National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Top Layer Networks IPS 5500 E Version 5.21

Models IPS 5500-150E, IPS 5500-500E, and IPS 5500-1000E

Report Number: CCEVS-VR-VID10302-2009

Dated: April 10, 2009

Version: Version 1.0

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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Franklin Haskell

Jean Hung

MITRE Corporation

Bedford, MA

Common Criteria Testing Laboratory

Sai Pulugurtha

Aruna Gandreti

Gary Grainger (Ashton Security Laboratories)

CygnaCom Solutions

McLean, VA

Table of Contents

List of Figures

List of Tables

1.0 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product Top Layer Networks IPS 5500 E Version 5.21 on Models IPS 5500-150E, IPS 5500-500E, and IPS 5500-1000E.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The Top Layer IPS 5500 E is a single-appliance security gateway Intrusion Protection System. The IPS Unit provides network-level and application-level protection to a network from good, bad and suspicious traffic. The TOE acts as an inline single-appliance security gateway providing three-dimensional protection to stop resource abuse, prohibit access to unauthorized clients and stop malicious content from entering the protected network. Top Layer's s ASIC technology and algorithms integrate stateful analysis techniques with deep packet inspection chip set and DoS (Denial of Service) attack protection to provide protection from Internet-based and internal threats. The difference between the TOE and a typical IDS is that the TOE (IPS Unit) is deployed inline and not in an offline or a passive mode.

The TOE may be configured to:

- Handle IP fragments, TCP header and Payload.
- Implement firewall rules.
- Perform protocol analysis.
- Perform deep packet inspections.
- Handle network and security management.
- Process events, logging, and reports.

The primary design goal of the TOE is reliable protection of customer's critical on-line assets. The IPS aspect of the TOE security policy may be configured based on the following three types of rules. The rules guide the following types of security checks:

Firewall Rules — Provide classic firewall blocking for traffic, based on IP addresses, Layer 4 ports, and segments (port pairs).

IPS Rules — Provide the following types of checks:

- Protocol validation
- Attack Signatures
- Acceptable use of network application

Rate Based Rules — Protect your resources from overuse by legitimate users, as well as abusive denial-of-service attackers. Provide limits for:

- Client requests
- Connections for both clients and servers
- SYN Flood controls
- Application rate limiting

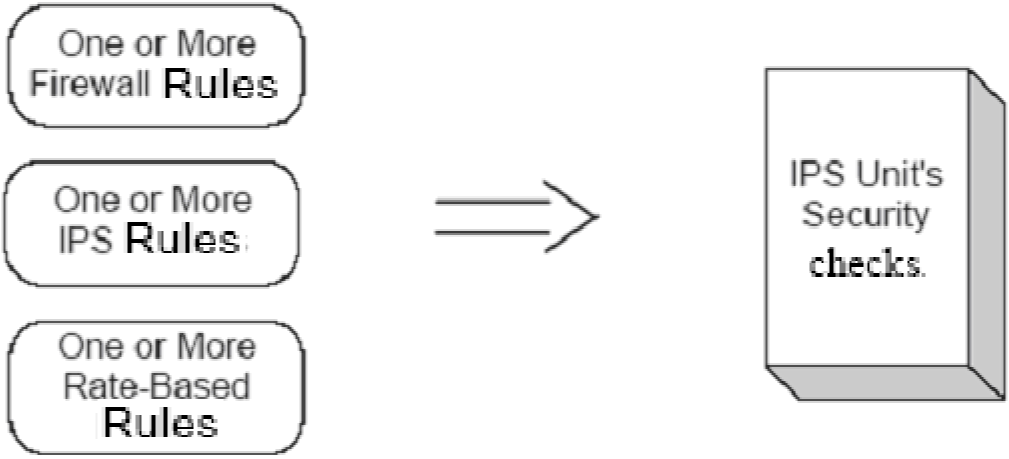
One or More Firewall Rules
One or More IPS Rules
One or More Rate-Based Rules
IPS Unit's Security checks.

Figure 1— IPS Unit's Security

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during February 2009. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 4 from the Common Methodology for Information Technology Security Evaluation, Version 2.3, [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap.ccevs.org. The Security Target (ST) is contained within the document "Top Layer Networks IPS 5500 E Security Target, Version .1.1", dated April 10, 2009.

2.0 Identification

Target of Evaluation: Top Layer Networks IPS 5500 E Version 5.21 software running on an IPS 5500 E series hardware platform.

The IPS 5500 series product line includes the following hardware models:

- IPS 5500-150E,
- IPS 5500-500E and
- IPS 5500-1000E

Evaluated Software: IPS 5500 E Version 5.21

Developer: Top Layer Networks, 2400 Computer Drive, Westboro, MA 01581

CCTL: CygnaCom Solutions
Suite 5200

7925 Jones Branch Drive
McLean, VA 22102

Evaluators: Sai Pulugurtha, Aruna Gandreti, Gary Grainger

Validation Scheme: National Information Assurance Partnership CCEVS

Validators: Franklin Haskell, Jean Hung, Brad O'Neill

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

CEM Identification: Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005

3.0 Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements. A description of the principle security policies is as follows:

3.1 Security Audit

During the process of receiving and transmitting traffic, the TOE performs many checks and other operations. Some of these operations, system events and user-related management interface tasks produce event messages. The IPS Unit contains a message managing system that makes these messages available based on the message controls established. These messages are collected as audit records in Alert logs and Event Log files. The TOE may also be configured to send messages to remote Syslog and SNMP servers. Only human users with authorized administrator or monitor privileges have the capability to view the audit data stored on the TOE.

