Top Layer Networks IPS 5500 E Security Target

Version 1.1

April 10, 2009

Prepared For:

Top Layer Networks
2400 Computer Drive
Westborough, MA 01581

Prepared By:

CygnaCom Solutions
Security Evaluations Laboratory
7925 Jones Branch Drive, Suite 5200
Mclean, VA 22031

© 2007 Top Layer Networks. All Rights Reserved.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:	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
ST Identification:	Top Layer Networks IPS 5500 E Security Target
ST Version:	1.1
ST Publish Date:	April 10, 2009
ST Authors:	CygnaCom Solutions
PP Identification:	None

1.2 CC Conformance Claim

The TOE is Common Criteria (CC) Version 2.3[1] Part 2 extended.

The TOE is Common Criteria (CC) Version 2.3 Part 3 conformant and meets the requirements of Evaluation Assurance Level (EAL) 4.

There are no applicable International (CCIMB) interpretations for CC Version 2.3 as of 12/21/2008.

This TOE is not conformant to any Protection Profiles (PPs).

1.3 Overview

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. It is a hardware-based, multi-processor system that has an onboard application level stateful firewall that works in conjunction with the Intrusion Prevention subsystems to provide security. The IPS 5500 provides a 3-Dimensional approach to secure networks of interest to:

- Stop Resource Abuse

[1] Common Criteria (CC) for Information Technology Security Evaluation – August 2005, Version 2.3, CCMB-2005-08-001.

- Prohibit Access to Unauthorized Clients
- Stop Malicious Content

The IPS Unit supports a number of management interfaces to manage it both locally and using a remote system. It provides logging of various security events.

1.4 Organization

Table 1-1: ST Organization and Description

Section	Title	Description
1	Introduction	Provides an overview of the Security Target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.
7	PP Claims	Protection Profile Conformance Claims
8	Rationale	Contains pointers to the rationales contained throughout the document.

1.5 Document Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. All of the components in this ST are taken directly from Part 2 of the CC except the ones noted with "_EXP" in the component name. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1 as:

Iteration:	allows a component to be used more than once with varying operations;
Assignment:	allows the specification of parameters;
Selection:	allows the specification of one or more items from a list; and
Refinement:	allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

Iterations are identified with a number in brackets "(#)" right after the short name.

Assignments and Selections specified by the ST author are in [***italicized bold text***].

Refinements to the CC text are specified **bold and underlined text**.

Explicitly Stated TOE Security Functional Requirements are specified with a "_EXP" added to the component name.

IT Environment Requirements are specified with a "_ENV" added to the component name.

Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *Application Note: italicized text.*

CCIMB Interpretations have been reviewed. The original CC text modified by the interpretation is neither denoted nor explained.

1.6 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.6.1 ST Specific Terminology

- **External IT entity** -- Any IT product or system, untrusted or trusted, outside of the TOE, that interacts with the TOE.
- **Identity** -- A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
- **Authentication data** -- Information used to verify the claimed identity of a user.
- **Authorized Administrator** - An administrator who has been identified and authenticated by the TOE and has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given to them.
- **Service -** A service is a policy element that identifies a protocol or set of protocols to the IPS Unit, for example, HTTP, DNS, or FTP.
- **Rules -** The IPS Unit contains hundreds of rules that it uses to check whether a given flow of traffic is acceptable or not. A rule may be based on packet checks (for example, Illegal ICMP Header) or protocol checks (for example, HTTP Unknown Method Name).
- **Actions -** An action is a response by the IPS Unit when traffic triggers a security rule. The IPS Unit can take one of the following actions when traffic triggers a rule:
  Allow — The IPS Unit passes the traffic.
  Drop — The IPS Unit discards the traffic.
  Reject — The IPS Unit discards the traffic and sends TCP reset to the connection source.
- **Client (Client Group)** -An IT entity (group of IT Entities) that is the source of an information flow.
- **Server (Server Group)** – An IT entity (group of IT Entities) to which an information flow is destined.

- **Host Groups (Client and Servers)** - A host group is a named set of IP address ranges. A host group can define a group of clients or a group of servers. A given host group may act as both clients and servers.
- **Connection Limits** — Limits the number of simultaneous connections allowed for a group of clients or a group of servers, and for individual members of the group.
- **Request Limits —** Limits the number of requests a client within a host group can make per minute for specified services**.**
- **SYN Flood Limits** — Provides limits for the number of incomplete SYN requests for servers and for various categories of clients (trusted, suspicious, malicious, etc.).
- **IP Address**--Internet Protocol Address, a 32-bit numeric identifier for a computer or a device on the network. The TOE does not support IPv6 packets.
- **Segments –** A pair of physical ports that handle internal and external network traffic (mission ports) is called a Segment. When configured to do so, the IPS Unit forwards all packets received on either of the ports in the pair to the other port in the pair, subject to the defined security policy filtering
- **Threat** - Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
- **Threat Agent** - Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.
- **TOE Security Function (TSF) Data** - Information used by the TSF in making TOE security policy (TSP) decisions. TSF data may be influenced by users if allowed by the TSP. Security attributes, authentication data and information flow control policy's subject and object security attributes are examples of TSF data.
- **Audit Data** - The logs generated based on the actions of the TOE itself. This includes the authentication of users accessing the TOE, actions taken directly on the TOE, and actions of the TOE itself. Audit data is a type of TSF data.
- **User** - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
- **User Data** - Data created by external IT entities that does not affect the operation of the TSP. User data is separate from the TSF data. The information flows created by Clients and Servers is an example of user Data.
- **VPN**-Virtual Private Network, a network constructed using public wires to connect nodes. For example, there are a number of systems that enable the administrator to create networks using the Internet as the medium for transporting data; these systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted
- **Vulnerability -** A weakness that can be exploited to violate the TOE security policy.
- **Protocol Validation** - Examining the payload of application datagrams and application streams for specific network protocols (DNS, FTP, HTTP, MSNET, SIP, SSH and Telnet) to ensure that the traffic conforms to the rules for a given protocol as well as the IPS Unit's rules for reasonable usage. The protocol validation rules are specific to the Top Layer IPS. These rules enable configuration of protocol specific parameters for application protocols to stop attackers who abuse weaknesses in a protocol's defined structure.

- **Content Inspection** - Checks for deliberate inclusion of malicious data or other malicious payloads into traffic that is otherwise well formed.
- **Attack Signatures** - An attack signature is a defined arrangement of information that can be used to identify an attacker's attempt to exploit a known vulnerability.
- **Firewall Rules** — Rules to provide classic firewall blocking for traffic, based on IP addresses, Layer 4 ports and segments (port pairs).
- **IPS Rules** — Rules to provide the following types of checks:
    - Protocol validation
    - Attack Signatures
    - Acceptable use of network application
- **Rate Based Rules** — Rules to protect your resources from overuse by legitimate users, as well as abusive denial-of-service attackers.
- **Bypass**- The IPS Unit provides a software-based bypass feature between Mission port-pairs. There are three modes of bypass control.
    - Never Bypass - The IPS Unit inspects all traffic, mitigates problem traffic, and records all information. All traffic flows through the IPS Unit’s functions.
    - Always Bypass - The IPS Unit inspects all traffic and records traffic statistics, but does not mitigate. All traffic always passes through the IPS Unit.
    - Bypass During System Reset - The IPS Unit starts out performing as in Never Bypass mode, checking and mitigating all traffic, but performs as Always Bypass mode (passes all traffic) if there is a software failure and the IPS Unit needs to reboot.

1.6.2 Acronyms

The acronyms used within this Security Target:

Table 1-2 Acronyms

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]
CIFS	Common Internet File System
DNS	Domain Name System
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

Acronym	Definition
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
ICMP	Internet Control Message Protocol
ID	Identifier
IP	Internet Protocol
IPS	Intrusion Protection System
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MSNET	Microsoft NETworks
NIC	Network Interface Card
OS	Operating System
SF	Security Function
SIP	Session Initiation Protocol
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
UDP	User Datagram Protocol
VPN	Virtual Private Network

2 TOE Description

2.1 TOE Overview

The TOE is an IPS 5500 E Hardware appliance with Version 5.21 software. The IPS Unit is managed using a Graphical User Interface (GUI), which is a Java Web Start™ application that runs as a stand-alone application on the Management Station. The Java Web Start application is also included in the TOE. 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 the 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 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

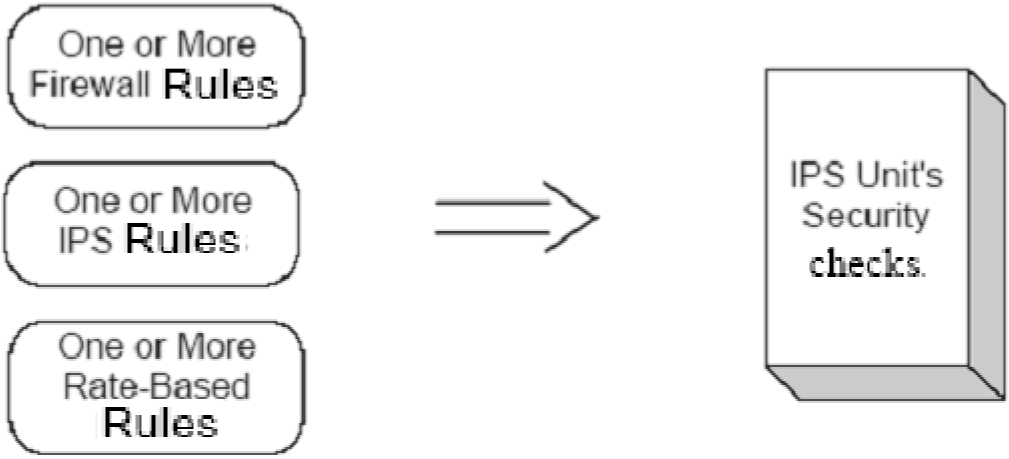
One or More Firewall Rules
One or More IPS Rules
One or More Rate-Based Rules
IPS Unit's Security checks

Figure 2-1 IPS Unit's Security

2.1.1 Categories of Deployment

The figures in this section provide general guidelines to a prospective customer for placing an IPS Unit in their networks.

To install and deploy the TOE in a secure evaluated configuration please see section 2.3.2 Evaluated Configuration. Also, please see section 2.3.3 Security Functionality in the IT Environment for a description of the security functionality provided by the IT Environment.

The IPS Unit can be deployed in the following ways in a prospective customer's network:

Network Perimeter Protection

Increases protection against targeted DDoS attacks and application level threats. Protects the network from cyber-threats that may traverse the VPN link.

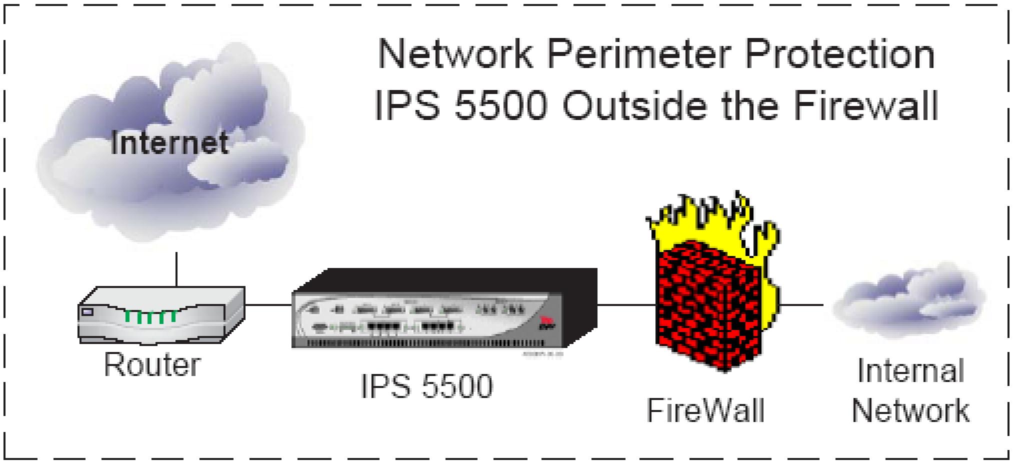

Figure 2-2 Network Perimeter Protection

Hosting Center Protection

Protects assets from network and application level threats regardless of whether they originate from inside or outside. The IPS unit when deployed this way could be used to protect servers in a dedicated manner.

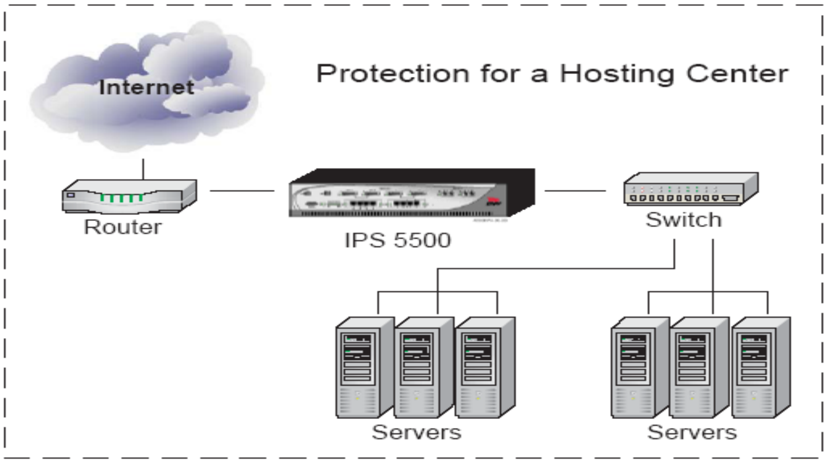

Figure 2-3 Protection for a Hosting Center

Critical Online Assets Protection

Protects network segments from threats and provides containment of infected segments. When IPS units are deployed between internal network segments, they can be configured with network segment specific policies, which provide better performance. This configuration can also keep infected segments separate from uninfected segments.

