come with certain default port roles (i.e., input, monitor) that cannot be changed.. The management port cannot be changed. The default port roles for each model are specified in Table 5.4.

6.1.4.5 SM-5 Default Values of Security Attributes

The Balancer comes to the consumer with a number of security attributes enabled or disabled. These are specified in Table 5.5 No one is authorized to change the security attributes.

6.1.4.6 SM-6 Management of Security Functions

The Administrator role can set configuration options to manage the following security functions: identification and authentication, audit, security management, time, and TOE access.

In contrast, the Monitor user role can only view TSF data, which consists of configuration files, event logs, and system specific information.

Security functions and the authorized roles required to execute them are listed in Table 5.2 in Section 5.1.

6.1.5 TSF Self-Protection

6.1.5.1 FPT-1 Non-Bypassability

The TSF ensures that TOE security functions are non-bypassable. The Balancer ensures that security protection enforcement functions are invoked and succeed before each function within the Balancer's scope of control is allowed to proceed. All management operations are conducted in the context of an associated management session. This management session is allocated *only* after successful authentication. Management operations are checked for conformance to the granted level of access and rejected if not conformant. The management session is destroyed when the corresponding administrator role logs out of that session. Administrators and monitors can only view the audit log(s), security attributes, and TSF data through a special administrative interface, and only after successfully identifying and authenticating themselves.

The Balancer maintains a security domain to track network traffic flow to determine on which input port traffic arrives and to which monitor port traffic is copied. Traffic flow is based on the information flow policy. Separation is maintained between data from different input ports.

The Balancer has no IP address so protocols that require an IP address cannot be used to bypass the security functions. Network packets cannot bypass the balancer. All network packets go through the balancer for examination. Packets are not changed as they pass through the Balancer.

6.1.5.2 FPT-2 Domain separation

The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. The Balancer appliance is a passive device in that it connects to networks via other devices, e.g. LAN switches, mirror ports or via network taps. As such it is not directly part of the network segments it is mirroring from. Also, there is no visible IP address for the device hence it appears transparent to other network nodes and users. Since the Balancer has no IP address, it cannot be subjected to any attacks from the network that require the target to have an IP address. If a malicious user on the network being monitored initiates a network attack, the Balancer simply passes the mirrored packets through transparently to the attached IDS.

The Balancer's protected domain includes the preloaded software residing on the Balancer's SanDisk. The Balancer's software is compiled and built as a single, monolithic entity and is then loaded onto the Balancer's SanDisk. The Balancer has no means for installing, uninstalling, or activating additional applications, or components such as libraries or single files below the level of decomposition of this single monolithic entity. The software can only be modified by physically removing the SanDisk, overwriting the appropriate executable file, and replacing the SanDisk and rebooting.

The TSF enforces separation between the security domains of subjects in the TSC. The Balancer keeps track of the input port on which network traffic arrives and mirrors it to the correct monitor port(s) based on the information flow policy. Separation is maintained between data from different input ports.

The SanDisk is separate from Balancer memory components and is used for non-volatile storage of the Balancer programs, audit log files, and configuration options.

In addition to the Balancer-specific software, other software files that are also stored and dynamically accessed on the SanDisk include the configuration files and log file. These files can only be modified by either violating the physical security of the Balancer and pulling out the SanDisk memory card and accessing those files, or using the appropriate Administrator-level CLI commands to modify the Balancer configuration, save the current Balancer configuration into the configuration file, or clear the event log.

Either one of these file modification methods requires physical access to the Balancer itself. The underlying assumption regarding the operation of the Balancer is that it is maintained in a physically secure environment. Should a breach in physical security occur, the Balancer is also protected by a tamper-proof seal that makes any physical tampering of the unit evident to the trusted user.

6.1.5.3 FPT-3 Reliable time stamps

The TOE retrieves and maintains reliable time stamps for its own use. The TOE is a Network Time Protocol (NTP) client. The NTP client accesses an NTP Server in the IT environment to obtain the time.

The trusted management network includes a computer system that serves as a dedicated Network Time Protocol (NTP) server. The Balancer uses Network Time Protocol (NTP as documented in RFC 1305) to configure its time settings. Synchronization with the NTP server enables time-specific events, such as system logs, to be correlated. The NTP server uses Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). When the Balancer receives NTP broadcasts, it determines the system time by querying an NTP server at the administrator-defined query interval. The Balancer then updates the system clock.

The Balancer maintains a “virtual software time”, also known as UTC time, as part of its functionality. When the Balancer acts as an NTP client receiving packets, the Balancer takes the time from the packet and compares that value with the UTC time. The UTC time is slowly adjusted to synch up with the time server. (Slowly adjusting the time avoids discontinuities in the timestamps.)

The Balancer uses the UTC time for the following purposes:

- Determining whether an “application flow timeout” condition has been reached (FDP_IFF.1)
- Determining whether the time interval of administrator inactivity has been reached (FTA.SSL.3)
- Stamping the date and time of event log records (FAU_GEN_LOG.1).

The Balancer converts the UTC time value to the local time value for time stamps. When the Balancer is initially set up, the administrator is asked to select the local time zone.

6.1.6 TOE Access

The Balancer provides two features—Console Session Timeout and Banner—that serve to protect against unauthorized access. These features are described below.

6.1.6.1 FTA-1 Timeout

The Balancer provides the capability to terminate the console session after an administrator-defined time period of inactivity. This timeout security function prevents unauthorized access to the Balancer should the administrator move away from the Balancer without logging off from an open management session. Only the administrator role administrator is able to perform this function.

A timer within the Balancer is started once a CLI management session begins. With each character of a CLI command entered during that session, the timer is reset. The Balancer continually checks against that timer with the console session timeout value set by the set security CLI command. When the set value is exceeded, the management session ends.

6.1.6.2 FTA-2 Banners

The Balancer allows an administrator to create a customizable banner that is capable of displaying an advisory warning about unauthorized use. The CLI offers an option in its Set Security CLI command to suppress display of the login banner or to set a custom banner (of up to 80 characters).

6.2 Assurance Measures

Table 6.1 identifies the assurance measures provided by the developer to satisfy the EAL2 assurance requirements.