3.2 User Data Protection

The TOE performs user data protection through the rate based security policy, the firewall filtering security policy and the intrusion prevention security policy. The TOE identifies external IT entities and remote administrator systems by their presumed IP addresses. Only legitimate external IT entities and authorized administrator systems are granted access to pass information through the TOE or to the TOE.

3.3 Identification and Authentication

The TOE provides a password based authentication mechanism to administrators and monitors.
The TOE communicates with the remote web browser of the administrator using the HTTPS protocol in order to encrypt the user id and password authentication data and all configuration information to maintain secrecy from an attacker. IT Entities are identified by their presumed IP addresses. Access to security functions and data is prohibited until a user is identified and authenticated.

3.4 Security Management

The TOE maintains administrator and monitor user management roles.

The TOE allows only authorized users with appropriate privileges to administer and manage the TOE. An administrative user can connect through an encrypted web interface using SSL for secrecy. Only authorized administrators may modify the TSF data related to the TSF, security attributes, and authentication data.

3.5 Protection of TOE Security Functions

The TOE transfers all the packets passing through the TOE only after processing the traffic based on the traffic attributes.

The TOE restricts management access to physically separate management interfaces and further by requiring users to log into the TOE using its GUI. HTTPS is used to protect the connection between the web browser in the IT Environment and the appliance. The TOE relies on Top Layer appliance hardware in general to ensure the TSP is enforced and to provide for domain separation. The TOE hardware appliance includes its own hardware clock, which provides reliable time stamps for use in audit and collected data records.

3.6 Trusted Path/Channels

The TOE, in conjunction with the IT environment, protects the TSF data from unauthorized disclosure or modification of TSF data when it is being transmitted between the IPS Unit and the management GUI on the remote management station.

A summary of the SFRs for the TOE and IT environment are included in the following tables. Note that _EXP in the SFR ID indicates explicitly specified requirements.

Table 1—TOE Security Functional Requirements

Item	SFR ID	SFR Title
1	FAU_GEN.1	Audit data generation
2	FAU_GEN.2	User identity association
3	FAU_SAA.1	Potential violation analysis
4	FAU_ARP.1	Security alarms
5	FAU_SAR.1	Audit review
6	FAU_SAR.3	Selectable Audit Review
7	FAU_SEL.1	Selective Audit
8	FAU_STG.1	Protected Audit Trail Storage

Item	SFR ID	SFR Title
9	FDP_IFC.1(1)	Subset information flow control (1)
10	FDP_IFF.1(1)	Simple security attributes (1)
11	FDP_IFC.1(2)	Subset information flow control (2)
12	FDP_IFF.1(2)	Simple security attributes (2)
13	FIA_AFL.1	Authentication failure handling
14	FIA_ATD.1	User attribute definition
15	FIA_UAU.1	Timing of Authentication
16	FIA_UAU.7	Protected authentication feedback
17	FIA_UID.2	User identification before any action
18	FMT_MOF.1	Management of security functions behaviour
19	FMT_MSA.3	Static attribute initialization
20	FMT_MSA.1	Management of security attributes
21	FMT_SMF.1	Specification of Management Functions
22	FMT_MTD.1	Management of TSF data
23	FMT_SMR.1	Security roles
24	FPT_TST.1	TSF Self-Testing
25	FPT_FLS.1	Failure with preservation of secure state
26	FPT_RVM_EXP.1	Partial Non-bypassability of the TSP
27	FPT_SEP_EXP.1	Partial TSF domain separation
28	FPT_STM_EXP.1	Reliable time stamps
29	FTP_TRP.1	Trusted Path

Table 2— Environment Security Functional Requirements

	Component	Component Name
1	FAU_STG_ENV.1	Partial protected audit trail storage
2	FIA_UAU_ENV.1	User Authentication before any action

	Component	Component Name
3	FIA_UID_ENV.1	User identification before any action
4	FPT_RVM_ENV.1	Partial non-bypassability of the TSP
5	FPT_SEP_ENV.1	Partial TSF domain separation
6	FPT_STM_ENV.1	Partial reliable time stamps

4.0 Assumptions and Clarification of Scope

4.1 Usage Assumptions

A.CONNECT The TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the external and internal networks without passing through the TOE.

A.BACKUP Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.

4.2 Personnel Assumptions

A.NOEVIL There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.AUTH It is assumed that administrators will protect their authentication data.