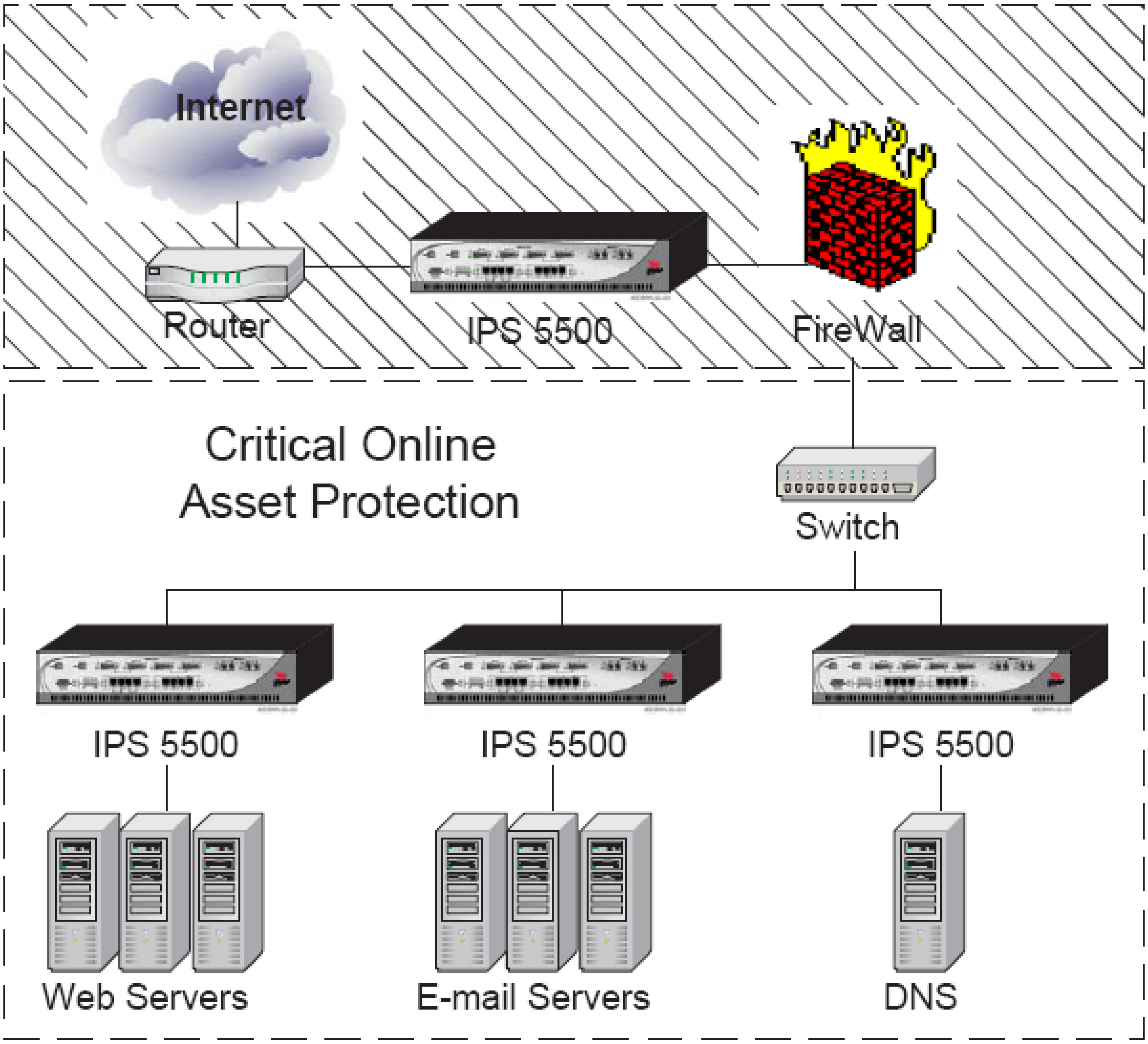

Figure 2-4 Protect Critical Online Assets

High Volume Configuration Single Inline with Peer

Provides additional, shared processing for high volume environments. In the Single Inline with Peer configuration, only one IPS Unit passes network traffic, but the second IPS Unit assists in detection processing and flow setup operations, increasing the traffic load that the IPS Units can handle and almost doubling the number of connections that can be created and analyzed.

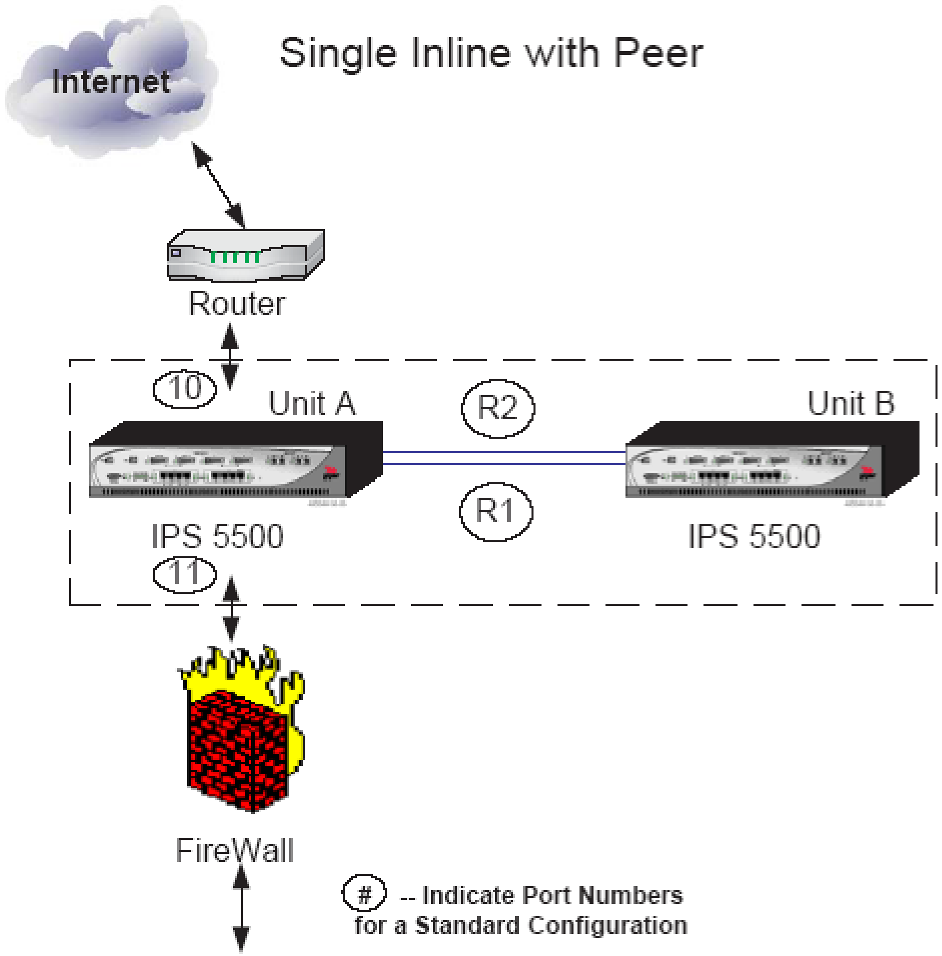

Figure 2-5 High Volume Single Inline with Peer

ProtectionCluster Configuration

Provides active redundancy to the current configuration. ProtectionCluster refers to a network configuration option that provides higher bandwidth and redundancy. This configuration connects multiple IPS Units together using a special pair of GbE links. These links, called R1 and R2, provide higher bandwidth for flow rebalancing in redundant configurations. A ProtectionCluster configuration also enables the IPS Units to share the intense processing required for deep and stateful protocol analysis necessary to detect attempted exploits of application-level vulnerabilities in both server and client groups. In this configuration, both sides of the configuration receive and pass the network traffic, unless there is a failure. This solution provides a redundant solution that offers maximum protection of the network resources. This solution, using a combination of IPS Units, protects up to two full duplex Gigabit input ports: stopping the "bad" traffic, while permitting the “good” traffic to pass to its destination.

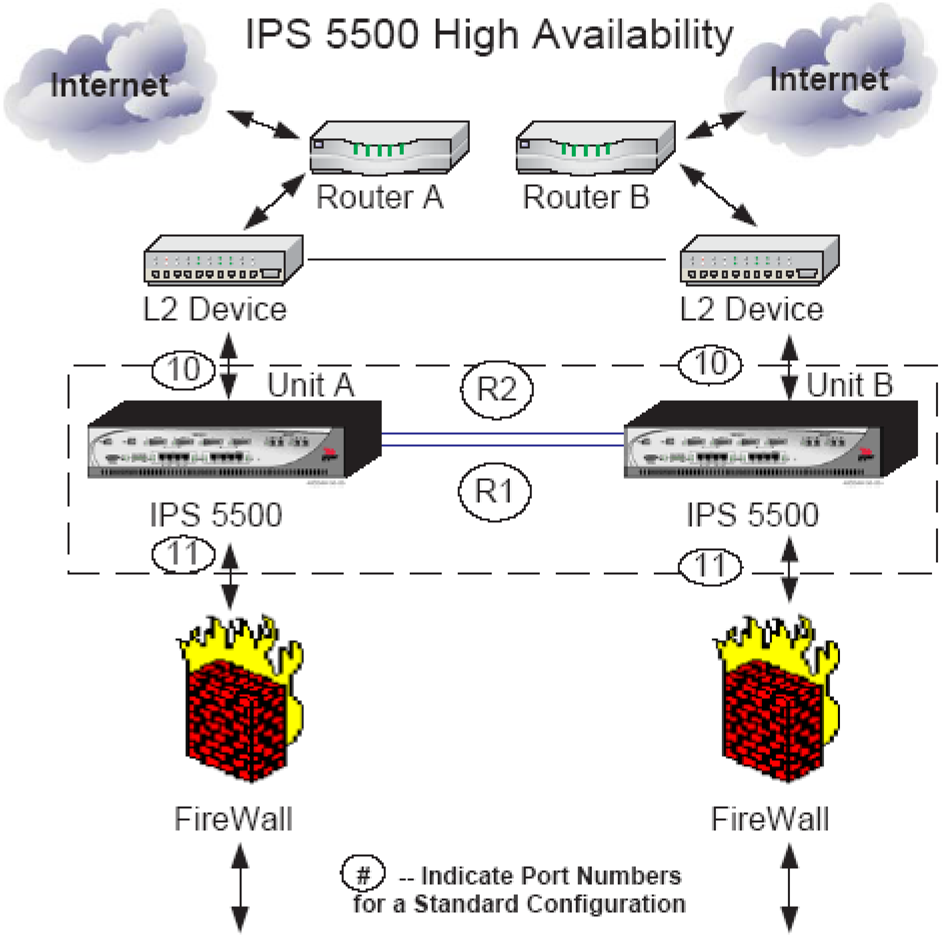

Figure 2-6 Two Unit Protection Cluster

2.2 Architecture Description

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

The figure below depicts the TOE as a device with multiple stages of security filtering performed by the subsystems mentioned above.

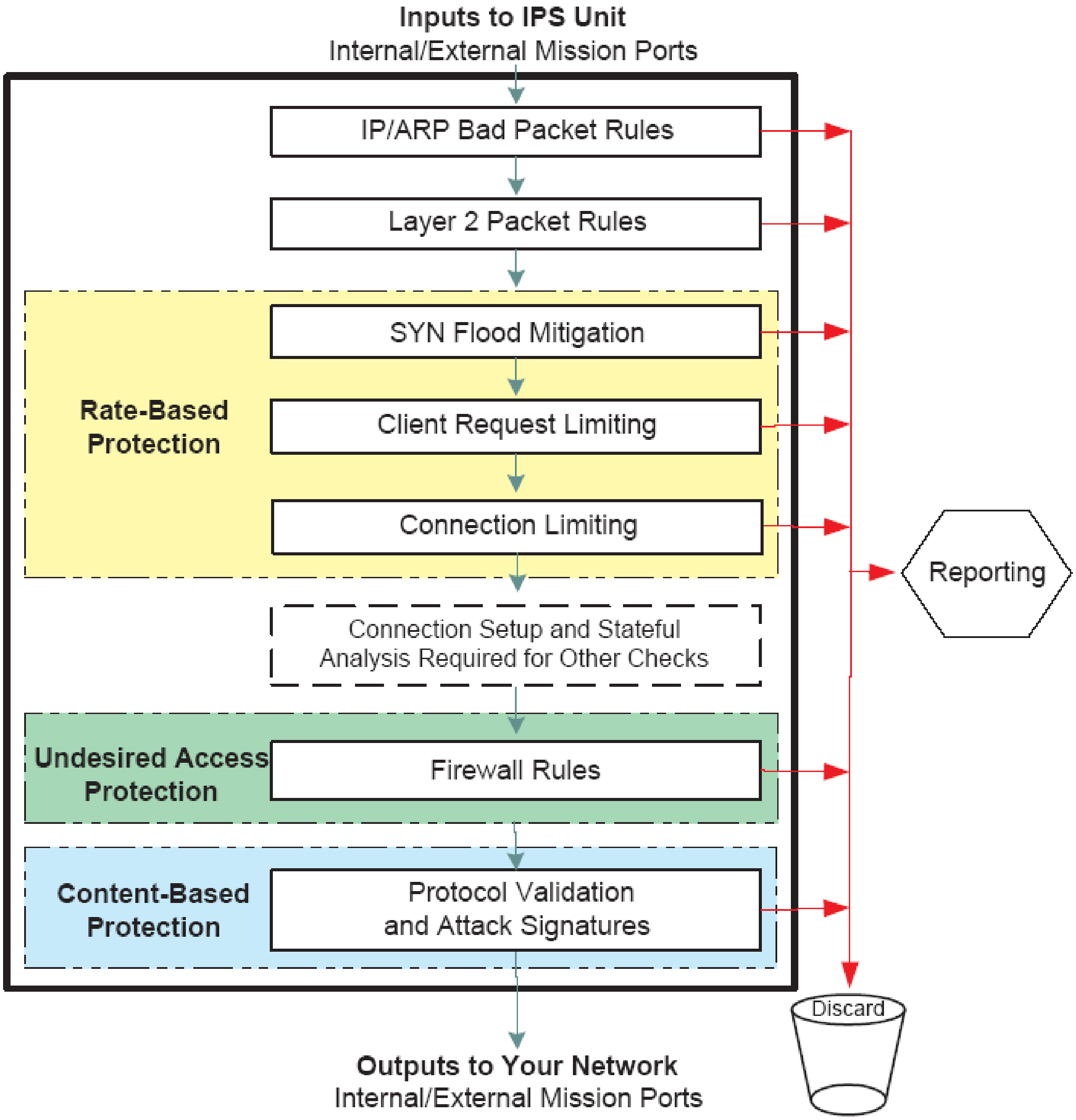

Figure 2-7 TOE Multi- Stage Architecture

2.3 Physical Boundaries

The physical boundary of the TOE is the IPS 5500 E Hardware appliance (150 E, 500 E or 1000 E) loaded with the IPS Software Version 5.21.

2.3.1 Physical Interfaces

The TOE has the following physical interfaces:

- Console port using a 9-pin D-sub connector
- 10BASE-T/100BASE-TX copper LAN ports,
- 1000BASE-T Copper ports
- 1000BASE-SX fiber optic HA

Please see the table below for more details on the hardware models:

Table 2-1 Hardware Models

Model	CPU	Ports	Memory	NIC Chipsets Used		Power Supply
150 E, 500E and 1000E	The TOE utilizes multiple CPU's. - 5 Top Layer proprietary ASIC chips running at 100 MHz - 1 AMD 520 chip running at 100 MHz - 2 Freescale PowerPC chips running at 825 MHz	Total Number of NIC Ports: 12 Total Number of Serial Ports: 1 Total number of HA Ports: 2	There is no hard drive in the TOE. It does utilize a 256 Meg compact flash card.	10/100	A combination of a Top Layer proprietary ASIC MAC chip and Marvell transceiver chip (Marvell part number 88E3082-BAR)	1 or 2
				1000 (Port Numbers 9 to 12)	A combination of a Top Layer proprietary ASIC MAC chip and HP IC SerDes Gigabit chip (HP part number HDMP-1646A)	
				1000 (R1 and R2)	A combination of a Top Layer proprietary ASIC MAC chip and Marvell IC Gigabit quad Phy SerDes chip (Marvell part number 88E1043-D2-BCA-C000)	

Each hardware model has 12 physical ports numbered 1 to 12 and two high availability ports numbered R1 and R2. Most of the ports on the IPS Unit can have several possible roles. A port can only be configured for one role at any given time and some ports have fixed roles.

In addition to port roles, the IPS unit supports the concept of Mission, Management, and Maintenance ports to further classify ports based on their role type.

Mission ports are ports that handle internal and external network traffic. Two matched ports, one with the role Internal and another port with the role External, are known as a Mission port-pair.

Management ports on the IPS unit are ports used to manage the IPS unit itself. By default, Port 8 on the IPS Unit is always configured to be a Management access port. All configured Management ports are bridged together and flooding occurs between these ports. An internal bridge logically connects Management ports. Packets received on Management ports are bridged to other Management ports. Packets received on Mission ports can be bridged to other Mission ports, but will never be forwarded to any Management port or to the management entity (e.g. management station).