Table 6.1 – Assurance Measures

Component	Title	Assurance Measure
ACM_CAP.2	Configuration Items and how they are uniquely identified	IDSB V2.2 Configuration Management Item List and Policies Version 1.4 DOC-00020
	Evidence that CM system is being used	Top Layer Networks, Inc. Operations and Delivery Procedures Guide Version 1.2, DOC-00022 IDSB V2.2 Configuration Management Item List and Policies Version 1.4 DOC-00020
ADO_DEL.1	Delivery procedures	Top Layer Networks, Inc. Operations and Delivery Procedures Guide Version 1.2, DOC-00022
ADO_IGS.1	Installation, generation, and start-up procedures	IDSB V2.2 Configuration and Management User Guide #990007203 TLN IDS Balancer™ Version 2.2 Command Line Interface (CLI) User Guide with Supplemental Guidance for Common Criteria V1.3 #990-0190-00 Top Layer 3500-Series Hardware Installation #990-0141-03 3500 Top Layer 4500-Series Hardware Installation #990-0142-04-4500 IDSB V2.2 Configuration Worksheets Version 6.0 IDSB V2.2 Release Notes #990-0171
ADV_FSP.1	Informal functional specification	IDSB V2.2 Product Development Specification Document Version 1.9 DOC-00013
ADV_HLD.1	Descriptive high-level design	IDSB V2.2 Product Development Specification Document Version 1.9 DOC-00013
ADV_RCR.1	Informal correspondence demonstration	IDSB V2.2 Representation Correspondence Version 1.6, DOC-00014
AGD_ADM.1	Administrator guidance	IDSB V2.2 Configuration and Management User Guide #990007203 TLN IDS Balancer™ Version 2.2 Command Line Interface (CLI) User Guide with Supplemental Guidance for Common Criteria V1.3 #990-0190-00 Top Layer 3500-Series Hardware Installation #990-0141-03 3500 Top Layer 4500-Series Hardware Installation #990-0142-04-4500 IDSB V2.2 Configuration Worksheets Version 6.0 IDSB V2.2 Release Notes #990-0171
AGD_USR.1	User guidance	Not applicable
ATE_COV.1	Evidence of coverage	ATE_Master List Version 1.1, PLN-00010
ATE_FUN.1	Functional testing	IDS Balancer™ Version 2.2 Appliance, ATE_Master List Version 1.1, PLN-00010 Supplemental Evidence Documentation referenced in the ATE_Master List Version 1.1, PLN-00010
ATE_IND.2	Independent testing – sample	TOE provided for testing
AVA_SOF.1	Strength of TOE	IDSB V2.2 Strength of Function Analysis Version 1.2, DOC-

	security function evaluation	00018
AVA_VLA.1	Developer vulnerability analysis	IDSB V2.2 Vulnerability Analysis Version 1.4, DOC-00017

6.2.1 Configuration management (ACM)

Top Layer utilizes procedures and tools to track the TOE during its development cycle through delivery and installation. Specific items tracked include TOE specifications, test plans, user and administrative guidance, and implementation changes, or deviations after the TOE is manufactured. These configuration items are tracked via:

- Engineering Change Request and Change Control Procedures
- Top Layer Networks Operations and Delivery Procedures Guide
- Software module additions and changes tracking via CASE tools
- Technical Documentation Control Policies
- Creating, Labeling, and Tracking serial numbers and MAC address of each TOE manufactured

The following document provides the configuration item list and describes how Top Layer uniquely identifies its configuration items:

- IDSB V2.2 Configuration Management Item List and Policies

The following documents provide evidence that a CM system is being used:

- Top Layer Networks, Inc. Operations and Delivery Procedures Guide
- IDSB V2.2 Configuration Management Item List and Policies

6.2.2 Delivery and Operation (ADO)

The following document is provided to meet the requirements for ADO_DEL.1 Delivery procedures

- Top Layer Networks Operations and Delivery Procedures Guide

Top Layer provides the documents to meet the requirements for ADO_IGS1 Installation, generation and start-up procedures.

Guidance on how to set up and use the TOE Security Functions of the Balancer and the process of installation, configuration, and usage are documented in:

- Top Layer 3500 Series Hardware Installation
- Top Layer 4500 Series Hardware Installation
- IDS Balancer Configuration and Management Guide (Annotated)
- IDS Balancer Release Notes (Annotated)
- IDSB V2.2 Configuration Worksheets

Guidance on how to install and operate the Balancer in the CC evaluated configuration can be found in:

- Top Layer IDSB V2.2 CLI Command User Guide

6.2.3 Development documentation (ADV)

Design documentation is provided describing the TOE interfaces, functions, and subsystems. This information is found in the following document:

- IDS Balancer Product Development Specification.

This document meets the requirements for ADV_FSP.1 Informal functional specification and ADV_HLD.1 Descriptive high-level design.

The Representation Correspondence document describes the following mappings:

- Mapping from Target of Evaluation Summary Specification (TSS) to the Functional Specification
- Mapping from Functional Specification to High Level Design

6.2.4 Guidance Documentation (AGD)

The following documents are provided to meet the requirements for AGD_ADM.1 Administrator guidance:

- IDS Balancer Configuration and Management Guide
- Top Layer 3500 Series Hardware Installation
- Top Layer 4500 Series Hardware Installation
- TLN IDS Balancer™ Version 2.2 Command Line Interface (CLI) User Guide with Supplemental Guidance for Common Criteria
- Configuration worksheets
- Release Notes

The requirements for AGD_USR.1 User guidance are not applicable, since there are no untrusted users.

6.2.5 Test procedures and test documentation (ATE)

The following documentation was provided to meet the ATE evidence requirements:

- IDS Balancer™ Version 2.2 Appliance,
- ATE_Master List Version 1.1, PLN-00010
- Supplemental Evidence Documentation referenced in the ATE_Master List Version 1.1, PLN-00010

6.2.6 Vulnerability analysis (AVA)

- IDSB V2.2 Strength of Function Analysis – Supplemental Common Criteria Evidence Documentation contains the SOF Analysis

- IDSBS V2.2 Vulnerability Analysis contains the Vulnerability Analysis.