4.3 Environmental Assumptions

A.PHYSICAL The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 4 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The TOE depends on the IT environment partially to provide the capability to read the audit records, protect audit information, user identification and authentication before action, run a suite of tests, reliable time stamps, non-bypassability, and TSF domain separation.
5. The following features do not contribute to meeting any of the Security Functional Requirements (SFRs) and are not included in the TOE scope:
   - VLAN Support
   - Management of the IPS with an IPS Controller, Command Line Interface over Telnet and SNMP (Get function)
   - Usage of the TOE with other Top Layer supporting products (Network Security Analyzer, IPS Controller, TopResponse Software)

Note: The functionality/protocol used by the TopResponse product to automatically update signatures is included in the scope of the evaluation. The TSFI for this functionality is included in the scope of the evaluation, documented in the FSP and is verified during testing. Hence the capability of the TOE to download latest set of "TopLayer Protection Packs" is included in the Scope of the evaluation.

- Usage of Graphs, Reports and Statistics

The ST provides additional information on the assumptions made and the threats countered.

5.0 Architectural Information

The TOE architecture offers network-level and application-level protection along with the flexibility to integrate application-specific protection mechanisms. Top Layer's ASIC technology provides the high-performance base required for protecting against internet based and internal threats. The TOE provides stateful analysis firewall technology to provide network level protection, identifying undesired access, illegal packets, illegal headers, and various network attacks. Top Layer's denial-of-service protection algorithms are used by the TOE to protect against flood-based attacks, such as ICMP, UDP, and TCP SYN Floods.

The TOE uses a packet inspection chip set to provide application-level protection against exploits of critical vulnerabilities, including worms and application-level attacks.

The TOE is composed of the following logical subsystems:

- IP/ARP Bad Packet Filters
- L2 Filters
- DDos Filters
- Resource Limit Filters
- Stateful Analysis
- Firewall Filters
- Protocol Validation
- Content Inspection

Each subsystem performs a set of specific checks

These specific checks, or rules, and their associated actions, make up the subsystem's security policy. The IPS unit organizes the subsystems in a particular order so that traffic that is filtered by an earlier subsystem is never seen by the later subsystems. The various subsystems work together to provide the three-dimensional security protection

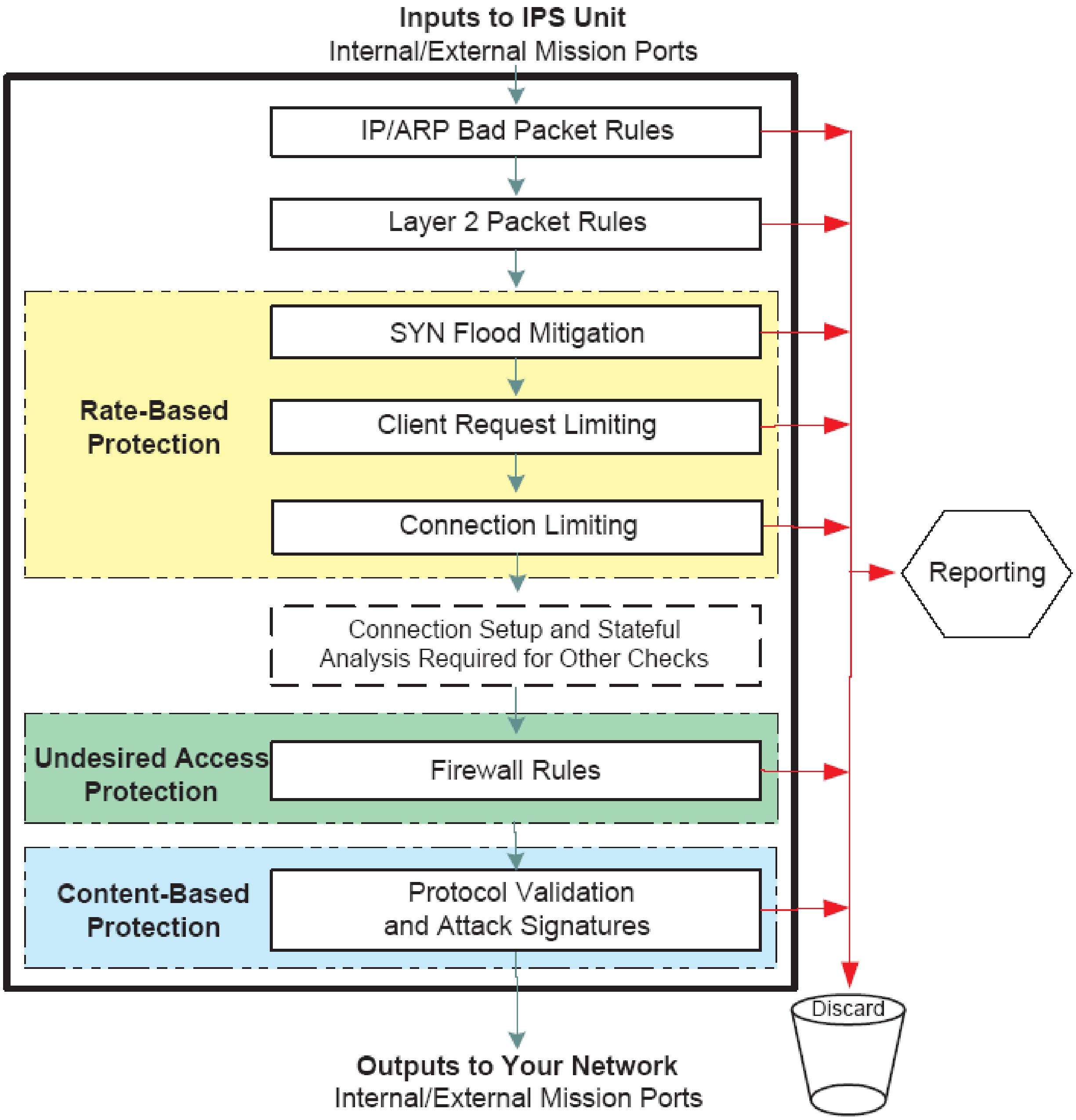

Figure 2—TOE Multi-Stage Architecture

The TOE depends on the IT Environment for the following security functions:

