National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report
Top Layer Networks
IDS Balancer™ Version 2.2 Appliance
(IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0)

Report Number: CCEVS-VR-04-0074
Dated: 03 September 2004
Version: 1.1

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

List of Tables

List of Figures

1. Executive Summary

The evaluation of the Top Layer Networks IDS Balancer™ Version 2.2 Appliance (hereafter referenced as the Balancer), models 3531, 3532, and 4508, was performed by CygnaCom Solutions, Inc. (an entrust Company) in the United States and was completed on 31 August 2004. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.1, Evaluation Assurance Level 2 (EAL2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 1.0.

CygnaCom Solutions, Inc. is an approved NIAP Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 2 (EAL2) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of the Balancer by any agency of the US Government and no warranty of the product is either expressed or implied.

1.1 Top Layer IDS Balancer™ Functionality

The IDS (Intrusion Detection System) Balancer is a passive non-inline network security appliance that is connected to one or more network segments. The Balancer copies and examines the packets on a network, determines their types, and directs them to the appropriate IDS sensor or other types of monitoring sensors such as network analyzers and forensic systems, for further analysis. The IDS Balancer also executes load balancing algorithms to distribute packets among multiple IDS sensors dedicated to processing a specific type of packet (e.g., HTTP, FTP).

The Balancer includes three ASIC-based platforms: the AS3531 and the AS3532 models in the 3500 series and the TL4508 series/model. All three hardware platforms run the same software—including the software for the security functions. The platforms differ only in the number and types of network ports that they support.

The Balancer performs the following 6 security functions, which are described in Section 3 of this report:

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

1.2 Evaluation Details

Table 1-1 provides the required evaluation identification details.

Table 1-1. Evaluation Details

Item	Identification
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	Top Layer Networks IDS Balancer™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0)
EAL	EAL2
Protection Profile	None
Security Target	Top Layer Networks IDS Balancer ™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0) Security Target, Version 2.3, 31 August 2004
Developer	Top Layer Networks, Inc. 2400 Computer Drive, Westborough, MA 01581
Evaluators	Shari Galitzer and Sai Pulugurtha CygnaCom Solutions, Inc. 7925 Jones Branch Drive, McLean, VA 22102-3321
Validator	Elizabeth A. Foreman Mitretek Systems, Inc., Falls Church, VA
Dates of Evaluation	26 September 2003 to 31 August 2004
Conformance Result	Part 2 extended, Part 3 conformant, and EAL2 conformant
Common Criteria (CC) Version	CC, version 2.1, August 1999, and all applicable International Interpretations thereto effective on 26 September 2003
Common Evaluation Methodology (CEM) Version	CEM [Part 1, Introduction and General Model, Version 0.6, January 1997, and Part 2, Evaluation Methodology, Version 1.0, August 1999] and all applicable International Interpretations thereto effective on 26 September 2003
Evaluation Technical Report	Top Layer Networks IDS Balancer™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0) Evaluation Technical Report: - Volume 1, Security Target Evaluation, version 1.2, 31 August 2004 - Volume 2, Evaluation of the TOE, version 1.4, 31 August 2004
Key words	Network Security, Load Balancing, Intrusion Detection System (IDS), Information Flow Control

1.3 Interpretations

The Evaluation Team performed an analysis of the international and national interpretations of the CC and the CEM effective on or before 26 September 2003 (the official starting date of the evaluation) and determined that the international interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) identified below in Table 2.1 were applicable to this evaluation. The Validator determined that the Evaluation Team correctly applied the CCIMB interpretations that it determined to be applicable. In addition, in accordance with CCIMB Interpretation 031's direction to seek guidance from the evaluation authority regarding the duration of the developer's search for obvious vulnerabilities, the developer complied with the guidance in CCEVS PD 008, "When should monitoring of the public domain for new 'obvious vulnerabilities' cease?".