6.3 Strength of Function Claim

The strength of function claim applies to the password authentication mechanism. The related IT security function is IA-2 User authentication. The Strength of Function claim for the password authentication mechanism (IA-2) is SOF-Basic.

A minimum password length of 8 is required in order for the TOE to be able to meet its SOF requirement.

7 PP Claims

The IDS Balancer^{TM} Security Target was not written to claim conformance to any existing Protection Profile.

8 RATIONALE

8.1 Security Objectives Rationale

Table 8.1 shows that all threats are countered and all assumptions are addressed by the security objectives. Rationale is provided following the Table 8.1. Table 8.2 shows that each security objective maps to at least one threat or assumption so that all of the objectives are necessary.

Table 8.1 – All Threats and Assumptions Addressed

Threat		**Objective**
	TOE	
T.EXAUTH	Administrators may be granted more authority than they need to perform their jobs due to the TOE implementing only one trusted role.	O.ROLES
T.GUESS	An attacker may try to guess administrator authentication data in order to use this information to launch attacks on the TOE.	O.PWDLEN
T.NOAUTH	An attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	O.IDAUTH O.NONBYPASS O.SECFUN O.SECSTA
T.NOBANNER	Necessary information about acceptable usage and warnings may not be communicated to the administrator at login increasing the risk of the administrator selecting insecure configuration options.	O.BANNER
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data resulting in an insecure configuration of the TOE.	O.SECSTA O.SELPRO
T.UNATTENDED	An administrator may leave the console unattended resulting in an unauthorized user gaining access to the TOE and making insecure changes to the configuration.	O.TIMEOUT OE.TIME
T.UNBALANCE	Too much network traffic may be directed to a single IDS so that it is unable to detect the intrusions that it was designed to detect.	O.BALANCE OE.TIME
T.UNDETECT	Security relevant events may go undetected and uncorrected due to not being recorded, stored, or viewed.	O.AUDREC OE.TIME
T.USAGE	The TOE may be inadvertently configured, used or administered in an insecure manner by either authorized or unauthorized persons.	O.SECFUN
	Assumptions	

A.CONNECT	The following TOE connectivity requirements are satisfied. The Management Port of the TOE is connected to the Trusted Management Network. The only system on the Trusted Management Network is the Network Time Protocol (NTP) Server. Those responsible for the TOE ensure that the NTP Server is properly configured and adequately protected, for example by a firewall, if it obtains the time from a reliable source over the internet. A VT100 terminal is connected to the local console port for system administration.	ON.CONNECT
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrative guidance.	ON.ADMTRA ON.GUIDANCE
A.PHYSICAL	The IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.	ON.PHYSICAL
A.TIME	The IT environment provides a Network Time Protocol (NTP) Server.	OE.TIME
A.TRUSTED_USERS	The only users of the TOE are trusted administrators.	ON.TRUSTED_USERS

T.EXAUTH states that administrators may be granted more authority than they need to perform their jobs due to the TOE implementing only one trusted role. This threat is countered by O.ROLES, which ensures that the TOE will support multiple administrative roles, so that some administrators can be granted more authority than others.

T.GUESS states that an attacker may try to guess administrator authentication data in order to use this information to launch attacks on the TOE. This threat is diminished by O.PWDLEN, which ensures that the TOE will enforce a minimum password length. This increases the average time required to guess a password using a brute force attack so that the TOE is able to meet its SOF requirement of SOF-Basic.

T.NOAUTH states that an attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE. This threat is countered by O.IDAUTH, O.SECFUN, O.SECSTA, and O.NONBYPASS. O.IDAUTH ensures that the TOE will uniquely identify and authenticate all users, before granting a user access to TOE functions. O.SECFUN ensures that the TOE provides functionality that enables an authorized administrator to use the TOE security functions, and will ensure that only authorized administrators are able to access such functionality. O.SECSTA ensures that the TOE provides default values for security attributes, so that the TOE does not compromise its resources upon initial startup O.NONBYPASS states that the TOE must ensure that the security functions of the TOE cannot be bypassed.

T.NOBANNER states that necessary information about acceptable usage and warnings may not be communicated to the administrator at login increasing the risk of the administrator selecting insecure configuration options. This threat is diminished by O.BANNER, which ensures that the TOE provides the capability of displaying an advisory warning about unauthorized use of the TOE at login.

T.SELPRO states that an unauthorized person may read, modify, or destroy security critical TOE configuration data resulting in an insecure configuration of the TOE. This threat is countered by O.SECSTA and O.SELPRO. O.SECSTA ensures that the TOE provides default values for security attributes, so that the TOE does not compromise its resources upon initial startup. O.SELPRO ensures that the TOE will protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

T.UNATTENDED states that an administrator may leave the console unattended resulting in an unauthorized user gaining access to the TOE and making insecure changes to the configuration. This threat is diminished by O.TIMEOUT, which ensures that the TOE provides the capability for the administrator to set a time limit on console session inactivity before the console session times out. O.TIMEOUT depends on OE.TIME which states that the TOE must obtain its time from an NTP server.

T.UNBALANCE states that too much network traffic may be directed to a single IDS, so that it is unable to detect the intrusions that it was designed to detect. This threat is countered by O.BALANCE. O.BALANCE ensures that the TOE provides a means of controlling the flow of network traffic from the network being monitored to a specific IDS or groups of IDSs. O. BALANCE depends on OE.TIME which states that the TOE must obtain its time from an NTP server.

T.UNDETECT states that security relevant events may go undetected and uncorrected due to not being recorded, stored, or viewed. This threat is countered by O.AUDREC. O.AUDREC ensures that the TOE provides a means to record and view a readable audit trail of security related events, with accurate dates and times. O.AUDREC depends on OE.TIME which states that the TOE must obtain its time from an NTP server.

T.USAGE states that the TOE may be inadvertently configured, used or administered in an insecure manner by either authorized or unauthorized persons. This threat is countered by O.SECFUN. O.SECFUN ensures that the TOE provides functionality that enables an authorized administrator to use the TOE security functions, and will ensure that only authorized administrators are able to access such functionality.