- Web browser – Used to access TOE administrative interfaces, including displaying alerts, reports, statistics, diagnostics and security logs
- SMTP, SNMP, Syslog servers – To receive audit events generated by the TOE
- NTP server – Used to set TOE hardware clock

The external IT entities send and receive network traffic through the TOE. Packet Capture Systems receive packets from Capture, Discard and Mirror Ports.

6.0 Documentation

CC Evaluation Evidence:

Note: An asterisk (*) indicates that the document is provided to the customers.

Table 3—Acronym and Document Title

Acronym	Document Title
FSP	IPS 5500 E-Series: Functional Specification For Common Criteria EAL4 Evaluation Version 1.2 14-November-2008
	Remote Management Protocol for Top Layer Applications April 3, 2008 Version 2.0
HLD, LLD	IPS 5500 E-Series:High Level Design Low Level Design For Common Criteria EAL4 Evaluation Version 1.6, 19-November-2008
TAT	IPS 5500 E-Series: Development Tools For Common Criteria EAL4 Evaluation Version 0.2 30-June-2008
LCD	IPS 5500 E-Series: Developer Life Cycle Model For Common Criteria EAL4 Evaluation Version 0.6 30-October-2008
COV_DPT	IPS 5500 E-Series: Test Coverage (ATE_COV.2) And Depth of Coverage (ATE_DPT.1) For Common Criteria EAL4 Evaluation Version 0.6 11-November-2008
TP	IPS 5500 E-Series: Test Plan For Common Criteria EAL4 Evaluation Version 1.0 14-November-2008
TE	Testing Evidence

Acronym	Document Title
TC	Test Procedures [TC] : IPS 5500 V5.21 -- Common Criteria Test Case Audit System Configuration and Audit Data Viewing IPS 5500 V5.21 -- Common Criteria Test Case Audit Event Triggers IPS 5500 V5.21 -- Common Criteria Test Case Installation and Abstract Machine Testing (Startup Testing) IPS 5500 V5.21 -- Common Criteria Test Case Software Configuration for Testing IPS 5500 V5.21 -- Common Criteria Test Case Domain Separation IPS 5500 V5.21 -- Common Criteria Test Case Firewall, Fragments, Midflows, and other IPS Checks IPS 5500 V5.21 -- Common Criteria Test Case Good Traffic does not Trigger Rules IPS 5500 V5.21 -- Common Criteria Test Case Management Controls IPS 5500 V5.21 -- Common Criteria Test Case Traffic Cannot Pass Until Checked IPS 5500 V5.21 -- Common Criteria Test Case Failure with Preservation of Secure State IPS 5500 V5.21 -- Common Criteria Test Case Protection Cluster IPS 5500 V5.21 -- Common Criteria Test Case Rate Based Security Features IPS 5500 V5.21 -- Common Criteria Test Case Reliable Time Stamp IPS 5500 V5.21 -- Common Criteria Test Case SNMP GET Operation Must Fail IPS 5500 V5.21 -- Common Criteria Test Case TOP Response Update IPS 5500 V5.21 -- Common Criteria Test Case Trusted Path
	Test_Coverage_Firewall + IPSAug.xls
	TestHarnessUserDocumentation.doc
MSU	IPS 5500 E-Series: Common Criteria Analysis Guidance For Common Criteria EAL4 Evaluation Version 0.4 20-October-2008
SOF	IPS 5500 E-Series: Strength of Function For Common Criteria EAL4 Evaluation Version 0.2 13-August-2008
VA	IPS 5500 E-Series: Vulnerability Analysis For Common Criteria EAL4 Evaluation Version 0.5 3-October-2008
ACM	IPS 5500 E-Series: Configuration Management For Common Criteria EAL4 Evaluation Version 0.8 14-August-2008
	IPS 5500 Software Build Process, Version 1.0 Issue Date:6-August-2005
	Software Release Process Version 1.6 19-June-2008

Acronym	Document Title
ADO	IPS 5500 E-Series: Delivery and Modification Detection For Common Criteria EAL4 Evaluation Version 0.7 18-November-2008
	IPS 5500 E-Series: Installation, Generation, and Start-up For Common Criteria EAL4 Evaluation Version 0.2 05-June-2008
AGD	IPS 5500 E-SERIES RELEASE NOTES, Software Version: Version V5.21.001, Date Oct 2008
	IPS 5500 E-Series: Administrator and User Guidance For Common Criteria EAL4 Evaluation Version 1.0 11-November-2008
	Top Layer 5000-Series Hardware Installation Part Number: 990-0183-07 Date: April 2008
	IPS 5500 and IPS 5500E Configuration and Management Part Number: 990-0188-09 Date: February 2008
	IPS5500-quick-protection.pdf
	MIB text file V1.6 January 24, 2005
	IPS Event logging system help
	IPS 5500 Online Help Files
DVS	IPS 5500 E-Series: Development Security Procedures For Common Criteria EAL4 Evaluation Version 0.6 13-August-2008