Maintenance ports are ports on the IPS unit that are used to manage events and mirror traffic on the IPS unit. These ports can have the role of Capture, Mirror, or Discard. Traffic on maintenance ports is handled using the Management Bridge.

The IPS Unit uses these roles and port types to determine how traffic passes through the IPS Unit. The table below presents details of Roles, Port Types and traffic isolation.

Table 2-2 Port Types

Role	Port Type	Traffic Isolation Handled by
Internal or External	Mission Port	Mission Bridge
Management	Management Port	Management Bridge
Capture, Mirror, Discard	Maintenance	Management Bridge
High Availability	HA Port	Not Applicable

The table below presents details of each port speed, possible roles, and the default role for each Port on the hardware models. Please note that the Port # in the first column in the table below represents the physical port number and not the number of ports.

Table 2-3 Port Information

Port #	Speed	Possible Roles	Default Role IPS 5500-150 IPS 5500-500 IPS 5500-1000
1	10/100	External, Mirror, Unused	External
2	10/100	Internal, Mirror, Unused	Internal
3	10/100	External, Mirror, Capture,	Capture

Port #	**Speed**	**Possible Roles**	**Default Role** **IPS 5500-150** **IPS 5500-500** **IPS 5500-1000**
		Unused	
4	10/100	Internal, Mirror, Capture, Discard, Unused	Discard
5	10/100	Management, Mirror, Capture, Discard, Unused	Unused
6	10/100	Management, Mirror, Capture, Discard, Unused	Unused
7	10/100	Management, Capture, Discard, Unused	Unused
8	10/100	Management	Management
9	1000	External Unused	External
10	1000	Internal Unused	Internal
11	1000	External, Capture, Unused	Unused
12	1000	Internal, Capture, Unused	Unused
R1	1000	HA	HA
R2	1000	HA	HA

The following table explains the port roles. Please note that the # of Ports in the second column represents the number of ports, not the physical port number.

Table 2-4 Port Roles

Port Role	**# of Ports that can have this Role**	**Operating Speed**	**Description**
Management	1,2,3,or 4	10/100	Use a port with the port role Management to manage the IPS Unit and as an output port for reporting traffic (using standard Syslog and SNMP traps).
Mirror	0,1,2,3,4,5, or 6	10/100	Identify one or more Mirror ports to create a mirror (copy) group. The IPS Unit copies all packets from specific traffic applications to the ports in the mirror group. It uses the Round Robin algorithm to balance traffic among the Mirror ports. All ports in the mirror group must be set to the same speed. No packets are received on a port with this role.
Discard	0 or 1	10/100	Use a port with the role Discard to send the dropped packets that caused events to a collecting system in the environment. Configure which packets go through the Discard port to the collecting system in the environment by configuring Policies
Capture	0 or 1	10/100/1000	Use a port with the role Capture as a single, mirroring output port. One of the Mission ports can be chosen to have all of its received and transmitted packets mirrored to this port.
External (Outside)	1,2,3, or 4	10/100/1000	Use a port with the role External to connect to the external network. The External port does not allow management access. The External port receives packets and forwards them (subject to policy checks) to its paired Internal port (known as Port-pair forwarding mode),
Internal (Inside)	1,2,3, or 4	10/100/1000	Use a port with the role Internal to connect to the internal network. The Internal port does not allow management access. The Internal port receives packets and, either forwards them (subject to policy checks) to its paired External port (known as Port-pair forwarding mode), or bridges them according to their destination MAC addresses.
High Availability	0,1, or 2	1000	Use a port with the role High Availability (HA) as a Gigabit port that is directly connected to a redundant IPS Unit. The HA port is used to balance traffic between redundant IPS Units.
Unused	Not Applicable	10/100/1000	A port with the role Unused is a port that is not configured. The Unused port does not accept traffic nor send any traffic. The IPS Unit will not recognize a link to this port.

2.3.2 Evaluated Configuration

Figure 2-8 Evaluated Configuration below depicts the TOE in the evaluated configuration.

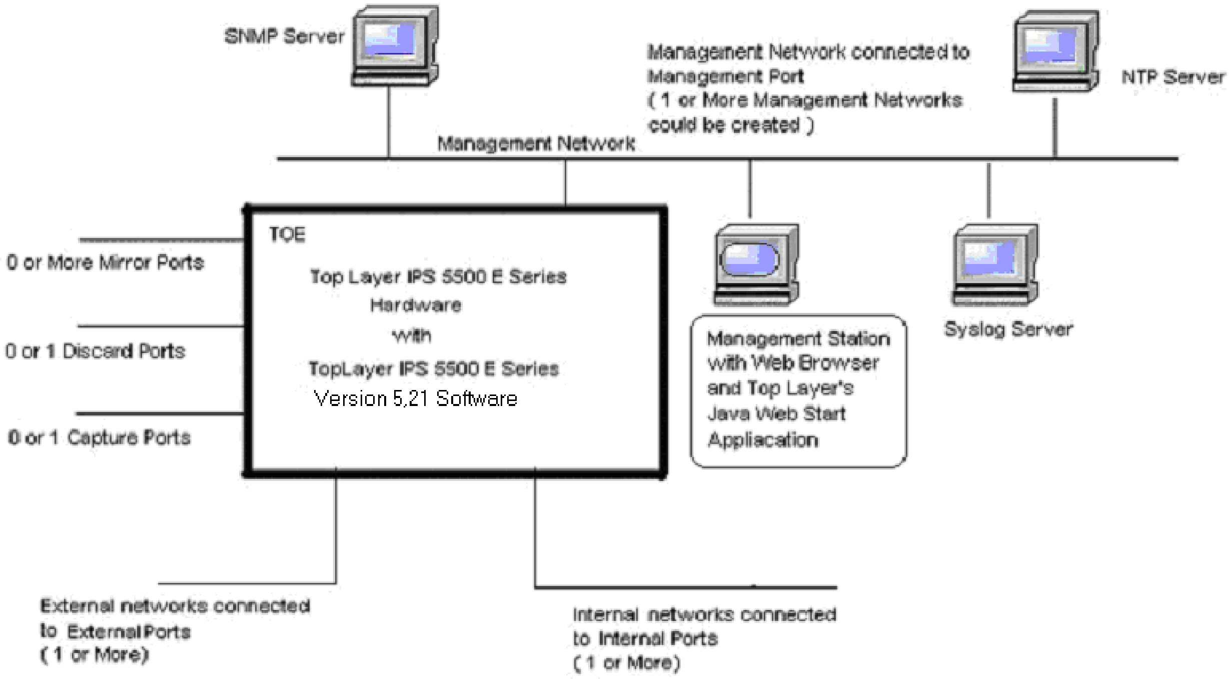
SNMP Server
Management Network connected to Management Port
(1 or More Management Networks could be created)
NTP Server
Management Network
TOE
Top Layer IPS 5500 E Series Hardware with TopLayer IPS 5500 E Series Version 5.21 Software
0 or More Mirror Ports
0 or 1 Discard Ports
0 or 1 Capture Ports
Management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

Figure 2-8 Evaluated Configuration

The IPS Unit is managed using a Graphical User Interface (GUI), which is a Java Web Start™ application that runs as a stand-alone application on the Management Station. The Java Web Start application is also included in the TOE.

In addition to the evaluated configuration shown above where a single IPS unit is used between networks, an additional configuration which includes two IPS units was used to test the Protection Cluster capability. This configuration ensures that if the IPS unit fails or is taken off-line, the second IPS unit takes the entire load, ensuring continued network operation.

Figure below depicts the TOE in the evaluated configuration with two IPS units.

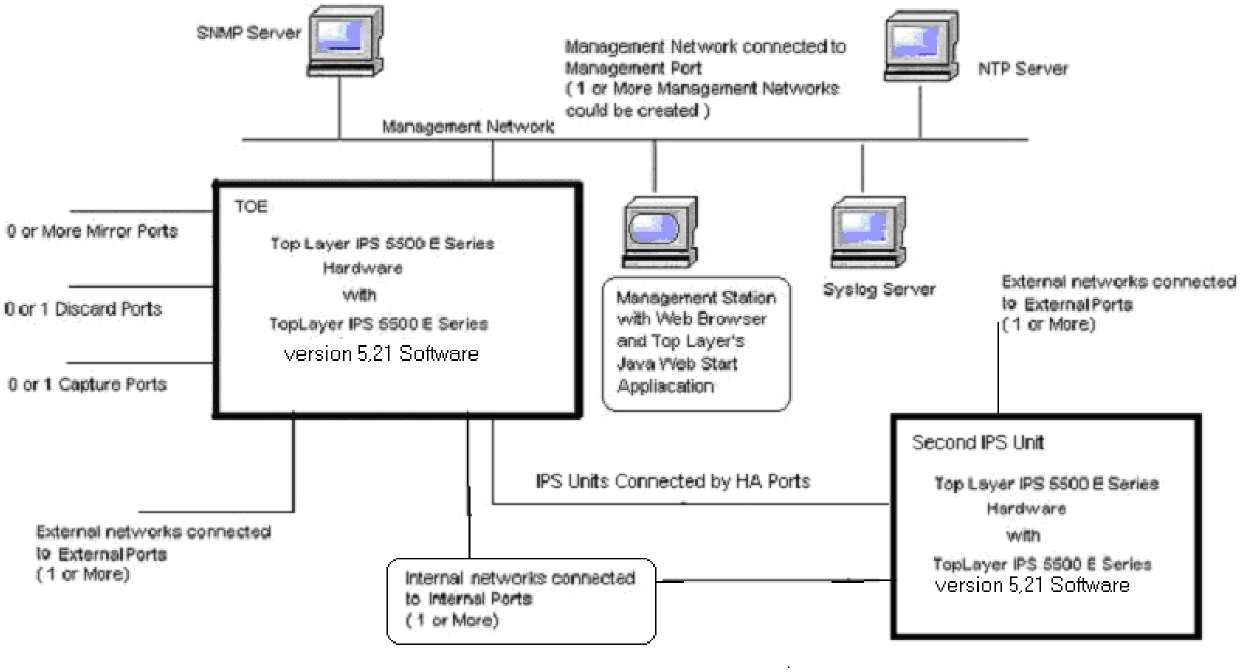
SNMP Server
Management Network connected to Management Port (1 or More Management Networks could be created)
NTP Server
Management Network
TOE
Top Layer IPS 5500 E Series Hardware with TopLayer IPS 5500 E Series version 5.21 Software
0 or More Mirror Ports
0 or 1 Discard Ports
0 or 1 Capture Ports
Management Station with Web Browser and Top Layer's Java Web Start Appliacation
Syslog Server
External networks connected to External Ports (1 or More)
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 2-9 Evaluated Configuration with High Availability Feature

Note: Customers who install only one IPS box (i.e., operating in the "single IPS box" mode of operation as shown in Figure 2-8 Evaluated Configuration) are also in the evaluated configuration.

2.3.3 Security Functionality in the IT Environment

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

- Web browser – Used to access TOE administrative interfaces and displays alerts, reports, statistics, diagnostics and security logs
- SMTP, SNMP, Syslog servers – Used 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.

2.3.4 Management Interfaces

The TOE supports a number of management interfaces:

Serial Console — The CONSOLE port on the front of the IPS Unit provides access to a limited Command Line Interface that can be used to perform basic setup.

Command Line Interface over Telnet —An extended CLI can be accessed using a Telnet session. The CLI provides access to nearly all the IPS Unit's configuration and management commands.

Graphical User Interface Access using HTTP and HTTPS — The Graphical User Interface (GUI) runs as a Java Web Start™ program over the World Wide Web. The GUI provides interface windows for configuring and managing the IPS Unit and provides access to context sensitive online help. The Java Web Start™ application, which communicates with the TOE to manage the TOE, is also included in the TOE. The application is loaded from the IPS 5500 E onto the client host and allows the administrator to affect the IPS 5500 E configuration and load audit information off the IPS 5500 E.

SNMP — The IPS Unit's Simple Network Management Protocol interface provides read-only access to many of the IPS Unit's settings.

IPS Controller — The IPS Controller is a separate product from Top Layer that allows for central management of multiple IPS Units.

All of the management interfaces described above, except the serial console, can be used to manage the TOE through a network interface port with management role.

In the evaluated configuration, management of the TOE, apart from the basic setup using the serial console, is done using the Graphical User Interface (GUI), which connects to the TOE over HTTPS.

2.4 Logical Boundaries

The security functions provided by the TOE include:

- Security audit
- User Data Protection
- Identification and authentication
- Security management
- Protection of TOE Security Functions
- Trusted Path /Channels

2.4.1 Security Audit

During the process of receiving and transmitting traffic, the TOE performs many checks and 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 to the user 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.

See the corresponding section in the TSS for more detailed information.

2.4.2 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.

See the corresponding section in the TSS for more detailed information.

2.4.3 Identification and Authentication

The TOE provides a password based authentication mechanism to users with the administrator and monitor role. The TOE communicates with the remote web browser of the administrator using the HTTPS protocol in order to encrypt the user id, 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.

See the corresponding section in the TSS for more detailed information.

2.4.4 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.

See the corresponding section in the TSS for more detailed information.

2.4.5 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 its interfaces 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 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.

See the corresponding section in the TSS for more detailed information

2.4.6 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.

See the corresponding section in the TSS for more detailed information.

2.5 Functionality Not Included in the TOE Scope

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

3 TOE Security Environment

The TOE is intended to be used in environments in which sensitive information is processed.

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

3.1 Assumptions

The assumptions are ordered into three categories: usage assumptions, personnel assumptions and physical environment assumptions.

3.1.1 Usage Assumptions

A.CONNECT The TOE will separate the network on which it is installed and operates 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.

3.1.2 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.

3.1.3 Physical Environment 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.

3.2 Threats

The TOE addresses the threats identified in this section. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

3.2.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below.

T.NOAUTH An unauthorized person 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.MANAGE An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete TSF data on the TOE

T.PROCOM An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

T.REPEAT An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

T.AUDIT Unauthorized attempts by users and external IT entities to access network resources through the TOE, TOE data or TOE security functions may go undetected because the actions they conduct are not audited or audit records are not reviewed, thus allowing an attacker to escape detection.

T.RATEBASED

An External IT Entity may exhaust service resources of the TOE or systems by passing information flows thorough the TOE.

T.ADDRESSSPOOF

An External IT Entity may illegitimately gain access to networks through the TOE by spoofing source IP address.

T.UNDESIREDACCESS

An External IT Entity may send impermissible information through the TOE, which results in the exploitation of resources.

T.CONTENTBASED

An External IT Entity may attack or tamper resources by sending information flows through the TOE, which contain malicious data or malicious inclusion of payloads that is otherwise well formed

3.3 Organisational Security Policies

There are no organizational security policies defined for this TOE.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions.

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

O.MANAGE
The TOE must protect stored TSF data from unauthorized disclosure, modification, or deletion.

O.ADMINISTRATION
The TOE must provide all the functions necessary to support the authorized users in their management of the security of the TOE. The TOE must provide the capability to allow or disallow remote administration of the TOE.

O.AUDIT The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.

O.ALERT The TOE must provide a record of the attacks detected and blocked by the TOE.

O.AUDITPROTECT
The TOE must provide the capability to protect audit information residing on the TOE.