A.CONNECT states that the following TOE connectivity requirements are satisfied: the Management Port of the TOE is connected to the Trusted Management Network; and that the only system on the Trusted Management Network is the Network Time Protocol (NTP) Server, those responsible for the TOE ensure that the NTP Server is properly configured and adequately protected, for example by a firewall, if it obtains the time from a reliable source over the internet, and a VT100 terminal is connected to the local console port for system administration. This assumption is addressed by ON.CONNECT, which ensures that the TOE connectivity requirements will be satisfied.

A.NO_EVIL states that administrators are non-hostile, appropriately trained and follow all administrative guidance. This assumption is addressed by ON.ADMTRA and ON.GUIDANCE. ON.ADMTRA ensures that authorized administrators are trained in the establishment and maintenance of security policies and practices. ON.GUIDANCE ensures that the TOE will be delivered, installed, administered, and operated in a manner that maintains security.

A.PHYSICAL states that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE. This assumption is addressed by ON.PHYSICAL, which ensures that sufficient physical security will be provided for the TOE platform.

A.TIME states that the IT environment provides a Network Time Protocol (NTP) Server. This assumption is directly addressed by OE.TIME, which ensures that the IT environment provides a RFC 1305- compliant Network Time Protocol (NTP) Server.

A.TRUSTED_USERS states that the only users of the TOE are trusted administrators. This assumption is addressed by ON.TRUSTED USERS, which states that the administrator ensures that no untrusted users are granted access to the TOE.

Table 8.2 – All Objectives Mapped to Threats or Assumptions

Objective	Threat or Assumption
O.AUDREC	T.UNDETECT
O.BALANCE	T.UNBALANCE
O.BANNER	T.NOBANNER
O.IDAUTH	T.NOAUTH
O.NONBYPASS	T.NOAUTH
O.PWDLEN	T.GUESS
O.ROLES	T.EXAUTH
O.SECFUN	T.NOAUTH T.USAGE
O.SECSTA	T.NOAUTH T.SELPRO
O.SELPRO	T.SELPRO
O.TIMEOUT	T.UNATTENDED
OE.TIME	A.TIME T.UNATTENDED T.UNBALANCE T.UNDETECT
ON.ADMTRA	A.NO_EVIL
ON.CONNECT	A.CONNECT
ON.GUIDANCE	A.NO_EVIL
ON.PHYSICAL	A.PHYSICAL
ON.TRUSTED_USERS	A.TRUSTED_USERS

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8.3 shows that all of the security objectives of the TOE are satisfied. Rationale text follows Table 8.3. Table 8.4 shows that each security functional requirement maps to at least one objective, so none of the requirements are unnecessary.

Table 8.3 - All Objectives Addressed by SFRs

Objective	Objective Description	SFR
O.AUDREC	The TOE must provide a means to record, store, and view a readable audit trail of the specified events relating to security management with accurate dates and times.	FAU_GEN_LOG.1 Audit log generation FAU_SAR.1 Audit review FAU_STG.1 Protected audit trail storage FPT_STM.1;1 Reliable time stamps [TOE]

O.BALANCE	The TOE must provide a means of controlling the flow of network traffic from the network being monitored to a specific IDS or groups of IDSs.	FDP_IFC.1 Subset information flow control FDP_IFF.1 Simple security attributes FPT_STM.1;1 Reliable time stamps [TOE]
O.BANNER	The TOE must provide the capability of displaying an advisory warning about unauthorized use of the TOE at login.	FTA_TAB.1 Default TOE access banners
O.IDAUTH	The TOE must uniquely identify and authenticate all users, before granting such users access to TOE functions.	FIA_ATD.1 User attribute definition FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action
O.NONBYPASS	The TOE must ensure that the security functions of the TOE cannot be bypassed.	FPT_RVM,1 Non-bypassability
O.PWDLEN	The TOE must enforce a minimum password length.	FIA_SOS.1 Verification of secrets
O.ROLES	The TOE must support two administrative roles, only one of which is granted read access.	FMT_SMR.1 Security roles
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	FMT_MOF.1 Management of security functions behaviour FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialization FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
O.SECSTA	The TOE must provide default values for security attributes, so that the TOE does not compromise its resources upon initial startup.	FMT_MSA.3 Static attribute initialization
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	FPT_RVM.1 Non-bypassability of the TSP FPT_SEP.1 TSF domain separation
O.TIMEOUT	The TOE must provide the capability for the administrator to set a time limit on console session inactivity before the console times out.	FTA_SSL.3 TSF-initiated termination FPT_STM.1;1 Reliable time stamps [TOE]
OE.TIME	The IT environment must provide a RFC 1305- compliant Network Time Protocol (NTP) Server.	FPT_STM.1;2 Reliable time stamps [IT Environment]

O.AUDREC states that the TOE must provide a means to record and view a readable audit trail of the specified events relating to security management with accurate dates and times. This objective is met by FAU_GEN_LOG.1 Audit log generation, FAU_SAR.1 Audit Review, and FPT_STM.1;1 Reliable time stamps [TOE]. FAU_GEN_LOG.1 requires that the TOE record the specific security management events identified in that component. FAU_SAR.1 requires that the TOE provide the capability to review auditable events. FAU_STG.1 requires that the audit records be stored and protected from modification. FPT_STM.1;1 requires that the TOE provide reliable time stamps to be recorded in the audit record.

O.BALANCE states that the TOE must provide a means of controlling the flow of network traffic from the network being monitored to a specific IDS or groups of IDSs. This objective is met by FDP_IFC.1 Subset information flow control, FDP_IFF.1 Simple security attributes, and FMT_MSA.3 Static attribute initialization. FDP_IFC.1 and FDP_IFF.1 require that the information flow security policy defined in those components be enforced. FPT_STM.1;1 requires that the TOE provide reliable time stamps to be used to determine if an application flow timeout has occurred.

O.BANNER states that the TOE must provide the capability of displaying an advisory warning about unauthorized use of the TOE at login. This objective is met by FTA_TAB.1 Default TOE access banners, which requires that the TOE must provide an advisory warning regarding unauthorised use of the TOE.