Table 1-2. CCIMB Interpretations Applied to the Evaluation

Interp #	Interpretation Title
003	Unique Identification of Configuration Items in the Configuration List
006	Virtual Machine Description
008	Augmented and Conformant Overlap
009	Definition of Counter
016	Objective for ADO_DEL
024	COTS Product in TOE Providing Security
025	Level of Detail Required for Hardware Descriptions
027	Events and Actions
031	Obvious Vulnerabilities
032	Strength of Function Analysis in ASE_TSS
037	ACM on Product or TOE?
043	Meaning of "Clearly Stated" in APE/ASE_OBJ.1
049	Threats Met by Environment
051	Use of Documentation Without C & P Elements
058	Confusion Over Refinement
064	Apparent Higher Standard for Explicitly Stated Requirements
065	No Component to Call Out Security Function Management
067	Application Notes Missing
075	Duplicate Informative Text for Different Work Units
084	Aspects of Objectives in TOE and Environment
104	Association of Information Flow Attributes with Subjects and Objects
116	Indistinguishable Work Units for ADO_DEL
127	Work Unit Not at the Right Place
138	Iteration and Narrowing of Scope
140	Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR
141	Some Modifications to the Audit Trail are Authorized
150	A Completely Evaluated ST is not Required When TOE Evaluation Starts
202	Selecting one or More Items in a Selection Operation and Using "None" in an Assignment

2. Identification of the TOE

The Top Layer IDS Balancer™ Version 2.2 Appliance includes three ASIC-based platforms, which are listed below with their proper and unique identifications:

- The AS3531 platform: IDSB3531-CCV1.0
- The AS3532 platform: IDSB3532-CCV1.0
- The TL4508 platform: IDSB4508-CCV1.0

All three hardware platforms run the same software—including the software for the security functions. As Table 2-1 below indicates, the platforms/models differ in the number and types of network ports that they support.

Table 2-1. Top Layer Balancer Version 2.2 Appliance Ports Supported

Port Types	Number of Ports Supported Per Platform		
	AS3531	AS3532	TL4508
10BASE-T/ 100BASE-TX	12*	12*	08*
1000BASE-SX		02	04
GBIC ports: 1000BASE-SX or 1000BASE-LX or 1000BASE-TX			04
Total Ports Supported	12	14	16

* Note that 1 port is used as a Management Port

Each of the three platforms of the Balancer has the following components:

1. Physical platform/box/enclosure and electrical connector;
2. Three types of network ports—input, management, and monitor—the number of input and monitor ports depending on the product model;
3. Various application-specific integrated circuits (ASICs) and the memory and clock that they provide and use;
4. The proprietary software on the ASICs that executes the security functions described in sections 2.3 and 6.1 of the Security Target
5. Removable memory, namely, the SanDisk Compact Flash(R) memory card on which the Balancer-specific software has been pre-loaded and on which audit records are stored;
6. One local serial console port to which the customer must connect a VT-100 terminal to use the Command Line Interface (CLI) to perform the security management functions;
7. Guidance and installation documentation; and
8. The following 6 services:
    - 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); and
- OpenSSH: A form of Secure Shell used for Telnet sessions.

However, the TOE consists only of items 1 to 7 of the list above. The 6 services in item 8 and their documentation were not included in the evaluated configuration (i.e., they were neither evaluated nor tested) and the installation procedures for the TOE provide directions to the customer to disable those 6 services.

The TOE consumer will need to provide the following:

- The intrusion detection systems (IDS), protocol analyzers, or other network security devices to which the IDS Balancer distributes packets;
- A VT-100 terminal for administrative CLI-based management/configuration of the IDS Balancer;
- A trusted management network on which the NTP server from which the IDS Balancer retrieves the date and time resides and is accessed;
- An RFC-1305-compliant NTP server;
- Trained administrators; and
- Physical security of the IDS Balancer and the VT-100 terminal attached thereto.

3. Security Policy

Each of the three models of the Balancer provides the same security functions:

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

3.1 Information Flow Control

The Balancer is a passive, non-inline network appliance that sends copies of data traffic to multiple IDS sensors for different kinds of examination and balances this traffic over one or more IDSs for maximum efficiency of resources.

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 an 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 delivery to different kinds of security devices, for example, network analyzers or forensics systems. 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 – for example, IP versus non-IP; TCP, UDP, or other IP protocol; and TCP or UDP Port.