O.UNDESIREDACCESS
The TOE must control unauthorized information flow between internal and external networks based on security policies.

O.RATEBASED
The TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDoS and other network flooding attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DoS and DDoS attacks, and authorized users who may overuse resources.

O.CONTENTBASED

The TOE must filter the content in the information flows through the TOE to prevent malicious intruders from exploiting system vulnerabilities or network based protocol weaknesses, as well as more direct attacks through e-mail based worms and viruses.

O.TIME The TOE must provide a reliable clock to maintain the system time.

O.TRANSMISSION

The TOE must provide a HTTPS session for communication between the User Management GUI on the Management Station and the TOE.

Application Note: A Management Station is a workstation on the management network that the TOE administrator uses to access the TOE using an HTTPS enabled web browser. There can be one or more Management stations.

4.2 Security Objectives For The Environment

The following are the IT security objectives that are to be addressed by Environment

OE.AUDIT The IT environment must provide a long term audit and alert store for the TOE.

OE.PROTECT

The IT environment must protect itself against attempts by unauthorized users to bypass, de-activate, or tamper with its security functions.

OE.TIME The IT environment must be configured with an NTP server that is able to provide reliable time to the TOE.

The following are the non technical IT security objectives that are to be addressed by the Environment. The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

ON.CONNECT

Those responsible for the TOE must ensure that the TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the networks without passing through the TOE.

ON.BACKUP Those responsible for the TOE must ensure that the audit files, configuration files are backed up and disk usage is monitored to ensure audit information is not lost.

ON.NOEVIL Those responsible for the TOE must ensure that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains and the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

ON.AUTH Those responsible for the TOE must ensure that they protect their authentication data.

ON.PHYSICAL Those responsible for the TOE must ensure that 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.

5 IT Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST. This ST does not define any security functional requirements to be levied on the IT environment. The security requirements levied on the TOE are defined in Sections 5.1 - 5.2.

Table 5-1: Security Functional Requirements for the TOE

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
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 initialisation
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

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components

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

a) Start-up and shut-down of the audit functions;

b) All auditable events for the [***not specified***] level of audit; and

c) [***Auditable events in Table below***]

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***information specified in table below***]

Dependencies: FPT_STM.1 Reliable time stamps

Table 5-2: Auditable Events

Functional Component ID	Auditable Events	Additional Information
FAU_ARP.1	Actions taken due to imminent security violations.	Type of Alarm Generated.
FAU_SAA.1	Enabling and disabling of any of the analysis mechanism	Authorized administrator User Identity
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection function is operating.	Authorized administrator User Identity

FDP_IFF.1(1)
FDP_IFF.1(2)
	Decision to permit requested information flows	Information of the Packet, severity the Rule Name of the Rule that Triggered the decision

FIA_AFL.1	Reaching the threshold of unsuccessful authentication attempts and the action taken	User Name presented to the TOE during Identification and Authentication

Functional Component ID	Auditable Events	Additional Information
FIA_UAU.1	Successful and Unsuccessful authentication attempt	User Name presented to the TOE during Identification and Authentication
FIA_UID.2	Successful and Unsuccessful user identification	User Name presented to the TOE during Identification and Authentication
FMT_SMF.1	Use of the security management functions	User name of the authorized administrator making the change.
FMT_SMR.1	Modifications to the group of administrator that are part of a role	User name of the authorized administrator making the change.
FPT_STM_EXP.1	Changes to the time	
FMT_MSA.1	All modifications to security attributes	Modified security attribute values
FMT_MSA.3	Modifications to the basic setup of allowing rules or restriction rules All modifications to the default value of security attributes	Modified security attribute values
FMT_MTD.1	All modifications to the TSF data	Modified TSF data – values before modification and after modification
FPT_TRP.1	Failures of the trusted path functions.	

5.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

Application Note: When the user is a human user (administrator or monitor), the user identity is associated with the event. When the event is associated with an IT entity the presumed source IP address of the IT entity is associated with the event.

5.1.1.3 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [

- ***All Hardware and Software failures detected by the TSF***
- ***IPS Unit operational events crossing Event Thresholds***
- ***Other rules for the events defined in FAU_GEN.1, added by an authorized administrator***

] known to indicate a potential security violation

b) [none]

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.4 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [

one or more of the following actions:

- ***generate SNMP Traps***
- ***Send Message via the IPS Console Port to an authorized administrator***
- ***Generate and Log Audit Records***
- ***Send Message to Syslog server***
- ***Block the attack***

]

upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

5.1.1.5 FAU_SAR.1 Audit review

Hierarchical to: No other component

FAU_SAR.1.1 The TSF shall provide [***Administrator and Monitor***] with the capability to read [***all audit data***] 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

Application Note: Only Audit data that resides on the TOE can be reviewed by Administrators and Monitors. Audit data collected by Syslog servers and SNMP servers can not be reviewed *using the local audit review GUI.*

5.1.1.6 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

FAU_SAR.3.1 The TSF shall provide the ability to perform ***searching and sorting*** of audit data based on [

All possible combinations of the following fields:

- ***Severity***
- ***IP address of the IT identity***
- ***Protocol***
- ***Rule Name***
- ***Date and Time***
- ***Physical port that received this traffic***
- ***Type of event***

]

Dependencies: FAU_SAR.1 Audit review

5.1.1.7 FAU_SEL.1 Selective audit

Hierarchical to: No other components

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set

of audited events based on the following attributes:

a) [
Message Type i.e. Event type
]

b) [

The Rule that Triggered the Message
Severity

]

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

5.1.1.8 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

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

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

Dependencies: FAU_GEN.1 Audit data generation

Application Note: Audit data resides on the TOE hardware appliance and can only be accessed using the management GUI. The TOE does not allow unauthorized modifications to the audit data residing on it through any of its management GUIs. The management GUI does not provide an option for administrators and monitors to delete audit data. The TOE automatically deletes old audit data when audit storage is exhausted.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_IFC.1 (1) Subset information flow control (1)

Hierarchical to: FDP_IFC.1

FDP_IFC.1.1 The TSF shall enforce the [***Rate Based Security Policy***] on:

[

a) Subject:

Source Subjects: External IT Entities requesting Server TCP connections and UDP flows through the TOE (Clients)

Destination Subjects: External IT Entities accepting TCP Client connections and UDP flows through the TOE (Servers)

b) Information:

TCP Service Connections and UDP Service flows information on the TOE between source subjects and destination subjects

c) Operation:

Establish a TCP connection through the TOE
Establish a UDP flow through the TOE

]

Dependencies: FDP_IFF.1 Simple security attributes

5.1.2.2 FDP_IFF.1 (1) Simple security attributes (1)

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [***Rate Based Security Policy***] based on the types of subject and information security attributes: [

© 2007 Top Layer Networks. All Rights Reserved.

a) Subject security attributes:

Source Subjects: Presumed IP address of the Client

Destination Subject: Presumed IP address of the Server

b) Information security attributes:

- ***Client (IP address)***
- ***Client Group (IP address range of a group of Clients)***
- ***Server (IP address)***
- ***Server Group (IP address range of Server Group)***
- ***Service requested by each Client***

- ***Connection Limiting Attributes***
  - ***Total simultaneous TCP connections for each Client***
  - ***Total simultaneous TCP connections from each client Group***
  - ***Total simultaneous TCP connections to each Server***
  - ***Total Simultaneous TCP connections to each Server Group***
- ***Request Limiting Attributes***
  - ***Total Number of TCP connection requests or UDP flow requests made by each client in any one minute period for each service***
  - ***Total Number of TCP connection requests or UDP flow requests made by each client in any one minute period for all services***
- ***SYN Flood Limiting Attributes***
  - ***Total Number of incomplete SYN requests outstanding from each client and client group***
  - ***Total Number of incomplete SYN requests outstanding for each server and server group***

- ***Request Limit***
- ***Connection Limit***
- ***SYN flood Limit***

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject

and **another controlled subject** via a controlled operation if the following rules hold:

© 2007 Top Layer Networks. All Rights Reserved.

[

All the three rules (a), (b) and (c) must be satisfied:

a) A TCP or UDP Service Information flow from a Client to a Server is allowed if

- ***Total Number of TCP connection requests or UDP flow requests made by the client in any one minute period for that specific service***

  and

- ***Total Number of TCP connection requests and UDP flow requests made by the client in any one minute period for all the services***

are with in the Request Limit values.

b) A TCP Service Information flow from a Client to a Server is allowed if

- ***the number of simultaneous TCP connections for that client,***
- ***the number of simultaneous TCP connections for the client in the client group,***
- ***the number of simultaneous TCP connections for the Server and***
- ***The number of simultaneous TCP connections for the Server Group of the Server***

are with in the Connection Limit values.

c) A TCP Service Information flow from a Client to a Server is allowed if

- ***Number of incomplete SYN requests outstanding from the client and***
- ***Number of incomplete SYN requests outstanding to the Server group***

are with in the SYN Flood Limit values.

]

FDP_IFF.1.3 The TSF shall enforce the

[

None

].

FDP_IFF.1.4 The TSF shall provide the following

[

Capability to:

Copy the associated traffic of an information flow to the Discard port.

].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules:

[***unidirectional information flow where the source is the TOE***].

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

5.1.2.3 FDP_IFC.1 (2) Subset information flow control (2)

Hierarchical to: No other components

FDP_IFC.1.1 The TSF shall enforce the [***Firewall + IPS Security Policy***] on:

[

a) Subject:

Source Subjects: TOE interface on which information is received Destination Subjects: TOE interface to which information is destined;

a) ***Information :***

Network packets sent through the TOE from the subject to another

b) Operation :

Pass information

]

Dependencies: FDP_IFF.1 Simple security attributes

5.1.2.4 FDP_IFF.1 (2) Simple security attributes (2)

Hierarchical to: No other components

FDP_IFF.1.1 The TSF shall enforce the [***Firewall + IPS Security Policy***] based on the following types of subject and information security attributes:

[

a) Subject security attributes:

Source Subjects: set of source subject IP addresses;

Destination Subject: set of destination subject IP addresses;

b) Information security attributes:

FW Traffic Treatment Attributes:

Presumed IP address of the Source
Presumed IP address of the Destination
Service

IPS Traffic Treatment Attributes:

Datalink Layer (MAC) Protocol Header
Network Layer Protocol Header
Transport Layer Protocol Header
Application Protocol Header
Application Payload

]

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

[

a) The Firewall Traffic Treatment information security attribute values are unambiguously permitted by the information flow rules configured by the administrator

b) The IPS Traffic Treatment information security attribute values are unambiguously permitted by the information flow rules configured by the administrator .

The rules are based on the following types of IPS traffic treatment checks:

Network Protocol Checks:

IP:
- IP option value

ICMP:
- Max Ping Length, Max ICMP Length, ICMP Rate

TCP:

- All non-SYN packets must be part of an established connection

Application Protocol Checks:

DNS:

- ***DNS Protocol Settings***

FTP:

- ***FTP authentication settings***
- ***FTP command setting***
- ***FTP Path Settings***

HTTP:

- ***HTTP Start Line Length***
- ***HTTP Request Settings***
- ***HTTP Method Settings***
- ***HTTP URI Settings***
- ***HTTP Header Length settings***
- ***HTTP Host Filter name***
-

MSNET (RPC and CIFS)

- ***CIFS Settings (Protocol Version, Length of Account name)***
- ***RPC Services (UUID, Stub length)***

SSH

- ***SSH Protocol Version***
- ***Client Message Length***
- ***SSH Plain text message length***

SMTP

- ***SMTP Command***
- ***Attachment***

Telnet

- ***Environment Variables***
- ***Telnet Options***
- ***Telnet User Account name***

Attack Signatures:

- ***ASCII printable character strings***
- ***Sequence of binary bytes***

Packet Base Checks:

Mangled/Defective traffic based on:
IP/ARP Packet and Layer 2 (MAC) Header Checks

]

FDP_IFF.1.3 The TSF shall enforce the

[

Following rules:

a) prior to applying the information policy rule set, the TOE statefully inspects, reorders and assembles packets for proper analysis

]

Application Note: The IPS Unit records critical information about each packet in a flow record stored in its Flow Table, an internal memory structure. Recording this information enables the IPS Unit to statefully inspect each packet and to reorder packets for proper analysis. At the start of each transaction, the IPS Unit creates or "sets up" the appropriate Flow Table entries. The IPS Unit checks these entries when it receives subsequent packets of that transaction.

FDP_IFF.1.4 The TSF shall provide the following

[

Capability to:
Copy the associated traffic of an information flow to the Discard port.

Block IP Fragments

Block TCP Mid-flows

Reject an information flow by sending a TCP reset packet

Copy the associated traffic of an information flow to the ports in the mirror group.

Bypass the application of the information policy rule set during System Reset of the TOE (Bypass During System Reset Mode)

]

Application notes:

IP Fragments:

When an incoming network packet is too large for the network equipment to handle, the following may occur:

- *The packet can be fragmented and sent on to its destination within the network.*
- *An ICMP error indication (MTU Exceeded) can be returned to the source and the source can then send the information as smaller packets.*

Because fragments are often used as sources of attacks, it is preferable to block fragments for all applications. Instead of allowing fragments (since most networks support Path Max Transmission Unit Discovery [MTU discovery]), send the packet back to the source for repackaging. If an application must use fragments, it can be configured as an exception.

Mid-flows:

Many types of attacks use common scanning techniques, which create incomplete TCP connections to locate vulnerabilities. Examples of such attacks include the FIN ACK Sweep, Xmas Tree, and Null scans. The IPS Unit watches for proper TCP connection setup and tear-down processes and when it identifies incomplete TCP connections, it categorizes this traffic as mid-session (midflow) traffic. When configured, , the IPS Unit drops midflows, and, therefore, prevents attacks that use incomplete TCP connections. If the IPS Unit is configured to drop traffic when it does not detect a proper session setup, in most cases, the dropped traffic simply causes the clients to retry the connection, often without any noticeable effect on end users.

Top Layer strongly recommends that the customer implement a security policy to drop TCP mid-session traffic. Failing to do so can allow attacks to circumvent the mitigation features of the IPS Unit.

Mirror Flow:

The mirror group uses the Round Robin algorithm to balance traffic among the Mirror ports.

Bypass during Reset:

The IPS Unit starts out performing in Never Bypass mode, checking and mitigating all traffic, but performs in Always Bypass mode (passes all traffic) if there is a software failure and the IPS Unit needs to reboot. Once the IPS Unit resumes normal operation, it returns to full mitigation behavior. Bypass during System Reset mode is useful once the customer has completed testing the IPS Unit and wants to mitigate traffic, but also wants to pass unchecked traffic during a software failure rather than block unchecked traffic.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules:

[***unidirectional information flow where the source is the TOE***]

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following

Rules:

[

The rules described in FDP_IFF.1.2 do not exist.

]

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when [***an authorized administrator configurable positive integer within the range 1 to 999***] unsuccessful authentication attempts occur related to [***administrator authentication attempts***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [***prevent authentication until an action is taken by the authorized administrator to unlock the user account*** **.** ***The TSF shall not allow the last or only user account to be completely locked out***].

Application Note: The TOE does not allow the last or only administrator account to be completely locked out. This prevents the TOE from becoming completely unmanageable.