O.IDAUTH states that the TOE must uniquely identify and authenticate all users, before granting such users access to TOE functions. This objective is met by FIA_ATD.1 User attribute definition, FIA_UAU.2 User authentication before any action, and FIA_UID.2 User identification before any action. FIA_UID.2 and FIA_UAU.2 together require user identification and authentication before the TSF allows any other TSF-mediated actions on the behalf of the user. FIA_ATD.1 requires the specification of user attributes, which include username for identification and password for authentication. FIA_UID.2 requires that users always be identified and FIA_UAU.2 requires that users always be authenticated.

O.NONBYPASS states that the TOE must ensure that the security functions of the TOE cannot be bypassed. This objective is met by FPT_RVM.1 Non-bypassability, which requires that TSP enforcement functions be invoked and succeed before each function with the TSC is allowed to proceed.

O.PWDLEN states that the TOE must enforce a minimum password length. This objective is directly met by FIA_SOS.1 Verification of secrets, which requires a minimum password length.

O.ROLES states that the TOE must support two administrative roles, only one of which is granted read access. This objective is met by FMT_SMR.1 Security roles, which requires two administrative roles: administrator and monitor. The monitor role can only view security attributes and configuration options, but not change them. The Administrator role can modify the values of security attributes and configuration options as well as view them.

O.SECFUN states that the TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality. This objective is met by FMT_MOF.1 Management of TSF data, FMT_MSA.1 Management of security attributes, FMT_MSA.3 Static attribute initialisation, FMT_SMF.1 Specification of management functions, and FMT_SMR.1 Security roles. FMT_MOF.1 and FMT_MSA.1 specify the security functions available to the authorized administrators and the security attributes that the administrators can manage. FMT_MSA.3 specifies that no one is authorized to change the default values. FMT_SMF.1 specifies the security management functions that the TOE supports. FMT_SMR.1 specifies the authorized roles of administrator and monitor.

O.SECSTA states that the TOE must provide default values for security attributes, so that the TOE does not compromise its resources upon initial startup. This objective is met by FMT_MSA.3 Static attribute initialization, which requires that the initial values of security attributes be secure.

O.SELPRO states that the TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. This objective is met by FPT_RVM.1 Non-bypassability of the TSP and FPT_SEP.1 TSF domain separation. FPT_RVM.1 requires that the TOE security functions by non-bypassable. FPT_SEP.1 requires that the TSF provide a domain for its own protection so that its security functions cannot be deactivated or tampered with.

O.TIMEOUT states that the TOE must provide the capability for the administrator to set a time limit on console session inactivity before the console session times out. This objective is met by FTA_SSL.3, which requires that the TSF terminate a session after an administrator-specified period of inactivity. FPT_STM.1;1 requires that the TOE provide reliable time stamps to be used to determine if the time limit for a period of inactivity has been reached.

OE.TIME states that the IT environment must provide an RFC 1305- compliant Network Time Protocol (NTP) Server. This objective is met by FPT_STM.1;2 Reliable time stamps, which requires that the IT environment provide reliable time via an NTP Server.

Table 8.4 – All SFRs Mapped to Objectives

Ref #	Component	Component Title	Objective
		Requirements for the TOE	
1	FAU_GEN_LOG.1	Audit log generation	O.AUDREC
2	FAU_SAR.1	Audit review	O.AUDREC
3	FAU_STG.1	Protected audit trail storage	O.AUDREC
4	FDP_IFC.1	Subset information flow control	O.BALANCE
5	FDP_IFF.1	Simple security attributes	O.BALANCE
6	FIA_ATD.1	User attribute definition	O.IDAUTH
7	FIA_SOS.1	Verification of Secrets	O.PWDLEN
8	FIA_UAU.2	User authentication before any action	O.IDAUTH
9	FIA_UID.2	User identification before any action	O.IDAUTH
10	FMT_MOF.1	Management of security functions behavior	O.SECFUN
11	FMT_MSA.1	Management of security attributes	O.SECFUN
12	FMT_MSA.3	Static attribute initialization	O.SECFUN O.SECSTA
13	FMT_SMF.1	Specification of management functions	O.SECFUN
14	FMT_SMR.1	Security roles	O.ROLES O.SECFUN
15	FPT_RVM.1	Non-bypassability of the TSP	O.NONBYPASS O.SELPRO
16	FPT_SEP.1	TSF domain separation	O.SELPRO
17	FPT_STM.1;1	Reliable time stamps [TOE]	O.AUDREC O.BALANCE O.TIMEOUT
18	FTA_SSL.3	TSF-initiated termination	O.TIMEOUT
19	FTA_TAB.1	Default TOE access banners	O.BANNER
		Requirements for the IT Environment	
1E	FPT_STM.1;2	Reliable time stamps [IT Environment]	OE.TIME

8.2.2 Dependencies

Table 8.5 shows that all SFR dependencies are satisfied. The dependencies of FAU_SAR.1 and FAU_STG.1 on FAU_GEN.1 are met by FAU_GEN_LOG.1 instead. The dependencies of FIA_UAU.1 and FMT_SMR.1 on FIA_UID.1 are met by FIA_UID.2, which is hierarchical to FIA_UID.1.

Table 8.5 – All Dependencies Satisfied

Ref #	Component	Component Name	Dependencies from Part 2	Reference
1	FAU_GEN_LOG.1	Audit log generation	FPT_STM.1	17 1E

Ref #	Component	Component Name	Dependencies from Part 2	Reference
2	FAU_SAR.1	Audit Review	FAU_GEN.1	1 (in lieu of FAU_GEN.1)
3	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1 (in lieu of FAU_GEN.1)
4	FDP_IFC.1	Subset information flow control	FDP_IFF.1	5
5	FDP_IFF.1	Simple security attributes	FDP_IFC.1 FMT_MSA.3	4
6	FIA_ATD.1	User attribute definition	None	-
7	FIA_SOS.1	Verification of Secrets	None	-
8	FIA_UAU.2	User authentication before any action	FIA_UID.1	9 (H)
9	FIA_UID.2	User identification before any action	None	-
10	FMT_MOF.1	Management of security functions behaviour	FMT_SMF.1 FMT_SMR.1	13 14
11	FMT_MSA.1	Management of security attributes	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	4 13 14
12	FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	11 14
13	FMT_SMF.1	Specification of management functions	None	-
14	FMT_SMR.1	Security roles	FIA_UID.1	9 (H)
15	FPT_RVM.1	Non-bypassability of the TSP	None	-
16	FPT_SEP.1	TSF domain separation	None	-
17	FPT_STM.1;1	Reliable time stamps [TOE]	None	-
18	FTA_SSL.3	TSF-initiated time stamps	None	-
19	FTA_TAB.1	Default TOE access banners	None	-
		Requirements for the IT Environment		
IE	FPT_STM.1;2	Reliable time stamps [IT Environment]	None	-

The above table shows that all dependencies identified in the CC Part 2 are satisfied. In addition, although not indicated in the CC text, FDP_IFF.1 and FTA_SSL.3 have dependencies on reliable time stamps, FPT_STM.1.