7.0 IT Product Testing

At EAL 4, the overall purpose of the testing activity is “to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests.” (ATE_IND.2, 14.9.5.1 [CEM])

At EAL 4, the developer’s test evidence must “demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.” (ATE_COV.2, 14.9.2.3)

This section describes the testing efforts of the vendor and the evaluation team.

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the evaluation team.

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the evaluation team.

The developer and evaluator independent and penetration testing was conducted at:

Top Layer Networks, 2400 Computer Drive, Westboro, MA 01581

The Independent testing was performed over a week period from 1/12/09–1/16/09. Installation Testing was performed the first day. Developer testing and Evaluator Testing was performed from 1/12/09–1/16/09. The test plan and results, as well as the evaluation team's review of the testing in the Evaluation Technical Report, were well written and complete.

7.1 Developer Testing

The test approach consists of manual and automated tests that were grouped together under the TOE IT Security Function and SFR being tested. The tests were designed to cover all of the security functions as described in the SFR and TSS section of the ST.

The test plan & procedures do not cover every possible combination of parameters for a given interface and every possible combination of parameters for a given security function. However, the test plan & procedures do stimulate every external interface and all of the security functions.

The individual tests were performed and the results were collected and verified by the developer. The results were archived, recorded, and sent to the evaluator for review.

The vendor's testing purposefully intended to cover all the security functions of Security Audit, User Data Protection, Identification and Authentication, Security Management, Protection of TOE Functions, and Trusted Path as defined in Section 6 of the ST.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL4 evaluation.

7.2 Evaluator Independent Testing

The test approach consists of providing full coverage of all the TOE's security functions between the developer tests and team-defined functional tests as required under EAL 4.

7.2.1 TEST HARDWARE

Top Layer Networks has provided the test setup for CygnaCom testing. The figure below shows logical connections. The test setup is intended to be consistent with the available Top Layer test facilities.

CygnaCom has tested both Basic (Single IPS unit) and Protection Cluster (High Availability) configurations. Evaluators ensured that all models (IPS 5500-150E, IPS 5500-500E, and IPS 5500-1000E) are tested.

The basic setup is as shown in the Figure below:

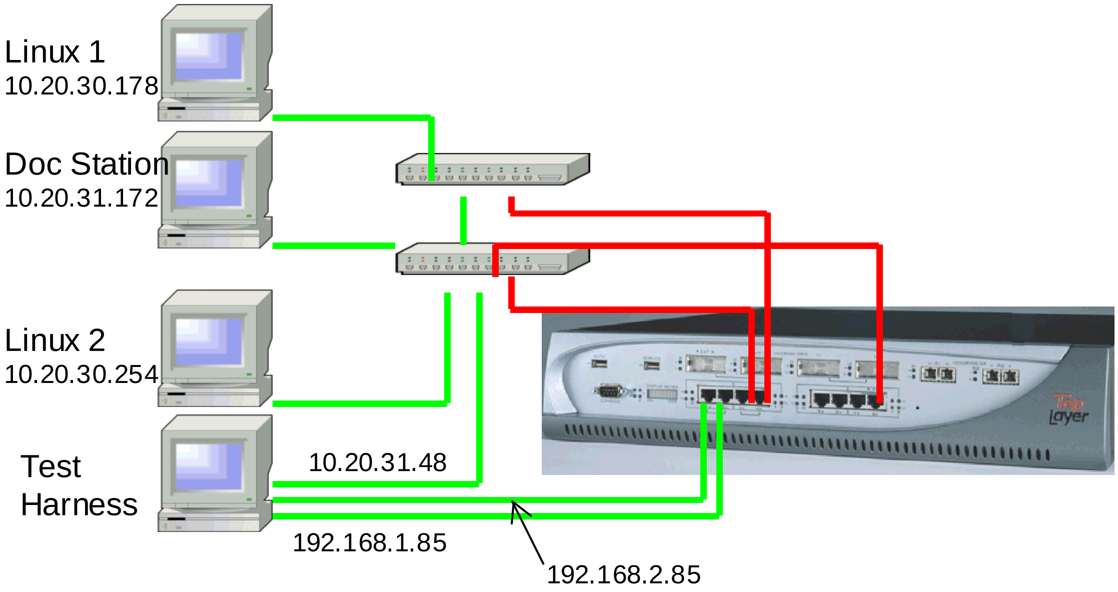

Figure 3- Test Configuration without Cluster

An out-of-the-box IPS 5500 E-Series unit issued by Top Layer to the Common Criteria testers (IPS5500-150E-CC)