Figure 3-1 illustrates a sample configuration of the AS3532 model with two input groups and two monitor groups.

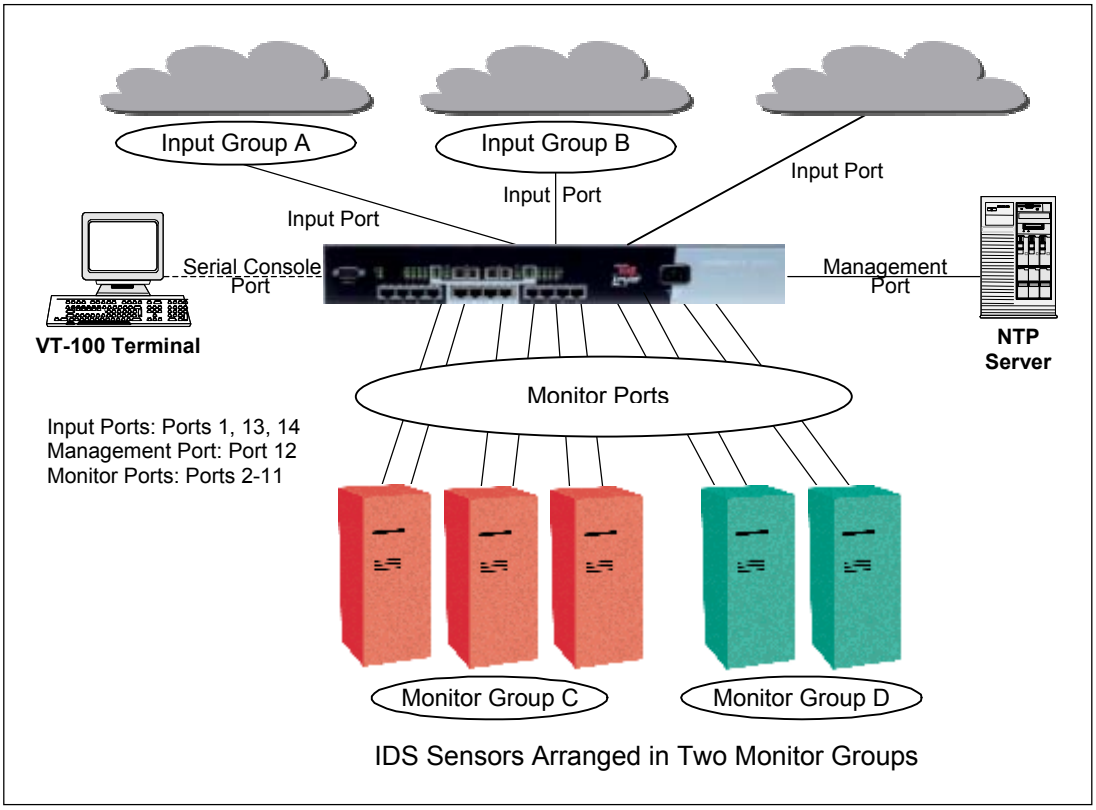

Figure 3-1. Sample Configuration of Model AS 3532 Balancer in a Network

The Balancer allows only one type of information flow from a Monitor Port to an Input Port: forwarding a TCP reset packet. The Balancer forwards TCP reset packets received from a Monitor Port to an Input Port if the destination Medium Access Control (MAC) address in the TCP reset packet matches the Static MAC address entry set for an Input Port. This is how the Balancer recognizes the Input Port(s) to 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.

The policy that is used 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. Section 5.1 2 of the Security Target specifies the packet and port characteristics that an information flow control policy may address and the information flow control algorithm that is followed for input-port-to-monitor-port and monitor-port-to-input-port flows.

3.2 Security Management

Although there are no untrusted Balancer users, there are two trusted user roles: administrator and monitor. Trusted users with the administrator role can set configuration and management options while those with the monitor role can only view them. Security management is accomplished through Command Line Interface commands.

3.3 Identification and Authentication of Administrators

Users with either administrative role must identify and authenticate themselves to the Balancer before initiating a management session. Only local identification and authentication is allowed from a VT-100 terminal connected to the Balancer's Serial Console Port from which the administrator or monitor enters commands with the Command Line Interface.