The dependencies for the assurance requirements are satisfied, since EAL2 is defined so that all the assurance dependencies are satisfied.

8.2.3 Mutual Support

This section provides the rationale that the Security Functional Requirements support each other.

Section 8.2.1 shows that all of the security objectives are satisfied and the all of the security requirements trace to objectives.

Section 8.2.2 shows that all dependencies are satisfied.

Even when no dependency between these requirements is indicated, the security requirements support each other where necessary in the following ways:

- FPT_RVM.1 prevents bypass of other security functional requirements.
- FPT_SEP.1 prevents tampering with other security functional requirements.
- FMT_MOF.1 and FMT_MSA.1 prevent de-activation of other security functional requirements.

- FAU_GEN_LOG.1 enables detection of attacks aimed at defeating other security functional requirements.

The operations on the security functional requirements were reviewed to ensure that they did not affect the mutual support between the requirements.

8.2.4 Requirements Consistency

The Security Functional Requirements are consistent with each other. Inconsistent SFRs (such as identification of users and anonymity) were not selected. Operations were completed in a consistent manner. The following assignments are consistent between SFRs: audit information, information flow control SFP, information to be controlled (packets), information flow control security attributes, and user attributes.

8.2.5 Strength of Function

A strength of function level of SOF-Basic counters an attack level of low. This is sufficient for this TOE, which is intended to be used in environments where the level of risk is low. The SOF claim applies to FIA_UAU.1 and FIA_SOS.1. The SOF analysis is in the following document: IDSB V2.2 Strength of Function Analysis – Supplemental Common Criteria Evidence Documentation.

8.2.6 Assurance Requirements

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.7 Explicitly Stated Requirements

FAU_GEN_LOG.1 was explicitly stated as a substitute for FAU_GEN.1 as the TOE does not record the identity of the subject as FAU_GEN.1.2a requires. FAU_GEN_LOG.1 uses the text of FAU_GEN.1 as a model. The only differences are that the auditable events are explicitly listed and subject is not included in the list of information to be recorded. This ensures that the requirement is measurable and states objective evaluation requirements. This also ensures that including FAU_GEN_LOG.1 does not introduce the need for additional assurance measures. EAL2 assurance measures that are appropriate for FAU_GEN.1 are also appropriate for FAU_GEN_LOG.1

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8.6 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements. Rationale text follows Table 8.6.

Table 8.6 – Mapping of SFRs to IT Security Functions

Ref #	Component	Component Title	IT Security Function
1	FAU_GEN_LOG.1	Audit log generation	AU-1 Event Log

			AU-2 Auditable Events
			AU-3 Audit Information
2	FAU_SAR.1	Audit Review	AU-4 Audit Review
3	FAU_STG.1	Protected audit trail storage	AU-1 Event Log
4	FDP_IFC.1	Subset information flow control	IFF-1 Information Flow Control
5	FDP_IFF.1	Simple security attributes	IFF-1 Information Flow Control
6	FIA_ATD.1	User attribute definition	IA-3 User Attributes
7	FIA_SOS.1	Verification of Secrets	IA-4 Minimum Password Length
8	FIA_UAU.2	User authentication before any action	IA-2 User Authentication
9	FIA_UID.2	User identification before any action	IA-1 User Identification
10	FMT_MOF.1	Management of security functions behaviour	SM-6 Management of Security Functions
11	FMT_MSA.1	Management of security attributes	SM-2 Management of security attributes
			SM-3 View Security Attributes
12	FMT_MSA.3	Static attribute initialization	SM-4 Default Port Roles
			SM-5 Default Values of Security Attributes
13	FMT_SMF.1	Specification of management functions	SM-2 Management of security attributes
			SM-3 View Security Attributes
			SM-6 Management of Security Functions
14	FMT_SMR.1	Security roles	SM-1 Roles
15	FPT_RVM.1	Non-bypassability of the TSP	FPT-1 Non-Bypassability
16	FPT_SEP.1	TSF domain separation	FPT-2 Domain separation
17	FPT_STM.1;1	Reliable time stamps	FPT-3 Reliable time stamps
18	FTA_SSL.3	TSF-initiated termination	FTA-1 Timeout
19	FTA_TAB.1	Default TOE access banners	FTA-2 Banners

FAU_GEN_LOG.1 Audit log generation: This security function is implemented by AU-1 Event Log, AU-2 Auditable Events, and AU-3 Audit Information. AU-1 states that the TOE is able to record events in the audit log. AU-2 identifies the types of events that are logged. AU-3 states that the type of event, time and date are recorded.

FAU_SAR.1 Audit Review is implemented by AU-4 Audit Review, which states that the administrator and monitor roles can view audit records through the command line interface.

FAU_STG.1 Protected audit trail storage is implemented by AU-1 Event Log, which states that the audit log is stored on the SanDisk and there is no interface to modify individual audit records.

FDP_IFC.1 Subset information flow control is implemented by IFF-1 Information Flow Control, which states that the subjects are external IT entities, the protected information is network traffic, and the controlled operations are 1) copy network traffic to monitor port, 2) Forward TCP Reset Packets, and 3) drop the traffic.

FDP_IFF.1 Simple security attributes is also implemented by IFF-1 Information Flow Control. IFF-1 specifies the subjects, information, and operations, identifies the information flow control attributes, and describes the algorithm used to determine whether or not to mirror the network traffic to a monitor port. It also describes the two additional capabilities: TCP Reset Packet Forwarding and Application Flow Control Timeout.