- Documentation Kit (software CDs, HW manual, Quick Start Card, welcome letter)
- Power cord (type is based on country shipped to)
- Cable and Mounting Kit (mounting brackets with hardware, Console port cable, Ethernet cable-regular, Ethernet cable-crossover)

A preconfigured “Test Harness” Linux workstation used as follows:

- Three Network Interface Cards (10.20.31.48/16), (192.168.1.85), (192.168.2.85).
- Perform initial IPS 5500 E-Series setup via the IPS CONSOLE port and the workstation serial port.
- Access the IPS 5500 E-Series management GUI for TOE configuration and examination.
- Access the Top Layer Test Harness via the network to send targeted PCAP “bad” traffic through the TOE mission ports 1 and 2. The Top Layer Test Harness is a set of TK/TCL programs that uses a Top Layer RMP client CLI test program to configure the IPS 5500 E and tcpreplay to run PCAP’s through the IPS 55000 E. For each PCAP run through the test harness, it compares the rule fired to the expected rules fired for a given test. A single test case scripts can run many PCAP files and the test harness will print a result for each PCAP test executed.

- Two switches connecting different network segments.
- The document station must be at IP address 10.20.31.172/16.

- The document station having Wireshark version .99.6a or later installed.
- The Network in the diagram contains one FTP server, one HTTP server and a Linux box running Fedora Core 5, workstation at 10.20.30.254 on the 10.20.30.0/16 network. The Linux box at 10.20.30.254 contains the Neptune tool (included with test package).
- Two Fedora Core 5 (VM) machines, Linux 1 (10.20.30.178/16) and Linux 2 (10.20.30.254/16), with Neptune compiled on them. These machines are used for Rate Based testing and other manual tests. Both machines have SSH and Apache web servers running on them.

7.2.2 TEST SOFTWARE

The Linux station is supplied with the following CC test-related software:

Linux: version 2.6.22.14-72.fe6

Syslog server: version sysklogd 1.4.1, with remote syslog daemon configured.

Mozilla web browser

Putty (terminal emulator): version 0.60
Special Configuration: A Saved Session with TOE access configuration matching the terminal setup in the *Top Layer 5000-Series Hardware Installation* [INSTALL] guide.

Java Realtime Engine (JRE): version 1.6.0_06

Java Development Kit (JDK): version JDK 1.6.0_07

AdventNet SNMP API: version 4.0 STD

TCP Replay (packet capture and replay utility): version 3.2.0

Top Layer Test Harness version (manage test traffic and record IPS results) version 1.0

The Client Workstation is supplied with the following CC test-related software:

Wireshark Version .99.6a

Neptune tool

All tools are available at Top Layer facility and are used for Developer tests.

7.3 Strategy for Devising Test Subset

CygnaCom has selected approximately (at least) 90% of the tests Top Layer provided as evaluation evidence. The tests were selected to exercise security functions from the externally visible TSFI.

The evaluator ensured that the test sample included the tests such that:

- All Security Functions are tested

- All interfaces are exercised
- All Security Functional Requirements are tested.

Since the product is an Intrusion Protection System emphasis was on Security Management (SM), Identification and Authentication functionality (I & A) and Information Flow Control/Security attributes (FDP_IFC/IFF). The test provided by the developer and the test sample of the developer tests selected tested security functions at appropriate level of rigor.

CygnaCom's independent tests augment and supplement the tests Top Layer provided as evaluation evidence. Again, the emphasis is on the TOE interfaces. The independent tests are and described in detail in the Test Report and ETR.

7.4 Coverage Provided by Devised Test Subset

The evaluator ensured that the test sample included the tests such that:

- All Security Functions are tested
- All interfaces are exercised
- All Security Functional Requirements are tested.
- More emphasis is laid on the Network Interface being tested.
- All security relevant features mentioned in the Administration/User Guides are covered in testing.
- Functional Specification references to the FW + IPS Rules are covered.
- Since the product is primarily a network gateway product providing advanced Intrusion Prevention functionality at the perimeter, it is difficult to gauge the extent of coverage for the network interfaces. Evaluators work with Developer Top Layer based on the guidance provided by the Validator during the evaluation of the FSP to determine the complete extent of coverage.

In testing the functionality of the network interface through which the FDP_IFC*/FDP_IFF* requirements are tested, Top Layer used their proprietary test harness to devise and run tests using Hundreds of PCAP (Packet Capture files) and respective cache files. During the process several tools like TCP replay and Neptune are used. For broad requirements where it pertains to testing signatures, worms, viruses, rules etc. Top Layer has tested them using several PCAP files.

The penetration tests cover hypothesized vulnerabilities and potential misuse of guidance. The list hypothesized vulnerabilities was developed based on Top Layer's vulnerability assessment and analysis of evaluation evidence. The tests for potential misuse of guidance cover installing the TOE from guidance documentation and sampling administrator procedures.