5.1.3.2 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 **authorized administrators**:

[

- ***User Name***
- ***User's current Status (active, inactive, or locked)***
- ***Level of User Privileges***
- ***User password***
- ***Expiration time allowed for the user's password***
- ***Group***

]

Dependencies: No dependencies

5.1.3.3 FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [***Receipt of information flows from external IT entities for TSP enforcement***] on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification

5.1.3.4 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

FIA_UAU.7.1 The TSF shall provide only [***user ID, "*" for each password character provided, success or deny message***] to the **administrator** while the authentication is in progress.

5.1.3.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of the user.

Dependencies: No dependencies

Application Note: All users, whether authenticated or not, will always be identified. External IT Entities will be identified by an IP address. Authorized administrators will be identified by "User Name".

5.1.4 Security Management (FMT)

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 [***behaviour specified in table below***] the functions [***specified in table below***] to [***specified in table below***].

Table 5-3: Management of security functions behaviour

Behaviour	**Functions**	**Users**
determine the behaviour of, disable, enable, modify the behaviour of	Auditing, Identification and Authentication	Administrator
Enable	Reboot	Administrator
determine the behaviour of	Auditing Identification and Authentication	Monitor

Dependencies:FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

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 [***Rate Based Security Policy , Firewall + IPS Security Policy***] to restrict the ability to [***manipulate***] the security attributes [***listed in FDP_IFF.1.1(1) and FDP_IFF.1.1(2)***] to [***administrator***].

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Application Note: The term "manipulate" is used to indicate that the security attributes in FDP_IFF.1.1(1) and FDP_IFF.1.1(2) may be used to create additional "attributes" that can be used in specifying information flow policy rules.

The administrators do not manage or change the packet attributes.

5.1.4.3 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [***Rate Based Security Policy , Firewall + IPS Security Policy***] to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***administrator***] 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

5.1.4.4 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

FMT_MTD.1.1 The TSF shall restrict the ability to [***see operations specified in Table below*** *]* the [***TSF Data as specified in Table below***] to [***the authorized user as specified in the Table below***].

Table 5-4 Management of TSF Data

Security Function	Operation	TSF data	Administrator/ Monitor
Security Audit	View and Configure	Security Logs and Report settings	Administrator
	View	Security Logs and Report settings	Monitor
Identification and Authentication	Create, Modify and Delete	Users with User attributes defined in FIA_ATD.1	Administrator
	View	Users with User attributes defined in FIA_ATD.1 except password	Monitor
	View, Modify	Global User account Security Settings: Password Length, Allowed Characters, Expiration time frame, History Depth, Number of allowed unsuccessful login attempts	Administrator
	View	Global User account Security Settings	Monitor
	View, Unlock	Locked accounts	Administrator
	View	Locked accounts	Monitor
Security Management	Configure	HTTP Service, HTTPS Service, SNMP, Telnet Service, IPS Controller	Administrator
	View	HTTP Service, HTTPS Service, SNMP, Telnet Service, IPS Controller	Monitor
	View and Configure	Rate Based Security Policy	Administrator
	View	Rate Based Security Policy	Monitor
	View and Configure	FW + IPS Security Policy	Administrator
	View	FW + IPS Security Policy	Monitor
	View, Configure	Port Settings	Administrator
	View	Port Settings	Monitor
	View, Configure	Time Settings Time Zone Settings	Administrator

Security Function	Operation	TSF data	Administrator/ Monitor
	View	Time Settings Time Zone Settings	Monitor
	View	System Information Port Statistics MAC Address Table ARP Table Current Application Connections	Administrator, Monitor
	View	Blocked and Detected Attacks	Administrator, Monitor
	View	Dropped Packet Statistics	
	Reset	SYN Flood and Connection Counters	Administrator
	Reset to Factory Defaults	Configuration Files	Administrator
	Activate, upload and download	Configuration Files	Administrator
	Update	IPS Units Software	Administrator
	View, Modify	Port configuration, including bypass setting, port pairs, speeds.	Administrator
	View	Port configuration, including bypass setting, port pairs, speeds.	Monitor

Dependencies:FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Application Note: Any logged on user will have at a minimum the Monitor Role privileges and can perform all the Monitor functions.

5.1.4.5 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: [

a) Management of security function behaviour

- ***Items specified in FMT_MOF.1***

b) Management of security attributes

- ***Items specified in FMT_MSA.1, FMT_MSA.3***

c) Management of TSF data

- ***Items specified in FMT_MTD.1***

d) Management of security roles

- ***Items specified in FMT_SMR.1***

]

Dependencies: No Dependencies

5.1.4.6 FMT_SMR.1 Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the roles

[

- ***Administrator***
- ***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 Protection of TSF (FPT)

5.1.5.1 FPT_TST.1 TSF self-testing

Hierarchical to: No other components

FPT_TST.1.1 The TSF shall run a suite of tests [***during each start-up]*** to demonstrate the correct operation of [***the TSF***].

Dependencies: No dependencies

5.1.5.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of

failures occur: [

- ***Power Failure***

]

Dependencies: ADV_SPM.1 Informal TOE security policy model

Application Note:

Secure State for this product is defined as the state when the TOE (IPS Unit) inspects all traffic, mitigates problem traffic, and records all information. All traffic flows through the IPS Unit's *functions. If power fails, the IPS Unit acts as an open wire and does not forward any traffic. This provides the most protection and ensures that, in case of failure, unchecked traffic will not pass. This state is also known as "Fail Close" in firewall terminology (closes the door to all traffic). The IPS Unit can support dual power supplies and will continue to function when its primary power supply fails. However, the IPS Unit does not pass traffic if there is a failure of all power to the unit, or other hardware-based failure.*

5.1.6 Trusted Path/Channels (FTP)

5.1.6.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] **human users on management network** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [***remote*** **human** **users on management network**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***initial*** **human** **users on management network** ***authentication***, [***subsequent management of TOE***]].

Dependencies: No dependencies

5.2 Explicitly Stated TOE Security Functional Requirements

5.2.1 Protection of TSF (FPT)

5.2.1.1 FPT_STM_EXP.1 Reliable time stamps

Hierarchical to: No other components

FPT_STM_EXP.1.1 The TSF with the support of an NTP Server in the IT environment shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.2.1.2 FPT_RVM_EXP.1 Partial Non-bypassability of the TSP

Hierarchical to: No other components

FPT_RVM_EXP.1.1 The IPS Unit appliance portion of the TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the IPS Unit appliance portion's scope is allowed to proceed.

FPT_RVM_EXP.1.2 The software portion of the TSF executing in the GUI on the Management Station, when invoked by the underlying OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSF software portion's scope of control is allowed to proceed.

Dependencies: No dependencies

5.2.1.3 FPT_SEP_EXP.1 Partial TSF domain separation

Hierarchical to: No other components

FPT_SEP_EXP.1.1 The IPS Unit appliance portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP_EXP.1.2 The software portion of the TSF executing in the GUI on the Management Station shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.3 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.3 Security Requirements for the IT Environment

Table below lists the Security Functional Requirements provided by the IT Environment. The SFRs defined in this section are taken from Part 2 of the CC.

.

Table 5-5: Security Functional Requirements for the IT Environment

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

5.3.1 Class FAU: Security audit

FAU_STG_ENV.1 Protected Audit Trail Storage

FAU_STG_ENV.1.1 The remote log servers in the IT Environment shall protect the stored audit records from unauthorized deletion.

FAU_STG_ENV.1.2 The remote log servers in the IT Environment shall be able to prevent unauthorized modifications to stored audit records.

5.3.2 Class FIA: Identification and Authentication

5.3.2.1 FIA_UAU_ENV.1 User Authentication before Action

FIA_UAU_ENV.1.1 The IT Environment shall require each user to be successfully authenticated before allowing any other IT Environment-mediated actions

5.3.2.2 FIA_UID_ENV.1 User Identification before any Action

FIA_UID_ENV.1.1 The IT Environment shall require each user to be successfully identified before allowing any other IT Environment-mediated actions

5.3.3 Class FPT: Protection of the TOE Security Functions

5.3.3.1 FPT_RVM_ENV.1 Non-bypassibility of the IT Environment

FPT_RVM_ENV.1.1 The security functions of the IT environment shall ensure that IT environment security policy enforcement functions are invoked and succeed before each function within the scope of control of the IT environment is allowed to proceed.

5.3.3.2 FPT_SEP_ENV.1 Domain Separation in IT Environment

FPT_SEP_ENV.1.1 The security functions of the IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope and control of the IT environment.

FPT_SEP_ENV.1.2 The security functions of the IT environment shall enforce separation between the security domains of subjects in the scope of control of the IT environment.

5.3.3.3 FPT_STM_ENV.1 Reliable Time Stamps

FPT_STM_ENV.1.1 The NTP server in the IT Environment shall be able to provide reliable time stamps for the TOE's use.

5.4 TOE Strength of Function Claim

The TOE minimum strength of function is SOF-medium for the Identification and Authentication security function. This is consistent with the SOF claim for FIA_UAU.1..

5.5 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 4 as defined by the CC. The assurance components are summarized in the following table.

Table 5-6 - Assurance Requirements: EAL4

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	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: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ATE: Tests	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: Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent Vulnerability Analysis

6 TOE Summary Specification

6.1 TOE Security Functions

This section provides a high-level description of the security functions and assurance measures provided by the TOE to meet the requirements specified in Section 5.

The following table identifies the TOE Security Functions and the Security Functional Requirements to which they must conform.

Table 6-1: TSF Description

TSF	Sub-function	Sub-function description	SFR
Security Audit	AU-1	Audit data generation	FAU_GEN.1
	AU-2	User identity association	FAU_GEN.2
	AU-3	Potential violation analysis	FAU_SAA.1
	AU-4	Security alarms	FAU_ARP.1
	AU-5	Audit review	FAU_SAR.1
	AU-6	Selectable Audit Review	FAU_SAR.3
	AU-7	Selective Audit	FAU_SEL.1
	AU-8	Protected Audit Trail Storage	FAU_STG.1
User Data Protection	IFC-1	Rate Based Control	FDP_IFC.1(1)
			FDP_IFF.1(1)
	IFC-2	Intrusion Prevention	FDP_IFC.1(2)
			FDP_IFF.1(2)
Identification and Authentication	IA-1	Authentication failure handling	FIA_AFL.1
	IA-2	User attribute definition	FIA_ATD.1
	IA-3	Timing of Authentication	FIA_UAU.1
	IA-4	Protected authentication feedback	FIA_UAU.7
	IA-5	User identification before any action	FIA_UID.2
Security Management	SM-1	Management of security functions behaviour	FMT_MOF.1
	SM-2	Static attribute initialisation	FMT_MSA.3

© 2007 Top Layer Networks. All Rights Reserved.

TSF	Sub-function	Sub-function description	SFR
	SM-3	Management of security attributes	FMT_MSA.1
	SM-4	Specification of Management Functions	FMT_SMF.1
	SM-5	Management of TSF Data	FMT_MTD.1
	SM-6	Security Roles	FMT_SMR.1
Protection of TSF	SP-1	TSF Self-Test	FPT_TST.1
	SP-2	Failure with preservation of secure state	FPT_FLS.1
	SP-3	Non-bypassability of the TSP	FPT_RVM_EXP.1
	SP-4	TSF domain separation	FPT_SEP_EXP.1
	SP-5	Reliable time stamps	FPT_STM_EXP.1
Trusted Path	TC-1	Trusted Path	FTP_TRP.1

6.1.1 Security Audit

Enabling Auditing

By default, detailed Alert, System, and Security Event auditing is enabled. Major Administrative Events, such as logon and logoff, are enabled for auditing by default however detailed Administrative Events relating to configuration changes are turned off by default. To enable full Administrative Event auditing go to the IPS GUI and navigate to **Configure System->Advanced System Configuration -> Audit Logging**. In the Audit Logging Dialog Box, check the **Enable audit logging** and **Send audit data to syslog server(s)** check boxes. Then press the **Ok** button.

Alert, System, and Security Event auditing can be enabled and disabled by configuring the Event Logging System. This process is documented in the *IPS 5500 and IPS 5500E Configuration and Management* under the Understand Event Logging chapter. The administrator should use this information to set the level of auditing that is required.

General Event Log Auditing

Administrative Events, System Events, and Alert Events are all audited using the System Log Viewer. The viewer reads appropriate log file, Audit, Event, or Alert respectively, and allows the log to be sorted or searched in an easy to use manner.

Because the IPS is a security appliance, all logs are rotated when they are 2 Megabytes in size. The IPS, therefore, should not be used for long-term storage of audit records. Six versions of each log, however, are kept on the IPS allowing for some degree of history and storage of audit information locally. These three versions of a log file are identified as the Latest File, <logtype>.LOG and <logtype>1.LO1, etc., where <logtype> is AUDIT, EVENT, and ALERT for Administrative Events, System Events, and Alert Events respectively.

For all logs, the **Detail** section of the log message can be searched using the System Log Viewer Search feature, which is present on the View Log File screen. This feature allows an administrator to drill down into a selective view.

Auditing Administrative Events

Administrative Events can be audited by using the System Log Viewer to view, sort, or search the Audit logs. Using the IPS GUI, navigate to **Monitor System ->System Log Viewer**. In the **View Log File** dialog box, select the **Log Type** of **Audit Log** and then select the version of the Audit log to be viewed.

All Audit logs can be sorted by Day, Time, Event ID, Device, Action, User, Table, or Details.

- The Event ID is a Top Layer assigned Event ID associated with the Administrative Event.
- The User is the user that performed the action logged.
- The Action is ADD, DELETE, POWER_ON, or UPDATE.
- The Table is the MDB database table that was modified by the user.
- The Details contain details about the actual modification that took place.

Auditing System Events

System Events can be audited by using the System Log Viewer to view, sort, or search the Event logs. Using the IPS GUI, navigate to **Monitor System ->System Log Viewer**. In the **View Log File** dialog box, select the **Log Type** of **Event Log** and then select the version of the Event log to be viewed.

All Event logs can be sorted by ID, Day, Time, ID2, Device, or Details.

- The ID is a Top Layer assigned Event ID associated with the System Event.
- The ID2 is a Top Layer assigned Event ID associated with the System Event with a tln-<rule-number> format.
- The Details contain details about the actual system event that took place.

Auditing Alert Events

Alert Events can be audited by using the System Log Viewer to view, sort, or search the Alert logs. Using the IPS GUI, navigate to **Monitor System ->System Log Viewer**. In the **View Log File** dialog box, select the **Log Type** of **Alert Log** and then select the version of the Alert log to be viewed.

All Alert logs can be sorted by ID, Day, Time, ID2, Device, or Details.

- The ID is a Top Layer assigned Event ID associated with the Alert Event.
- The ID2 is a Top Layer assigned Event ID associated with the Alert Event with a tln-<rule-number> format.
- The Details contain details about the actual alert that took place.

Auditing Security Events

Auditing of Security Events is described in detail in the IPS 5500 and IPS 5500E Configuration and Management document under the Security Event Viewer chapter.

6.1.1.1 SA-1 Audit Data Generation (FAU_GEN.1)

Audit records are generated within the TOE by the TSF for the events listed in FAU_GEN.1. Audit records contain a timestamp, the information of the entity triggering the event (e.g. username, IP address of subject), and a summary of the event as well as the additional information listed in Table listed in Section 5.1.1.1.

6.1.1.2 SA-2 User Identity Association (FAU_GEN.2)

For audit events resulting from actions of identified users, the TOE is able to associate each auditable event with the identity of the user that caused the event. For audit events resulting from information flows from external IT entities, the TOE is able to associate each auditable event with the presumed IP address of the IT entity.