FIA_ATD.1 User attribute definition is implemented by IA-3 User Attributes, which states that the TSF maintains the user attributes: User Name, User Role, and User password.

FIA_SOS.1 Verification of Secrets is implemented by IA-4 Minimum Password Length, which states that the TSF is able to enforce a minimum password length.

FIA_UAU.2 User authentication before any action is implemented by IA-2 User Authentication, which states that the TOE provides a password mechanism to authenticate each user before they are able to access the TOE.

FIA_UID.2 User identification before any action is implemented by IA-1 User Identification, which states that the TSF identifies each user before they are able to access the TOE. Users are identified by their user name.

FMT_MOF.1 Management of security functions behaviour is implemented by SM-6 Management of Security Functions, which describes the management of security functions.

FMT_MSA.1 Management of security attributes is implemented by SM-2 Management of security attributes and SM-3 View Security Attributes.   SM-2 Management of security attributes describes how the administrator role can create, modify, and delete the security attributes. SM-3 View Security Attributes describes how the monitor role can view security attributes.

FMT_MSA.3 Static attribute initialisation is implemented by SM-4 Default Port Roles and SM-5 Default Values of Security Attributes. SM-4 Default Port Roles lists the default port roles for each platform. SM-5 Default Values of Security Attributes lists the default values of security attributes.

FMT_SMF.1 Specification of management functions is implemented by SM-2 Management of security attributes, SM-3 View Security Attributes, and SM-6 Management of Security Functions. SM-2 Management of security attributes describes security management of attributes that can be performed by the administrator role. SM-3 View Security Attributes describes security attributes that can be viewed by the monitor role.   SM-6 Management of Security Functions describes the management of security functions.

FMT_SMR.1 Security roles are implemented by SM-1 Roles, which identifies the two trusted roles: administrator and monitor.

FPT_RVM.1 Non-bypassability of the TSP is implemented by FPT-1 Non-Bypassability, which describes how the Balancer ensures that its security functions are non-bypassable.

FPT_SEP.1 TSF domain separation is implemented by FPT-2 Domain separation, which describes how the Balancer maintains a security domain that protects itself from interference and tampering.

FPT_STM.1;1 Reliable time stamps is implemented by FPT-3 Reliable time stamps, which states that the TOE maintains reliable time stamps for its own use and implements an NTP client to obtain the time from an NTP server.

FTA_SSL.3 TSF-initiated termination is implemented by FTA-1 Timeout, which states that the TSF terminates the console session of a time period of inactivity specified by the administrator.

FTA_TAB.1 Default TOE access banners is implemented by FTA-2 Banners, which states that the TSF is capable of displaying an advisory warning about unauthorized use of the TOE.

Table 8.7 - Mapping of IT Security Functions to SFRs

IT Security Function	Component	Component Title
IFF-1 Information Flow Control	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
IA-1 User Identification	FIA_UID.2	User identification before any action
IA-2 User Authentication	FIA_UAU.2	User authentication before any

		action
IA-3 User Attributes	FIA_ATD.1	User attribute definition
IA-4 Minimum Password Length	FIA_SOS.1	Verification of Secrets
AU-1 Event Log	FAU_GEN_LOG.1	Audit log generation
	FAU_STG.1	Protected audit trail storage
AU-2 Auditable Events	FAU_GEN_LOG.1	Audit log generation
AU-3 Audit Information	FAU_GEN_LOG.1	Audit log generation
AU-4 Audit review	FAU_SAR.1	Audit review
SM-1 Roles	FMT_SMR.1	Security roles
SM-2 Management of security attributes	FMT_MSA.1	Management of security attributes
	FMT_SMF.1	Specification of management functions
SM-3 View Security Attributes	FMT_MSA.1	Management of security attributes
	FMT_SMF.1	Specification of management functions
SM-4 Default Port Roles	FMT_MSA.3	Static attribute initialisation
SM-5 Default Values of Security Attributes	FMT_MSA.3	Static attribute initialisation
SM-6 Management of Security Functions	FMT_MOF.1	Management of security functions behaviour
	FMT_SMF.1	Specification of management functions
FPT-1 Non-Bypassability	FPT_RVM.1	Non-bypassability of the TSP
FPT-2 Domain separation	FPT_SEP.1	TSF domain separation
FPT-3 Reliable time stamps	FPT_STM.1;1	Reliable time stamps
FTA-1 Timeout	FTA_SSL.3	TSF-initiated terminated
FTA-2 Banner	FTA_TAB.1	Default security banners

8.3.2 Assurance Measures Rationale

Table 8.8 identifies the assurance measures provided by the developer to satisfy the EAL2 assurance requirements.

Table 8.8 – Assurance Measures

Component	Title	Assurance Measure
ACM_CAP.2	Configuration Items and how they are uniquely identified	IDSB V2.2 Configuration Management Item List and Policies Version 1.4 DOC-00020
	Evidence that CM system is being used	Top Layer Networks, Inc. Operations and Delivery Procedures Guide Version 1.2, DOC-00022 IDSB V2.2 Configuration Management Item List and Policies Version 1.4 DOC-00020
ADO_DEL.1	Delivery procedures	Top Layer Networks, Inc. Operations and Delivery Procedures Guide Version 1.2, DOC-00022
ADO_IGS.1	Installation, generation, and start-up procedures	IDSB V2.2 Configuration and Management User Guide #990007203 TLN IDS Balancer™ Version 2.2 Command Line Interface (CLI) User Guide with Supplemental Guidance for Common Criteria V1.3 #990-0190-00 Top Layer 3500-Series Hardware Installation #990-0141-03 3500