Passwords are used to authenticate the two types of administrators. The password is any combination of alphabetic and numeric characters with a minimum length of eight characters. The user with the administrator role may re-set the minimum password length to eight or more characters.

A management session is created when a user with the administrator or monitor role logs in by supplying a valid combination of user name and password. If this information is correct, that user is successfully authenticated and may proceed to issue the management commands associated with that particular user's role. If the login attempt is rejected, no management access is granted and no management session is established. When the authentication is successful, the management session ends when the administrator or monitor logs off.

3.4 Security Audit

The Balancer generates event logs that are copied to the Compact Flash™ Card (also referred to as a SanDisk) located on the Balancer. Both the administrator and the monitor may view the event logs on the VT-100 terminal by using the Command Line Interface. The event log file in the SanDisk is persistent across management sessions unless the administrator clears the log with the clear-event-log CLI command, which removes the Balancer's event log file. However, when the next event occurs, a new event log file is created.

The Balancer creates an audit record for the following events – each record identifying the date, time, and type of event:

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

3.5 TOE Access

The Balancer provides two features—Console Session Timeout and Banner—that serve to protect the TOE 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 the administrator to create a customizable banner to display an advisory warning about unauthorized use.

3.6 Protection of the TOE Security Functions

The software and hardware subsystems work together to protect the TOE security functions.

3.6.1 Non-Bypassability of the TOE Security Functions

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 performed by an administrator or monitor are conducted in the context of an associated management session. This management session is allocated only after successful identification and authentication. Management operations are checked for conformance to the user's role and rejected if not conformant. The management session is destroyed when the corresponding administrator logs out of that session.

3.6.2 Domain Separation

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.

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 Command Line Interface 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 or monitor.

3.6.3 Reliable Time Stamps

The Balancer retrieves and maintains reliable time stamps for its own use. As a Network Time Protocol (NTP) client, it accesses an NTP Server in the IT environment to obtain the date and time. The Balancer maintains a real-time clock in its hardware, which is equipped with a battery backup

power source. The Balancer uses the Network Time Protocol (NTP as documented in RFC 1305) to configure its time settings. Periodic 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 the NTP server at the administrator-defined query interval. The Balancer then updates the system clock.

4. Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which the Balancer is expected to operate.

4.1 Usage Assumptions

The assumptions listed below are not addressed by any IT requirements but instead rely on the procedural or administrative measures applied to the operating environment.

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 VT-100 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.

4.2 Environmental Threats

The TOE is able to 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 unsecure 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.

5. Architectural Information

The Balancer has two subsystems: 1) the Software Subsystem, and 2) the Hardware Subsystem.

The Hardware Subsystem includes the platform (Models AS3531, AS3532, and TL4508) and the firmware. The platform consists of the following components: multiple ASICs, memory, 3 kinds of ports (input, monitor, and management), a local serial console port, the SanDisk, and the enclosure. The firmware is the software image loaded onto the ASICs.

The Software Subsystem consists of custom developed proprietary software that controls the entire system. All three hardware platforms run the same software. The entire software subsystem resides on the SanDisk (also referred to as a Compact Flash™ Card), and includes the following files: Balancer-specific software image; current.cfg; temp.cfg; backup.cfg; bootrom.cfg; and event.log. The old-event.log file is created if the event log reaches a size of 512 KB.

The two subsystems communicate during initialization and during operation via file input/output operations between an ASIC and the software files located on the SanDisk.

Table 5.1 identifies the subsystems involved with the TOE Security Functions.

Table 5-1. Subsystems for Security Functions

Security Function	TOE Subsystem(s)
Information Flow Control	Hardware
Identification and Authentication of Administrator	Hardware
Security Audit	Hardware and Software
Security Management	Hardware and Software
Protection of TOE Security Functions	Hardware and Software
TOE Access	Hardware

The Balancer has the following types of ports to communicate with external devices:

- Serial console port to which a VT-100 terminal is connected to support administrator access
- Three types of network ports:
  - Input ports from which packets from the network enter the Balancer
  - Monitor ports to which the Balancer sends the packets that it examines
  - Management port

The Balancer works with two external components to perform its security functions:

- A VT-100 console terminal that is connected to the Balancer via a serial console and that provides administrator access to the Security Management security function

- An NTP server that resides on a trusted management network that is connected to the Balancer's management port and which the Balancer accesses to synchronize its internal clock.