6.1.1.3 SA-3 Potential violation analysis (FAU_SAA.1)

The TOE maintains an internal representation of rules to monitor accumulated auditable events, which determine potential violation of the TSP. For certain IPS Unit operational events, thresholds can be set to determine when the IPS Unit should generate an event message. When the IPS Unit crosses a set threshold, it indicates a potential security violation. An example of event threshold would be very high TCP connection setup rate (35000 connections per sec). The auditable events are listed in FAU_SAA.1.2 in section 5.1.1.3.

6.1.1.4 SA-4 Security alarms (FAU_ARP.1)

The administrator can configure various methods of generating alarms to indicate potential security violations. An administrator can configure the TOE to take one or more actions as specified in the SFR FAU_ARP.1 in section 5.1.1.4.

6.1.1.5 SA-5 Audit review (FAU_SAR.1)

From the administrative interface available through the GUI, an authorized administrator or monitor can read all the audit data generated by the collection of events monitored by the TOE components. All audit records are displayed in a manner suitable for the administrator or monitor. Only Audit data that resides on the TOE can be reviewed by Administrators and Monitors. Audit data collected by Syslog servers and SNMP servers can not be reviewed using the local audit review GUI.

6.1.1.6 SA-6 Selectable Audit Review (FAU_SAR.3)

The TSF is able to perform searches and sorting of stored audit data based on various criteria with logical relations so that they can be reviewed by an authorized administrator. Searching and sorting of Audit data can be based on Severity, IP address of the IT identity, Protocol, Rule Name, Date and Time, Physical port that received this traffic and Type of event.

6.1.1.7 SA-7 Selective Audit (FAU_SEL.1)

The TSF provides a capability for authorized administrators to include or exclude the generation of auditable events related to event audit data of a selected type from the events screen of the administrative interface.

6.1.1.8 SA-8 Protected Audit Trail Storage (FAU_STG.1)

The TSF protects the stored audit records on the TOE from unauthorized deletion and modifications via the TSFI. The TSF retains log files on the local system. Log files are restricted by size. When the maximum allowed size of a log file is reached, the log file is rotated and the next log file is created by overwriting a previous log file. The TOE provides options for administrators to configure Syslog servers to store log messages.

6.1.2 User Data Protection

The Rate based, Firewall and IPS rules are the logical constructions that guide the IPS Unit's security decisions as it examines traffic flows. An IPS Unit security check is a logical definition that says: if a given traffic flow meets the following conditions, treat it in this manner.

The figure below shows how all of the subsystem rules together make up the overall security check that the IPS Unit follows when deciding how to handle the network traffic.

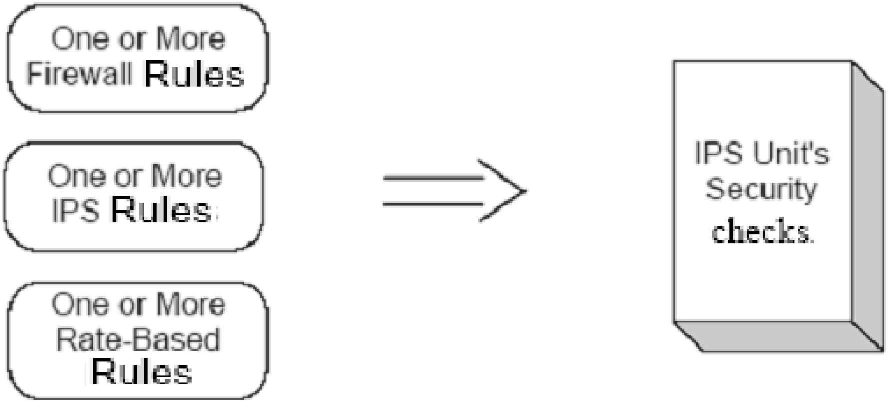
One or More Firewall Rules
One or More IPS Rules
One or More Rate-Based Rules
IPS Unit's Security checks.

Figure 6-1 IPS Unit Security Checks

The IPS Unit contains hundreds of rules that it uses to check whether a given flow of traffic is acceptable or not. A rule may be based on packet checks (for example, Illegal ICMP Header) or protocol checks (for example, HTTP Unknown Method Name). The IPS Unit contains rules for the following categories:

- Packet-based rules (global rules apply to all traffic, to check for IP/ARP bad packets and L2 MAC filters)
- Firewall rules
- Intrusion protection system rules (IPS Rules)
- Rate based rules

Rules also have "treatments" associated with them that tell the IPS Unit what should happen when a rule is triggered. Treatments include the action the IPS Unit should apply to the traffic that triggers the rule (allow, drop, reject), and the type of logging that should be performed. An administrator can modify the treatments for individual rules in these two sets. For IPS rules, there are multiple copies of the IPS rules, called "rule sets," and new copies can be created. An administrator can configure the treatment for the same rule differently in different rule sets.

Rate Based Rules

Rate based security rules protect the resources from overuse by legitimate users, as well as abusive denial-of-service attackers.

- The rules provide limits for:
  - Client requests:
    Defines the maximum number of requests that any client within the host group can make for specific services and all services during a one-minute period.
  - Connections for both clients and servers:

    Connection Limiting provides a way to limit the number of open connections allowed at one time between Clients and Servers.
  - SYN Flood controls:
    Defines the number of incomplete TCP connections from Client to Servers.

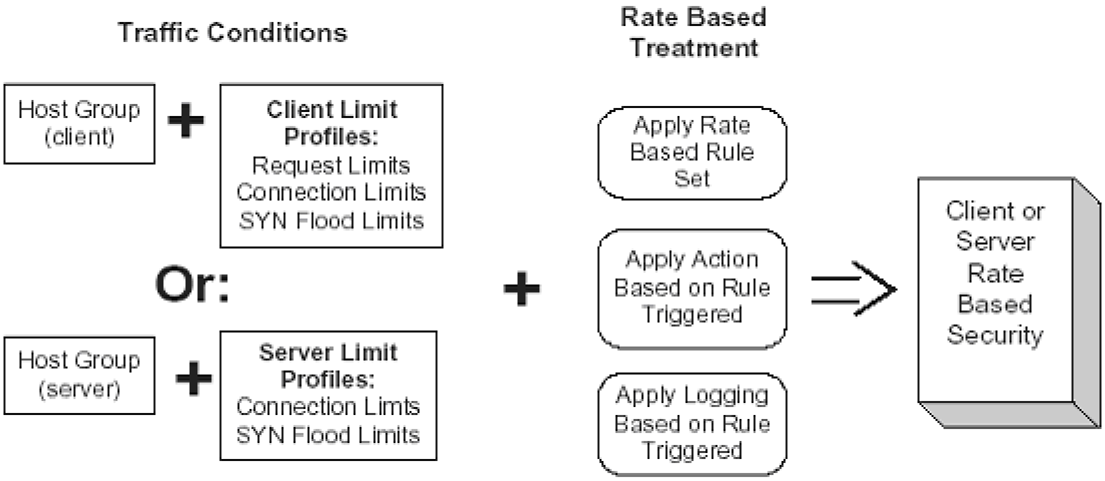

Figure 6-2 Rate Based Security

FW Rule and IPS Rules

- Provide classic firewall blocking for traffic, based on IP addresses, Layer 4 ports, and segments (port pairs);
- Provide the following types of checks:

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

The figure below shows how the subsystem policies together make up the overall FW + IPS security policy that the IPS Unit follows when deciding how to handle the network traffic.

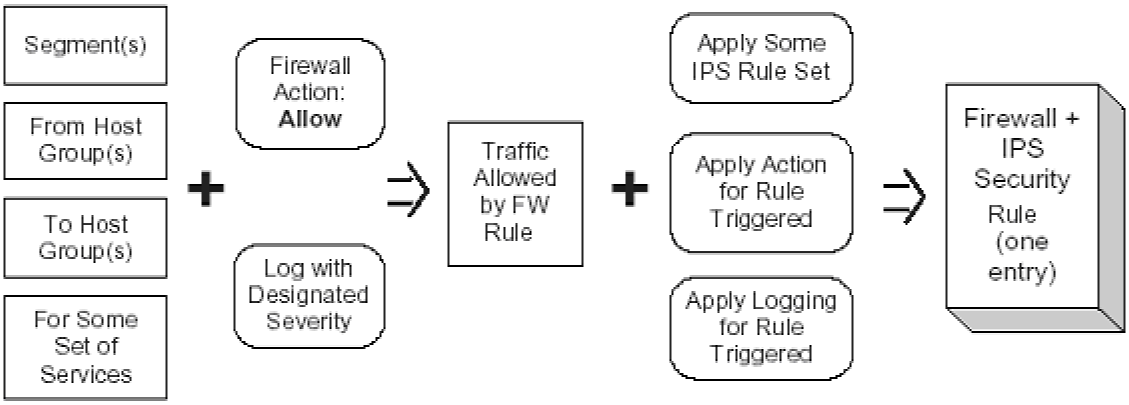
Segment(s)
From Host Group(s)
To Host Group(s)
For Some Set of Services
+
Firewall Action: Allow
Log with Designated Severity
⇒
Traffic Allowed by FW Rule
+
Apply Some IPS Rule Set
Apply Action for Rule Triggered
Apply Logging for Rule Triggered
⇒
Firewall + IPS Security Rule (one entry)

Figure 6-3 FW +IPS Security

Please also see the figure in section 2.2.

The IPS Unit's Security system is partitioned into logical subsystems to perform various security checks. 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.

6.1.2.1 IFC-1 Rate Based Control (FDP_IFC.1 (1), FDP_IFF.1 (1))

DDos Filters Subsystem:
Analyzes traffic patterns and removes malicious traffic attempting to deliberately overwhelm the resources of the TOE or internal networks (denial-of-service attacks), or to use computers in the internal network to attack other companies (distributed denial-of-service attacks). The TSF SYN Flood algorithms track the dynamic behavior of millions of individual IP addresses, classify those sources according to their threat level, and manage the addresses to stop or prevent denial-of-service attacks.

Resource Limit Filters Subsystem:
Protects resources from overuse by legitimate users as well as abusive denial-of-service attackers. Provides limits for:

- Client requests for specific services, Client requests for all services
- Connections for clients and servers (both specific clients and servers, and all clients or servers in a group)

- SYN flood controls

6.1.2.2 IFC-2 Intrusion Prevention (FDP_IFC.1 (2), FDP_IFF.1 (2))

IP/ARP Bad Packet Filters Subsystem:
Examines the IP headers of IP traffic and the payload of ARP packets. These checks look for badly mangled packets that the IPS Unit cannot reliably parse or even categorize by host group or application protocol. This reduces the load on other network appliances.

L2 Filters Subsystem:
Focuses on the MAC headers of network packets. Some of the checks look for malformed or abused fields in the MAC headers.

Stateful Analysis Subsystem:

Stores and analyzes information about each traffic connection. A flow (TCP or UDP) is the transfer of related packets over a TCP or UDP connection between a Client (source) and a Server (destination). Both TCP and UDP flows, at a minimum, use source address, destination address, protocol, source port and destination port as flow identifiers.

The IPS Unit records information about each packet in a flow record stored in its Flow Table (connection table), an internal memory structure. Recording this information enables the IPS Unit to statefully inspect each packet and to reorder packets for proper analysis. At the start of each transaction, the IPS Unit creates or "sets up" the appropriate Flow Table entries. The IPS Unit checks these entries when it receives subsequent packets of that transaction. This subsystem provides this information to other subsystems of the IPS Unit.

Firewall Filters Subsystem:
Provides classic firewall blocking for traffic, based on IP addresses, Layer 4 ports, and circuits (inside port versus outside port). The firewall’s capabilities break down into the following subcategories:

- Blocks clients from internal or external circuits.
- Performs spoof checking (that is, enforce allowed ingress circuits per IP address range).
- Enforces client access to services.
- Blocks packets from IP addresses deemed "malicious" by the SYN Flood mitigation subsystem.

Protocol Validation Subsystem:
Examines the payload of application datagrams and application streams for specific network protocols to ensure that the traffic conforms to the rules for a given protocol as well as the IPS Unit’s rules for reasonable usage. Stops attackers who abuse weaknesses in a protocol’s defined structure in order to attempt to pass malicious traffic. The protocols and checks are identified in FDP_IFF.1 (2).

Content Inspection subsystem:
Checks for deliberate inclusion of malicious data or other malicious payloads into traffic that is otherwise well formed. The Content Inspection subsystem inspects the transport layer header, application layer header and application layer payloads. This feature provides the ability to search the payloads of network protocols that are not natively parsed and decoded by the IPS Unit. The patterns that are supported by the IPS Unit can be either case sensitive or insensitive ASCII printable character strings or they can be a sequence of binary bytes. The IPS Unit's rules that correspond to these content patterns are also referred to as “signatures”.

6.1.3 Identification and Authentication

6.1.3.1 IA-1 Authentication failure handling (FIA_AFL.1)

The TOE warns the user when, during the authentication process, the defined number of unsuccessful authentication failures has been met. The TSF will prevent the user from authentication until an action is taken by an authorized administrator to unlock the user account. The TOE does not allow the last or only administrator account to be completely locked out. This is to prevent the TOE from becoming completely unmanageable

6.1.3.2 IA-2 User attribute definition (FIA_ATD.1)

The TSF maintains the following user security attributes for administrators:

- User Name
- User’s current Status (active, inactive, or locked)
- Level of User Privileges
- User password
- Expiration time allowed for the user’s password
- Group

6.1.3.3 IA-3 Timing of Authentication (FIA_UAU.1)

The TSF requires an administrator to be successfully authenticated with a password before being allowed any other management actions. An External IT entity may pass information flows through the TOE without any authentication.

6.1.3.4 IA-4 Protected authentication feedback (FIA_UAU.7)

The TSF displays only the user ID, a “*”for each password character entered, and a success or deny message to the administrator or monitor while the authentication is in progress.

6.1.3.5 IA-5 User identification before any action (FIA_UID.2)

The TSF requires each user to self identify before being allowed to perform any other actions. All users, whether authenticated or not, will always be identified. External IT Entities will be identified by an IP address. Authorized administrators are identified by “User Name”.

6.1.4 Security Management

The TSF provides several forms of management security:

Secure Architecture — The IPS Unit's architecture separates management traffic (traffic entering the IPS Unit's on one of the management ports) from mission traffic (traffic entering the IPS Unit's external and internal ports). The IPS Unit can bridge management traffic from one management port to another management port, but does not forward management traffic to any other IPS Unit mission port, nor does it forward non-management traffic to any management port.

User Account Administration — Creates and manages user accounts, providing different sets of privileges to individual users and groups of users.

User Authentication — Establishes a user's identity and privilege level.

Management Service Access Control — Provides overriding controls for each form of management access.

The IPS Unit provides several management services. For added security, the following services can be enabled and disabled:

HTTP or HTTPS – The IPS Unit provides persistent management sessions using HTTP (port 80) or HTTPS (port 443) allowing full management access through the firewall. The Graphical User Interface is not dependant on a Web browser. Instead, it uses the Java Web Start technology to provide a self-updating application that operates over the Web. The GUI is a Java WebStart application, downloaded from the IPS 5500 E as a set of jar files and cached by the Java WebStart application on the client host machine. After that, the GUI runs in a Java sandbox on the client host. Before accessing any of the IPS 5500 E functionality, the GUI must be authenticated by the IPS 5500 E. There is no authentication information in the IPS 5500 E GUI code and the authentication relies on authentication over HTTP(S).