8.0 Evaluated Configuration

The Evaluated Configuration (consistent with the ST):

- IPS5500-1000E (Software Version 5.21)

The Management Workstation: Linux version 2.6.22.14-72.fe6, Syslog server: version sysklogd 1.4.1 with remote syslog daemon configured, Mozilla web browser, Putty (terminal emulator): version 0.60, Java Realtime Engine (JRE): version 1.6.0_06, Java Development Kit (JDK): version JDK 1.6.0_07, AdventNet SNMP API: version 4.0 STD, TCP Replay (packet capture and replay utility): version 3.2.0, Top Layer Test Harness version (manage test traffic and record IPS results) version 1.0

- The Client Workstation: Windows XP Service Pack 3, Intel platform, hard disk and removable storage components and device drivers, Wireshark version .99.6a
- NTP Server
- SNMP Server
- Syslog Server
- Two Fedora Core 5 (VM) machines, Linux 1 (10.20.30.178/16) and Linux 2 (10.20.30.254/16), with Neptune compiled on them and running SSH and Apache Web servers. (These machines used for Rate Based testing and other manual tests).

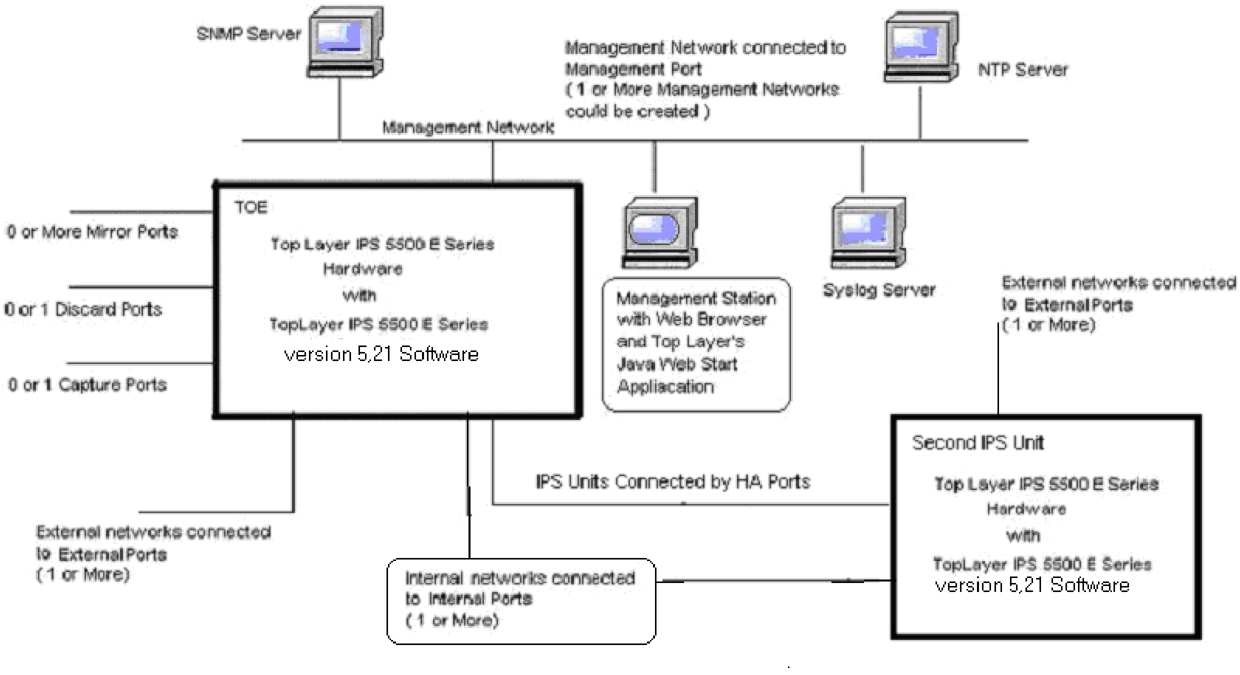
SNMP Server
Management Network connected to Management Port
(1 or More Management Networks could be created)
NTP Server
Management Network
0 or More Mirror Ports
0 or 1 Discard Ports
0 or 1 Capture Ports
TOE
Top Layer IPS 5500 E Series Hardware with TopLayer IPS 5500 E Series version 5.21 Software
Management Station with Web Browser and Top Layer's Java Web Start Appliacation
Syslog Server
External networks connected to External Ports (1 or More)
Second IPS Unit
Top Layer IPS 5500 E Series Hardware with TopLayer IPS 5500 E Series version 5.21 Software
IPS Units Connected by HA Ports
External networks connected to External Ports (1 or More)
Internal networks connected to Internal Ports (1 or More)