6. Documentation

Top Layer Networks provides the following documentation with the Balancer to consumers:

- For all three models:
  - 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
  - IDSB V2.2 Configuration Worksheets Version 6.0
  - IDSB V2.2 Release Notes #990-0171
- For Models AS3531 and AS3532:
  - Top Layer 3500-Series Hardware Installation #990-0141-03 3500
- For Model TL4508:
  - Top Layer 4500-Series Hardware Installation #990-0142-04-4500

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Tests

The developer provided test plans, procedures, test results, and a test coverage analysis. The Plan identified the test configuration and the specific test hardware and tools that were used for the tests. The developer used a mixture of both positive and negative test cases.

The Evaluation Team determined that the developer's approach and effort were appropriate for this EAL2 evaluation.

Since all of the security functions behave in the same way on all three models, the developer chose to perform all tests on the 4508 model. The developer used manual tests whereby testers entered Command Line Interface commands into a VT-100 terminal to test all six of the security functions, including (but not limited to) operations like the following:

- Installation and configuration of the Balancer
- Management of the security attributes
- Managing the six security functions (set password length, clear/show the audit log)
- Retrieval of the timestamp and date from the NTP server

The developer then referred to the screen shots that were captured for each step/command entered for a particular test scenario to verify whether the actual results were consistent with the expected results.

For tests of the Balancer's information flow control function, the developer used a network traffic generator to generate and send packets to 3 Input Ports and a PC with multiple Network Interface Cards to simulate the IDSs (configured in 4 monitor groups) to which the Balancer would distribute those packets, depending on the policies that were configured for the Input and Monitor Ports. Note that the number of Input Ports and Monitor Ports that were in operation differed depending on the particular set-ups for each test. The PCs collected the traffic that was sent to them and Top Layer testers used a traffic analyzer tool to verify that the correct input packets were received.

7.2 Evaluation Team Independent Testing

Since the primary function of the IDS Balancer system is information flow control, the information flow security functions were considered to be the most important functions to test. The remaining security functions support information flow control through identification and authentication, security management, self-protection, and audit.

The Evaluation Team's goals were to gain additional confidence in Top Layer's test results and to provide independent confirmation of those results. The Evaluation Team selected 30 per cent of the developer's tests for each security function. Additional tests in excess of this sample were selected in accordance with the following criteria:

- Significance of security function: Since the Balancer is mainly an information control product, the information flow control security function and the security management

security function that is used to manage and configure the Balancer were determined to be of primary significance

- Complexity of the security function: The information flow control security function also met this criterion.

The Evaluation Team wrote tests to cover all security functions but emphasized testing the information flow control function because of its significance and the identification and authentication security functions because Top Layer's testing was lightest for that security function.

The Evaluation Team ran tests on models 4508 and 3532 at the Top Layer Networks Westborough, MA, facility:

- Model 4508: Team-defined manual tests and developer-provided information flow tests
- Model 3532: Team-defined information flow tests, developer-provided manual tests, and penetration testing

The test configuration was similar to the developer's regarding the number of input and monitor ports used – with the number of input ports and monitor ports varying depending on the tests. While a VT-100 terminal simulator, an IDS Balancer, and an NTP server were sufficient to run the tests of the Security Management, Identification and Authentication, and Audit security functions, the Information Flow Control-related tests required the usage of a single Linux computer with multiple Network Interface Cards to simulate multiple IDSs and the NTP server. Another Linux computer was used to simulate the VT-100 terminal. A traffic analyzer tool was used to verify the text files that were created as a result of receiving traffic from the Balancer.

The tests were successful, with the actual results matching the expected results.

7.3 Evaluation Team Penetration Tests

Building on the developer's vulnerability analysis, the Evaluation Team performed tests to do the following:

- Verify the duration of time needed to identify and authenticate an administrator to confirm the assumption in the developer's Strength of Function (SOF) analysis regarding the identification and authentication mechanism
- Verify that the telnet, SSH, and other web GUI interfaces are unavailable in the evaluated configuration
- Analyze the management port interface by using NMAP scanners for any obvious backdoors.