Telnet Session - Disabled in the evaluated configuration and

Serial Console - The CONSOLE port on the front of the IPS Unit provides access to a limited Command Line Interface that can be used to perform basic setup. The serial console port supports an authentication feature, which provides an extra layer of protection for IPS deployments where the IPS Unit is deployed in an environment without physical security. In the evaluated configuration, the authentication of the CLI is enabled and, only authorized users are allowed to access the CLI.

IPS Controller - The IPS Controller is used to manage multiple IPS Units and runs on a separate device. (Not included in the evaluated configuration)

Using the Management Port Control window, an authorized administrator can allow, deny, or restrict access to each management form. The Telnet Session and HTTP are disabled in the evaluated configuration.

The IPS Unit creates a management session whenever a successfully authenticated user connects to the IPS Unit. The session continues until the user ends the session or there is a network disruption that causes the session to time out. Any given user can have multiple simultaneous management sessions over any management service. The CONSOLE port supports only one management session.

The TSF maintains and reports all relevant information for each management session, which includes:

- User name
- Session privileges
- Login time (start of session)
- Management access method (HTTP, HTTPS, Telnet, Console, etc.)
- IP address of user
- MAC address of user
- Unique session ID
- Logout time (end of session)

In addition to the Management session information, the TSF uses the following user account information to grant or deny access to a particular security function:

- User's current status (active or inactive)
- Level of user privileges
  - **Administrator** — Can perform all IPS Unit configuration tasks and view all IPS Unit operations, statistics, and reports.
  - **Monitor** — Can view all IPS Unit operations, statistics, and reports. Cannot configure the IPS Unit, nor add or edit any user profiles.
- User password
- Expiration time allowed for the user's password.

The IPS Unit authenticates a user through a login name and password.

6.1.4.1 SM-1 Management of security functions (FMT_MOF.1)

The TOE's primary security management interface is the WebUI, which is a Java web application loaded from the TOE onto the Management Station via an SSL channel. TOE Administrators and Monitors interact with the applet, sending commands to the TSF.

The security management functions that can be modified are specified in 5.1.4.1 FMT_MOF.1 Management of security functions behaviour.

6.1.4.2 SM-2 Static attribute initialisation (FMT_MSA.3)

The TSF allows only authorized administrators to modify the initial value of the security attributes of the subjects, objects and information of Rate based information flow policy and FW + IP information flow policy.

6.1.4.3 SM-3 Management of security attributes (FMT_MSA.1)

The TSF provides administrators the capability to manipulate the security attributes of subjects, objects and information of Rate based information flow policy and FW + IP information flow policy. The term "manipulate" is used to indicate that the security attributes in FDP_IFF.1.1 (1) and FDP_IFF.1.1(2) may be used to create additional "attributes" that can be used in specifying information flow policy rules. FMT_MSA.1 restricts such capabilities to the Security Administrator. An example of this would be to group a set of service identifiers that are to have the same rule applied, rather than having to specify a separate rule for each service identifier. However, an administrator cannot change or manage the attributes associated with a packet.

6.1.4.4 SM-4 Specification of Management Functions (FMT_SMF.1)

The TSF is capable of performing the following security management functions:

a) Items specified in FMT_MOF.1

b) Management of security attributes

- Items specified in FMT_MSA.1, FMT_MSA.3

c) Management of TSF data

- Items specified in FMT_MTD.1

d) Management of security roles

- Items specified in FMT_SMR.1

6.1.4.5 SM-5 Management of TSF Data (FMT_MTD.1)

The TSF restricts the ability to manage TSF data based on the Level of user privileges. There are two User Level Privileges.

- Administrator — Can perform all IPS Unit configuration tasks and view all IPS Unit operations, statistics, and reports.
- Monitor — Can view all IPS Unit operations, statistics, and reports. Cannot configure the IPS Unit, nor add or edit any user profiles

The TSF restricts the ability to perform operations as specified in section 5.1.4.4 by restricting the ability to operate on TSF data to the Authorized Administrator and Monitor

6.1.4.6 SM-6 Security Roles (FMT_SMR.1)

The TSF maintains two roles :

- Administrator — Can perform all IPS Unit configuration tasks and view all IPS Unit operations, statistics, and reports.
- Monitor — Can view all IPS Unit operations, statistics, and reports. Cannot configure the IPS Unit, nor add or edit any user profiles

For maintenance purposes, a user with ‘admin’ (Administrator Role) privileges can authenticate through the Serial Console with user name and password. There exists a default ‘admin’ and ‘password’, which must be changed after the basic setup.

6.1.5 Protection of TOE Security functions

6.1.5.1 SP-1 TSF Self-testing (FPT_TST.1)

The TSF can run a suite of tests during initial start-up to demonstrate the correct operation of the TSF. The TSF can not start up if the expected results from the assumptions do not match the actual result.

The TOE tests operation of the following list of components to ensure correct operation of the TSF during initial start-up:

- Sandisk/code load valid (required for basic operations)
- The SC subsystem FLASH and SDRAM (required for audit functions)
- The FPGAs (required for all security functions of the TSF and basic operations)
- Memory tests (required for basic operations)
- Processor tests (required for basic operations)
- Processor connectivity test (required for basic operations)
- Basic OS tests (required for basic operations)

6.1.5.2 SP-2 Failure with preservation of Secure State (FPT_FLS.1)

The Secure State for this product is defined as the state when the TOE (IPS Unit) inspects all traffic, mitigates problem traffic, and records all information. All traffic flows through the IPS Unit's functions. If power fails, the IPS Unit acts as an open wire and does not forward any traffic. This provides the most protection and ensures that in case of failure, unchecked traffic will not pass. This state is also known as "Fail Close" in firewall terminology (closes the door to all traffic). The IPS Unit can support dual power supplies and will continue to function when its primary power supply fails. However, the IPS Unit does not pass traffic if there is a failure of all power to the unit, or other hardware-based failures.

6.1.5.3 SP-3 Partial Non-bypassability of the TSF (FPT_RVM_EXP.1)

The TOE resides as a network perimeter device thus physically separating the external networks from the protected networks. All network traffic flows from and to the internal networks flows through the TOE only after inspection of the traffic based on the information flow control policies. The TOE hardware and software ensure that all packets are forwarded to, and processed through the filtering functions of the information flow control policies and that the filtering functions are not bypassable

External users are not permitted to access the TOE management functions through the user GUI without successful identification and authentication. The TOE enables the administrator to restrict the access to TOE by enabling or disabling the HTTP, HTTPS, SNMP and Telnet Session. The http and telnet management interfaces are disabled in the evaluated configuration. The Serial Port Console interface is only accessible through a serial cable with DB-9 connectors to the CONSOLE port on management PC. The TOE is assumed to be hosted in a secure facility.

All remote communications to the TOE are protected over secure HTTPS connections.

The GUI software on the Management Station is a software only TOE component. It relies upon the protection mechanisms of the underlying operating system platform to protect itself against untrusted subjects bypassing the security mechanisms offered by the GUI. The GUI is designed to ensure that TSF policies are enforced when accessed through its own interfaces.

6.1.5.4 SP-4 TSF Domain Separation (FPT_SEP_EXP.1)

The TOE resides as a network perimeter device thus physically separating the external networks from the protected networks. IPS Unit determines the list of ports to which the packet may be forwarded. The IPS Unit never forwards a packet to the port on which the packet arrived.

The TSF creates a management session whenever a successfully authenticated user connects to the IPS Unit. The session continues until the user ends the session or the session times out. The IPS Unit enforces the concept of isolated management traffic. It does this by separating traffic using two logical bridges, the Mission Bridge and the Management Bridge. Each bridge is a logical device within the IPS Unit that enables traffic to flow between its source and destination. The IPS Unit can bridge management traffic from one management port to another management port, but does not forward management traffic to any other IPS Unit port, nor does it forward non-management traffic to any management port. Separate bridges also help avoid the problem of the IPS Unit itself being attacked by external entities. Packets received on Management ports are bridged to other Management ports or terminated to the Management entity (if destined to the management entity's IP address). Packets received on Mission ports can be bridged to another Mission port, but will never be forwarded to any Management port or to the management entity.

The GUI software on the Management Station is a software only TOE component. It relies upon the protection mechanisms of the underlying operating system platform to protect itself against untrusted subjects tampering with TSF code or data through OS interfaces. The GUI is designed to ensure that TSF policies are enforced when accessed through its own interfaces.

6.1.5.5 SP-5 Reliable Time Stamps (FPT_STM_EXP.1)

The TSF supports reliable time stamps for the use of the TSF. The TOE acquires the time from an NTP server and maintains it for the use of TSF functions executing on the IPS Unit.

6.1.6 Trusted Path/Channels

6.1.6.1 TC-1 Trusted Path (FTP_TRP.1)

The TSF uses the HTTPS protocol to build a trusted path when communicating between the IPS Unit and management GUI on the management station. A browser on the Management Station in the IT environment initiates the SSL connection to the IPS Unit to establish a secure session. The cipher suite used is RSA-RC4-SHA1. The RSA key is defined by the IPS Unit certificate and the RC4 key is 128 bits.

The secure session is used for management communications.

6.2 Security Assurance Measures & Rationale

The assurance documents listed below were developed to meet the developer action and content and presentation of evidence elements for each assurance required defined in the CC.

Table 6-2 - Assurance Measures & Rationale: EAL4

Assurance Requirement	Assurance Measures	Assurance Rationale

Assurance Requirement	**Assurance Measures**	**Assurance Rationale**
ACM_AUT.1	[ACM]	The CM plan defines the automated tools used in the CM system to ensure that only authorized changes are made to the TOE implementation representation and to generate the TOE. The CM plan also describes how these tools are used in the CM system
ACM_CAP.4	[ACM]	The configuration management documents defines the configuration items(CIs), provides measures for ensuring that all changes to CIs are authorized and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE. A CM plan describes how the CM system is used and how it supports the TOE generation. An acceptance plan includes procedures to accept changes to the CIs. Evidence that the CM system is operating in accordance with the CM plan and that all configuration items are under CM control is also provided.
ACM_SCP.2	[ACM]	The CI list provided includes the implementation representation, security flaws, and CC evaluation evidence.
ADO_DEL.2	[ADO]	The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer, procedures for detecting modification or discrepancies between the master copy and the version received by the customer are described, along with procedures for detecting attempts to masquerade as the vendor (developer) when communicating with the customer.
ADO_IGS.1	[ADO]	The installation documents describe the steps necessary for secure installation, generation and start-up of the TOE.
ADV_FSP.2	[FSP]	The informal functional specification (FSP) document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes details of all effects, exceptions, and error messages for each of the external TSF interfaces, as well as a rationale that the TSF is completely represented by the FSP.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADV_HLD.2	[HLD]	The security enforcing high-level design (HLD) describes the complete TSF in terms of subsystems, separating the TOE into TSP-enforcing and other subsystems. The security functions for each subsystem are described. The purpose and method of use for all subsystem interfaces are described and the externally visible interfaces are identified.
ADV_IMP.1	[IMP]	A selected subset of the TSF implementation representation is provided at a level such that the TSF can be generated without further design decisions.
ADV_LLD.1	[LLD]	The descriptive low-level design describes the complete TSF in terms of modules, separating the TOE into TSP-enforcing and other subsystems. The security functions for each subsystem are described. The purpose and method of use for all module interfaces are described and the externally visible interfaces are identified
ADV_RCR.1	[RCR]	The informal correspondence analysis demonstrates that the security functionality as described in the FSP and ST is correct and complete. Likewise for the functionality described in the FSP and HLD, in the HLD and LLD, and in the LLD and implementation representation.
ADV_SPM.1	[SPM]	The informal TOE security policy model describes the rules and characteristics of all policies in the TSP, including a rationale demonstrating its consistency and correctness with the FSP.
AGD_ADM.1	[AGD]	The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.
AGD_USR.1	N/A	The TOE is transparent to the entities sending data through the TOE and as such, there is no User Guide. Therefore, this SAR is implicitly satisfied.
ALC_DVS.1	[DVS]	The identification of security measures document describes the physical, procedural, personnel, and other security measures used to protect the confidentiality and integrity of the TOE design and implementation. Evidence that these measures are used will also be provided.
ALC_LCD.1	[LCD]	The developer defined life-cycle model describes the model used to provide control over the development and maintenance of the TOE.

Assurance Requirement	Assurance Measures	Assurance Rationale
ALC_TAT.1	[TAT]	The well-defined development tools document will define the development tools used to implement the TOE, as well as all statements and options used to develop the TOE
ATE_COV.2	[COV]	The test coverage analysis document provides a mapping of the test cases performed against the TSF, demonstrating that the correspondence between the TSF described in the FSP and the tests is complete.
ATE_DPT.1	[DPT]	The depth of testing document demonstrates that the tests are sufficient to demonstrate that the TSF operates in accordance with the HLD.
ATE_FUN.1	[FUN]	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	[IND]	The TOE hardware, software, guidance, and testing documentation were made available to the CC testing laboratory for independent testing.
AVA_MSU.2	[MSU]	The misuse analysis document demonstrates that the guidance documentation is complete.
AVA_SOF.1	[SOF]	The TOE does not include any probabilistic or permutational mechanisms, so this SAR is vacuously satisfied (not applicable).
AVA_VLA.2	[VLA]	The vulnerability analysis document identifies and describes the process used to discover vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified vulnerability. It also justifies that the TOE is resistant to obvious penetration attacks.

6.3 Appropriate Strength of Function Claim

The TOE minimum strength of function is SOF-medium for the Identification and Authentication security function. This is consistent with the claim of SOF-medium for the FIA_UAU.1. The evaluated TOE is intended to operate in commercial and basic robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in section 4.

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

This Security Target does not claim conformance to any Protection Profiles.

8.1 Security Objectives Rationale

The following sections provide the security objectives rationale.

8.1.1 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

Table 8-1 -All Threats to Security Countered

Item	Threat	Security Objective(s) Addressing Threat	Rationale
1	T.NOAUTH	O.IDAUTH O.SELFPROTECTION O.MANAGE OE.PROTECT	This threat is mitigated by O.IDAUTH, which provides for unique identification and authentication of administrative users. Also, O.SELFPROTECTION defends against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. O. MANAGE protects stored TSF data from unauthorized disclosure, modification, or deletion. OE.PROTECT defends against attempts by unauthorized users to bypass, deactivate or tamper with the IT environment security functions, thus preventing modification TSF code and data that resides in the IT environment.

Item	Threat	Security Objective(s) Addressing Threat	Rationale
2	T.MANAGE	O.MANAGE O.ADMINISTRATION O.SELFPROTECTION	This threat is mitigated by O.MANAGE, which requires that The TOE must protect stored TSF data from unauthorized disclosure, modification, or deletion. O.ADMINISTRATION provides all the functions necessary to support the authorized users in their management of the security of the TOE. O.SELFPROTECTION defends against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
3	T.PROCOM	O.TRANSMISSION	This threat is mitigated by O.TRANSMISSION, which requires that the TSF must provide a HTTPS session for communication between the User Management GUI on the Management Station and the TOE, thus protecting the communication between the GUI and the TSF.
4	T.REPEAT	O.IDAUTH	This threat is mitigated by O.IDAUTH. The TOE must prevent the administrative user from authentication after an administrator configured number of unsuccessful authentication attempts.