		Top Layer 4500-Series Hardware Installation #990-0142-04-4500 IDSB V2.2 Configuration Worksheets Version 6.0 IDSB V2.2 Release Notes #990-0171
ADV_FSP.1	Informal functional specification	IDSB V2.2 Product Development Specification Document Version 1.9 DOC-00013
ADV_HLD.1	Descriptive high-level design	IDSB V2.2 Product Development Specification Document Version 1.9 DOC-00013
ADV_RCR.1	Informal correspondence demonstration	IDSB V2.2 Representation Correspondence Version 1.6, DOC-00014
AGD_ADM.1	Administrator guidance	IDSB V2.2 Configuration and Management User Guide #990007203 TLN IDS Balancer™ Version 2.2 Command Line Interface (CLI) User Guide with Supplemental Guidance for Common Criteria V1.3 #990-0190-00 Top Layer 3500-Series Hardware Installation #990-0141-03 3500 Top Layer 4500-Series Hardware Installation #990-0142-04-4500 IDSB V2.2 Configuration Worksheets Version 6.0 IDSB V2.2 Release Notes #990-0171
AGD_USR.1	User guidance	Not applicable
ATE_COV.1	Evidence of coverage	ATE_Master List Version 1.1, PLN-00010
ATE_FUN.1	Functional testing	IDS Balancer™ Version 2.2 Appliance, ATE_Master List Version 1.1, PLN-00010 Supplemental Evidence Documentation referenced in the ATE_Master List Version 1.1, PLN-00010
ATE_IND.2	Independent testing – sample	TOE provided for testing
AVA_SOF.1	Strength of TOE security function evaluation	IDSB V2.2 Strength of Function Analysis Version 1.2, DOC-00018
AVA_VLA.1	Developer vulnerability analysis	IDSB V2.2 Vulnerability Analysis Version 1.4, DOC-00017

ACM_CAP.2

Top Layer provides that following document to specify the configuration item list and describe how Top Layer uniquely identifies its configuration items:

- IDSB V2.2 Configuration Management Item List and Policies

Top Layer provides the following documents as evidence that the CM system is being used:

- Top Layer Networks, Inc. Operations and Delivery Procedures Guide
- IDSB V2.2 Configuration Management Item List and Policies

ADO_DEL.1

Top Layer provides the following documents to meet the requirements for ADO_DEL.1 Delivery procedures

- Top Layer Networks Operations and Delivery Procedures Guide

ADO_IGS.1

Top Layer provides the following documents to meet the requirements for ADO_IGS1 Installation, generation and start-up procedures:

- IDSB V2.2 Configuration and Management User Guide – installation
- TLN IDS Balancer™ Version 2.2 Command Line Interface (CLI) User Guide with Supplemental Guidance for Common Criteria – installation in evaluated configuration
- Top Layer 3500-Series Hardware Installation – hardware installation
- Top Layer 4500-Series Hardware Installation – hardware installation
- IDSB V2.2 Release Notes - installation and configuration information
- IDSB V2.2 Configuration Worksheets –configuration aid

ADV_FSP.1

Top Layer provides the IDS Balancer Product Development Specification to meet the requirements for ADV_FSP.1 Informal functional specification.

ADV_HLD.1

Top Layer provides the IDS Balancer Product Development Specification to meet the requirements for ADV_HLD.1 Descriptive high-level design.

ADV_RCR.1

Top Layer provides the IDSB V2.2 Representation Correspondence to meet the requirements for ADV_RCR.1 Informal correspondence demonstration. This document provides the following mappings:

- Mapping from Target of Evaluation Summary Specification (TSS) to the Functional Specification
- Mapping from Functional Specification to High Level Design

AGD_ADM.1

Top Layer provides the following documents to meet the requirements for AGD_ADM.1 Administrator guidance:

- IDSB V2.2 Configuration and Management User Guide - general information on configuration and management of the IDSB
- TLN IDS Balancer™ Version 2.2 Command Line Interface (CLI) User Guide with Supplemental Guidance for Common Criteria - Provides specific information on managing the TOE in the evaluated configuration.
- Top Layer 3500-Series Hardware Installation – hardware installation
- Top Layer 4500-Series Hardware Installation - hardware installation
- IDSB V2.2 Configuration Worksheets - installation aid
- IDSB V2.2 Release Notes - information on configuration and management

AGD_USR.1

The requirements for AGD_USR.1 User guidance are not applicable, since there are no untrusted users.

ATE_COV.1:

Top Layer provides the ATE Master List to meet the requirements for ATE_COV.1

ATE_FUN.1:

Top Layer provides the following documents to meet the requirements for ATE_FUN.1:

- IDS Balancer™ Version 2.2 Appliance,
- ATE Master List Version 1.1,
- Supplemental Evidence Documentation referenced in the ATE_Master List

ATE_IND.2

Top Layer provides the TOE for testing.

AVA_SOF.1:

Top Layer provides the IDSB V2.2 Strength of Function Analysis – Supplemental Common Criteria Evidence Documentation to meet the requirements for AVA_SOF.1 Strength of security function analysis. This document contains the SOF Analysis.

AVA_VLA.1:

Top Layer provides the IDSBS V2.2 Vulnerability Analysis to meet the requirements for AVA_VLA.1.Developer vulnerability analysis. This document contains the developer vulnerability analysis.

8.3.3 Strength of Function (SOF) Rationale

The SOF requirement applies to the password authentication mechanism. The SOF claim for this mechanism is SOF-Basic. A strength of function level of SOF-Basic counters an attack level of low. This is sufficient for this TOE, which is intended to be used in environments where the level of risk is low. This meets the requirement for a minimum overall SOF level of SOF-Basic.

8.4 PP Claims Rationale

This ST does not claim conformance to any PP.

9 ACRONYMS and TERMINOLOGY

ASIC	Application Specific Integrated Circuit
CC	Common Criteria [for IT Security Evaluation]
COTS	Commercial-Off-The-Shelf
EAL	Evaluation Assurance Level
Flow	A unidirectional stream of related data packets
IT	Information Technology
IDS	Intrusion Detection System
IDSB	IDS Balancer
Mirror	Top Layer technology for passive copying packets from a network segment to an attached intrusion detection system
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TCP	Transmission Control Protocol
Treatment	IDS Balancer policy for mirroring packets from input ports to monitor ports
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UDP	User Datagram Protocol
WMI	Web Management Interface

10 References

Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.

Network Working Group, Request for Comments (RFC)-1305, Network Time Protocol (Version 3), Specification, Implementation and Analysis, Mills, David L., March 1992

U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments Version 1.1; April1999