In general, the penetration tests were successful, with the actual results being consistent with the expected results. The evaluator did not find any vulnerability during the penetration testing. However the results of some of the *ad hoc* tests that the evaluator also performed required clarification regarding the behavior of the Balancer from the developer – and inclusion of such clarification in the guidance documentation provided to consumers.

8. Evaluated Configuration

The Top Layer IDS Balancer™ Version 2.2 Appliance includes three ASIC-based platforms, which are listed below with their proper and unique identifications:

- The AS3531 platform: IDSB3531-CCV1.0
- The AS3532 platform: IDSB3532-CCV1.0
- The TL4508 platform: IDSB4508-CCV1.0

All three hardware platforms run the same software—including the software for the security functions. The platforms/models differ only in the number and types of network ports that they support (see Table 2-1).

Each of the three platforms of the Balancer has the following components:

1. Physical platform/box/enclosure and electrical connector;
2. Three types of network ports—input, management, and monitor—the number of input and monitor ports depending on the product model;
3. Various application-specific integrated circuits (ASICs) and the memory and clock that they provide and use;
4. The proprietary software on the ASICs that executes the security functions described in sections 2.3 and 6.1 of the Security Target
5. Removable memory, namely, the SanDisk Compact Flash(R) memory card on which the Balancer-specific software has been pre-loaded and on which audit records are stored;
6. One local serial console port to which the customer must connect a VT-100 terminal to use the Command Line Interface (CLI) to perform the security management functions;
7. Guidance and installation documentation.

9. Results of the Evaluation

The Balancer satisfies all of the EAL2 assurance requirements against which it was evaluated. The EAL2 assurance requirements include the following:

Table 9-1. EAL2 Components

EAL2 Component	EAL2 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

The Security Target provides a detailed description of how the Balancer meets each of the listed components.

10. Validation Comments/Recommendations

The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices.

The Validator agrees that the CCTL presented appropriate rationales to support the Evaluation Results presented in Section 4 of the ETR, volume 1, and the Conclusions presented in Section 5 of the ETR, volume 1.

The Validator, therefore, concludes that the evaluation and the Pass results for the TOE identified below is complete and correct:

> Top Layer Networks IDS Balancer™ Version 2.2 Appliance
> (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0)

11. Security Target

The Security Target is entitled, *Top Layer Networks IDS Balancer™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0) Security Target*, Version 2.3, 31August 2004.

12. List of Acronyms

Acronym	Definition
ASIC	Application-Specific Integrated Circuit
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
EAL2	Evaluation Assurance Level 2
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
MAC	Medium Access Control
NIAP	National Information Assurance Partnership
NMAP	Network Mapper
NTP	Network Time Protocol
PD	(CCEVS) Precedent Database
RFC	Reference For Comment
SNMP	Simple Network Management Protocol
SSH	Secure shell
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UDP	User Data Protocol
UTC	Coordinated Universal Time

13. Bibliography

The following documents were used in compiling this Validation Report:

- Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999:
  - Part 1: Introduction and General Model
  - Part 2: Security Functional Requirements
  - Part 2: Annexes
  - Part 3: Security Assurance Requirements

- Common Evaluation Methodology for Information Technology Security:
  - Part 1: Introduction and General Model, Version 0.6, 11 January 1997
  - Part 2: Evaluation Methodology, Version 1.0, August 1999

- Top Layer Networks IDS Balancer ™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0) Security Target, Version 2.3, 31 August 2004

- Top Layer Networks IDS Balancer™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0) Evaluation Technical Report, 31 August 2004:
  - Volume 1, Security Target Evaluation, Version 1.2
  - Volume 2, Evaluation of the TOE, Version 1.4

- Top Layer Networks IDS Balancer™ Version 2.2 Appliance (IDSB3531-CCV1.0, IDSB3532-CCV1.0, IDSB4508-CCV1.0) EAL2 On-Site Audit and Testing, Version 1.1, 26 August 2004