Item	Threat	Security Objective(s) Addressing Threat	Rationale
5	T.AUDIT	O.AUDIT O.ADMINISTRATION O.ALERT O.TIME O.AUDITPROTECT OE.TIME OE.AUDIT	This threat is mitigated by O.AUDIT which requires that the TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security. O.ALERT provides the alerting required to warn administrators. O.AUDITPROTECT requires that the TOE must protect the audit records stored internally on the TOE. O. ADMINISTRATION defends against attempts by unauthorized users to access and use security functions. OE.AUDIT requires that IT environment must provide a long term audit and alert store for the TOE. O.TIME AND OE.TIME ensure that Reliable time stamps are applied to audit records and allow the reconstruction of a sequence of events at a later date.
6	T.RATEBASED	O.RATEBASED	This threat is mitigated by O.RATEBASED, which requires that the TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDoS and other network flooding attacks). The TOE must also be able to serve as a rate based controller and police both malicious users who attempt to flood your network with DoS and DDoS attacks, and authorized users who may overuse resources.

Item	Threat	Security Objective(s) Addressing Threat	Rationale
7	T.ADDRESSSPOOF	O.UNDESIREDACCESS	This threat is mitigated by O.UNDESIREDACCESS, which requires that the TOE must control unauthorized information flow from the external network to the internal network based on security policies. This objective also prevents information flows of from spoofed IP addresses arriving at physical ports, which do not match the address range, associated with the ports.
8	T.UNDESIREDACCE SS	O.UNDESIREDACCESS	This threat is mitigated by O.UNDESIREDACCESS, which requires that the TOE must control unauthorized information flow from the external network to the internal network based on security policies.
9	T.CONTENTBASED	O.CONTENTBASED	This threat is mitigated by O.CONTENTBASED which requires that the TOE must filter the content in the information flows through the TOE to prevent malicious intruders from exploiting system vulnerabilities or network based protocol weaknesses, as well as more direct attacks through e-mail based worms and viruses

8.1.2 Rationale For Organizational Policy Coverage

This ST has no Organizational Security Policies.

8.1.3 Rationale For Assumption Coverage

The non-IT security objectives for the environment are, in part, a re-statement of the security assumptions and the rationale is self explanatory.

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements for the TOE

The table below shows that all of the security objectives for the TOE are satisfied by at least one security functional requirement (SFR).

Table 8-2 - All Objectives for the TOE Met by Functional Requirements for the TOE

Item	Objective ID	SFR(s)	Rationale
1	O.IDAUTH	FIA_UID.2, FIA_UAU.1, FIA_UAU.7, FIA_ATD.1, FIA_AFL.1 FPT_RVM_EXP.1	All users are successfully identified before allowing any other TSF-mediated actions on behalf of that user (FIA_UID.2) All authorized users are successfully authenticated before allowing any management actions on behalf of that user.(FIA_UAU.1) The feedback during the authentication is protected (FIA_UAU.7) User attributes required for authentication are stored by the TOE (FIA_ATD.1) When the defined number of unsuccessful authentication attempts has been met or surpassed, the TOE locks the user account until it is unlocked by an administrator (FIA_AFL.1) This objective is also met by the FPT_RVM_EXP.1 requirement, which provides for non-bypassability of the TOE

Item	Objective ID	SFR(s)	Rationale
2	O.SELFPROTECTION	FPT_RVM_EXP.1, FPT_SEP_EXP.1, FPT_TST.1, FPT_FLS.1	This objective is also met by the FPT_RVM_EXP.1 and FPT_SEP_EXP.1 requirements, which provides for domain separation and non-bypassability of the TOE. FPT_TST.1 ensures the correct operation of the TOE based on the Self-Tests during initial startup to ensure the correct operation of the TSF. FPT_FLS.1 ensures that the TOE preserves a secure state when there is a power failure.
3	O.MANAGE	FMT_MOF.1, FMT_MSA.3, FMT_MSA.1, FMT_SMF.1, FMT_MTD.1, FMT_SMR.1	This objective is met by supporting multiple management roles (FMT_SMR.1), and ensuring that the TOE security attributes may only be modified by an appropriate administrator/monitor (FMT_MSA.1, FMT_SMF.1). The TOE initializes all security attributes enforcing the SFP to default values (FMT_MSA.3), and allows for the appropriate management of functions for each role (FMT_MOF.1), and TSF data within each function (FMT_MTD.1).
4	O.ADMINISTRATION	FIA_UID.2, FIA_UAU.1, FMT_MTD.1, FMT_SMF.1,	All users are successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user (FIA_UID.2). An authorized administrator must successfully be authenticated before performing any management activities.(FIA_UAU.1) TSF Data is managed by authorized users (FMT_MTD.1 and FMT_SMF.1).

Item	Objective ID	SFR(s)	Rationale
5	O.AUDIT	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3 FAU_SAA.1, FAU_ARP.1, FAU_SEL.1, FAU_STG.1	An audit record can be generated for security-relevant events and a user is associated with the audit events (FAU_GEN.1 and FAU_GEN.2). The TOE is able to protect audit records stored internally (FAU_STG.1). The TOE is capable of providing searching and sorting capabilities of the audit records (FAU_SAR.1) and selection capabilities for auditing to include or exclude auditable events from the set of audited events (FAU_SAR.3). The TOE is capable of analyzing the audit records based on combination of rules (FAU_SAA.1) and generating alerts based on the analysis (FAU_ARP.1).
6	O.ALERT	FAU_SAA.1, FAU_ARP.1	The TOE is capable of analyzing the audit records based on combination of rules (FAU_SAA.1) and generating alerts based on the analysis (FAU_ARP.1).
7	O.AUDITPROTECT	FAU_STG.1	The TOE is able to protect audit records stored internally (FAU_STG.1).
8	O.UNDESIREDACCESS	FDP_IFF.1(2), FDP_IFC.1(2) FPT_FLS.1	The TOE mediates the flow of all information between clients and servers located on internal and external networks governed by the TOE and provides the firewall functionality (FDP_IFF.1(2) and FDP_IFF.1(2)). FPT_FLS.1 ensures that the TOE preserves a secure state when there is a power failure.

Item	Objective ID	SFR(s)	Rationale
9	O.RATEBASED	FDP_IFF.1(1), FDP_IFC.1(1)	The TOE enforces a Rate Based Security Policy based on request limits, connection limits and SYN flood limit parameters to ensure that the TOE or any of the IT resources on the internal network are not overused. This also ensures that they are not susceptible to DOS attacks (FDP_IFF.1(1), FDP_IFC.1(1)).
10	O.CONTENTBASED	FDP_IFF.1(2), FAU_IFC.1(2)	The TOE enforces a Packet Filter + IPS Policy based on the information flow characteristics, packet header and payload information to ensure that the TOE detects and prevents any intrusion. The TOE checks for both protocol anomaly and signature matching attacks and prevents them. (FDP_IFF.1(2), FDP_IFC.1(2)).
11	O.TIME	FPT_STM_EXP.1	This objective is met by FPT_STM_EXP.1, which requires that the TSF acquire time from an NTP Server in the IT environment and maintain the time reliably for its own use.
12	O.TRANSMISSION	FTP_TRP.1	FTP_TRP.1 requires cryptographic based communications protocols between the Management station in the IT environment and the TOE.

8.2.2 Security Functional Requirements for the IT Environment

The table below shows that all of the security objectives for the IT Environment are satisfied.

Table 8-3 - All Objectives for the IT Environment Met by SFRs for IT Environment

Item	Objective ID	SFR(s)	Rationale
1	OE.AUDIT	FAU_STG_ENV.1	This objective is met by FAU_STG_ENV.1, which specifies that the operating environment be provided with a log repository.

Item	Objective ID	SFR(s)	Rationale
2	OE.PROTECT	FPT_SEP_ENV.1, FPT_RVM_ENV.1, FIA_UID_ENV.1, FIA_UAU_ENV.1	This objective is met by FPT_RVM_ENV.1, which provides for non-bypassability of security functions, and FPT_SEP_ENV.1, which specifies protection of the TSF code and data. FIA_UAU_ENV.1 and FIA_UID_ENV.1 require that the IT environment does identification and authentication of users before accessing TSF data.
3	OE.TIME	FPT_STM_ENV.1	This objective is met by FPT_STM_ENV.1, which requires that the IT environment to supply time stamps to the TOE.

8.2.3 Explicitly Stated Requirements Rationale

FPT_STM_EXP.1 is explicitly stated because the functionality is provided partially by the TOE and partially by the IT environment. The TOE obtains the time from an NTP server in the IT environment.

FPT_RVM_EXP.1 and FPT_SEP_EXP.1 are explicitly stated because the functionality is provided partially by the TOE and partially by the IT environment. The TOE component running on the Management Station (Java Web Start Application) is software only and cannot protect itself or enforce non-bypassability without the support of the underlying platform

8.2.4 Rationale for TOE Security Assurance Requirements

EAL4 was chosen to provide a moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is low and the product will have undergone a search for flaws. Please see section 6.2.

8.2.5 Rationale For IT Security Requirement Dependencies

This section includes a table of all the security functional requirements, their dependencies, and a rationale for any dependencies that are not satisfied.

Table 8-4 – SFR Dependencies

Item	SFR ID	Dependencies	Reference
1	FAU_GEN.1	FPT_STM_EXP.1	28
2	FAU_GEN.2	FAU_GEN.1, FIA_UID.2	1, 17
3	FAU_SAA.1	FAU_GEN.1	1
4	FAU_ARP.1	FAU_SAA.1	3
5	FAU_SAR.1	FAU_GEN.1	1

Item	SFR ID	Dependencies	Reference
6	FAU_SAR.3	FAU_SAR.1	5
7	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	1 , 22
8	FAU_STG.1	FAU_GEN.1	1
9	FDP_IFC.1(1)	FDP_IFF.1(1)	10
10	FDP_IFF.1(1)	FDP_IFC.1(1), FMT_MSA.3	9, 19
11	FDP_IFC.1(2)	FDP_IFF.1(2)	12
12	FDP_IFF.1(2)	FDP_IFC.1(2), FMT_MSA.3	11, 19
13	FIA_AFL.1	FIA_UAU.1	15
14	FIA_ATD.1	None	
15	FIA_UAU.1	FIA_UID.1	17
16	FIA_UAU.7	FIA_UAU.1	15
17	FIA_UID.1	None	
18	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	21 , 23
19	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	20 , 23
20	FMT_MSA.1	FDP_IFC.1(1), FDP_IFC.1(2),FMT_SMF.1, FMT_SMR.1	9, 11 , 21, 23
21	FMT_SMF.1	None	
22	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	21 , 23
23	FMT_SMR.1	FIA_UID.1	17
24	FPT_TST.1	None	
25	FPT_FLS.1	ADV_SPM.1	
26	FPT_RVM_EXP.1	None	
27	FPT_SEP_EXP.1	None	
28	FPT_STM_EXP.1	None	
29	FTP_TRP.1	None	

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

Table 8-5 – TOE Security Function to SFR Mapping

SFR	TSF	Sub-function	Sub-function description

SFR	TSF	Sub-function	Sub-function description
FAU_GEN.1	Security Audit	AU-1	Audit data generation
FAU_GEN.2		AU-2	User identity association
FAU_SAA.1		AU-3	Potential violation analysis
FAU_ARP.1		AU-4	Security alarms
FAU_SAR.1		AU-5	Audit review
FAU_SAR.3		AU-6	Selectable Audit Review
FAU_SEL.1		AU-7	Selective Audit
FAU_STG.1		AU-8	Protected Audit Trail Storage
FDP_IFC.1(1)	User Data Protection	IFC-1	Rate Based information flow control
FDP_IFF.1(1)			
FDP_IFC.1(2)		IFC-2	Intrusion Prevention
FDP_IFF.1(2)			
FIA_AFL.1	Identification and Authentication	IA-1	Authentication failure handling
FIA_ATD.1		IA-2	User attribute definition
FIA_UAU.1		IA-3	Timing of Authentication
FIA_UAU.7		IA-4	Protected authentication feedback
FIA_UID.2		IA-5	User identification before any action
FMT_MOF.1	Security Management	SM-1	Management of security functions behaviour
FMT_MSA.3			
FMT_MSA.1		SM-2	Static attribute initialization
FMT_SMF.1		SM-3	Management of security attributes
FMT_MTD.1		SM-4	Specification of Management Functions

SFR	TSF	Sub-function	Sub-function description
		SM-5	Management of TSF Data
FMT_SMR.1		SM-6	Security roles
FPT_TST.1	Protection of TSF	SP-1	TSF self testing
FPT_FLS.1		SP-2	Failure with preservation of secure state
FPT_RVM_EXP.1		SP-3	Partial Non-bypassability of the TSP
FPT_SEP_EXP.1		SP-4	Partial TSF domain separation
FPT_STM_EXP.1		SP-5	Reliable time stamps
FTP_TRP.1	Trusted Path/Channels	TC-1	Trusted Path

8.4 Rationale For Strength of Function Claim

The TOE minimum strength of function is SOF-medium for the Identification and authentication security function and is consistent with the claim of SOF-medium for the FIA_UAU.1 SFR that maps to that security function. The evaluated TOE is intended to operate in commercial and medium robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in section 4.

8.5 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles.

9 References

This section contains descriptions of documents pertaining to this ST and or subject TOE.

Table 9-1 References

Document Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2005-08-002, Version 2.3, August 2005.	[CC]
IPS 5500 E-Series: Functional Specification For Common Criteria EAL4 Evaluation Version 1.2	[FSP]
IPS 5500 E-Series:High Level Design Low Level Design For Common Criteria EAL4 Evaluation Version 1.6	[HLD]
IPS 5500 E-Series:High Level Design Low Level Design For Common Criteria EAL4 Evaluation Version 1.6	[LLD]
Source Code Implementation	[IMP]
IPS 5500 E-Series:High Level Design Low Level Design For Common Criteria EAL4 Evaluation Version 1.6	[RCR]
Top Layer Networks IPS 5500 E Security Target, Version 1.1	[SPM]
IPS 5500 E Configuration and Management Guide Part number 990-0188-09 IPS Hardware Installation Guide Part Number 990-0183-07	[AGD]
IPS 5500 E-Series: Configuration Management For Common Criteria EAL4 Evaluation Version 0.8	[ACM]
IPS 5500 E-Series: Delivery and Modification Detection For Common Criteria EAL4 Evaluation Version 0.7	[ADO]
IPS 5500 E-Series: Development Security Procedures For Common Criteria EAL4 Evaluation Version 0.6	[DVS]
IPS 5500 E-Series: Developer Life Cycle Model For Common Criteria EAL4 Evaluation Version 0.6	[LCD]
IPS 5500 E-Series: Development Tools For Common Criteria EAL4 Evaluation Version 0.2	[TAT]
IPS 5500 E-Series: Test Coverage (ATE_COV.2) And Depth of Coverage (ATE_DPT.1) For Common Criteria EAL4 Evaluation Version 0.7	[COV]
IPS 5500 E-Series: Test Coverage (ATE_COV.2) And Depth of Coverage (ATE_DPT.1) For Common Criteria EAL4 Evaluation Version 0.7	[DPT]
IPS 5500 E-Series: Test Plan For Common Criteria EAL4 Evaluation Version 1.0	[FUN]
IPS 5500 E-Series: Common Criteria Analysis Guidance For Common Criteria EAL4 Evaluation Version 0.4	[MSU]
IPS 5500 E-Series: Strength of Function For Common Criteria EAL4 Evaluation Version 0.2	[SOF]
IPS 5500 E-Series: Vulnerability Analysis For Common Criteria EAL4 Evaluation Version 0.5	[VLA]