Figure 4- Evaluated Configuration (with High Availability) from ST

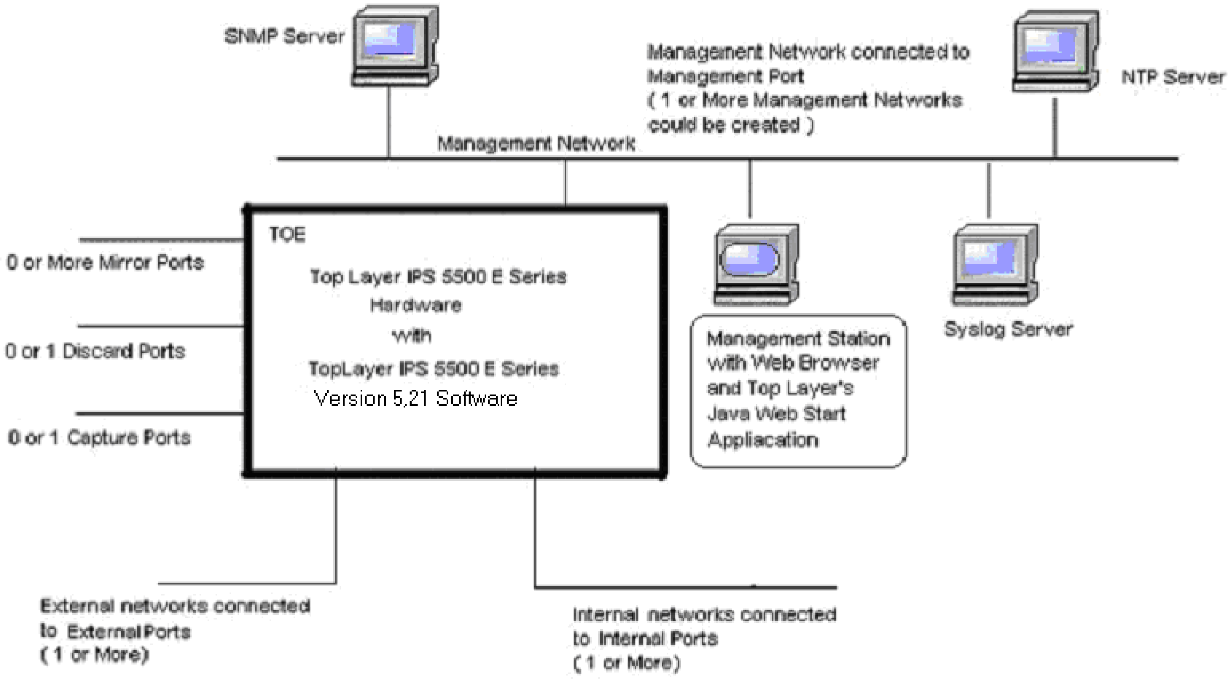
SNMP Server
Management Network connected to Management Port (1 or More Management Networks could be created)
NTP Server
Management Network
TOE
Top Layer IPS 5500 E Series Hardware with TopLayer IPS 5500 E Series Version 5.21 Software
0 or More Mirror Ports
0 or 1 Discard Ports
0 or 1 Capture Ports
Management Station with Web Browser and Top Layer's Java Web Start Appliacation
Syslog Server
External networks connected to External Ports (1 or More)
Internal networks connected to Internal Ports (1 or More)

Figure 5- Evaluated Configuration (without High Availability) from ST

Note: Though the above-evaluated configuration shows distinct machines for different servers (Syslog, SNMP) etc. the evaluator worked with the existing setup at Top Layer to put the TOE in the evaluated configuration. The evaluator ensured that the test setup at Top Layer is logically equivalent to the one shown in the above figure. Similarly when installing the TOE in protection Cluster Configuration, the evaluator ensured that the configuration used in the Test configuration are logically equivalent to the one in the security Target. Also, the evaluator covered all the Hardware models in the testing process.

9.0 Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE will meet to be evaluated at Evaluation Assurance Level 4. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted. These components are included by reference only as there are no parameters to be assigned; the body can be found in CC part 3.

ACM_AUT.1	Partial CM Automation
ACM_CAP.4	Generation Support and Acceptance Procedures
ACM_SCP.2	Problem Tracking CM Coverage
ADO_DEL.2	Detection of Modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of Security Measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing—sample
AVA_MSU.2	Validation of Analysis
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.2	Independent vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. During application of the AVA_VLA.2 CEM work units the evaluators found no residual vulnerabilities in the product. The evaluation team reached pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

The TOE is CC Part 2 Extended

The TOE is CC Part 3 Conformant for EAL4.

Strength of Function Rating of SOF-medium

10.0 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

11.0 Security Target

The Security Target is identified as Top Layer Networks IPS 5500 E Security Target, Version 1.1, dated April 10, 2009.

12.0 List of Acronyms

The acronyms used within this document:

Table 4—Acronym and Document Title

Acronym	Definition
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
ASIC	Application-Specific Integrated Circuit
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
FAU	Security Audit
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTP	Trusted Path/Channels
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
ICMP	Internet Control Message Protocol

Acronym	Definition
ID	Identifier
IP	Internet Protocol
IPS	Intrusion Protection System
IT	Information Technology
LAN	Local Area Network
OS	Operating System
SF	Security Function
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SFP	Security Function Policy
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification

13.0 Bibliography

URLs

Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

CygnaCom Solutions CCTL (http://www.cygnacom.com).

TopLayer Networks (http://www.toplayer.com/).

The validation team used the following documents to produce this Validation Report:

Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, Part 1

Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, Part 2

Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, Part 3

Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.

Top Layer Networks IPS 5500 E Security Target, Version 1.1, April 10, 2009

Evaluation Technical Report for a Target of Evaluation, IPS 5500 E Version 5.21, Volume 1

Evaluation Technical Report for a Target of Evaluation, IPS 5500 E Version 5.21, Volume 2

Evaluation Team Test Plan of Top Layer Networks IPS 5500 E Version 0.1