Trend Micro InterScan™ VirusWall™ Security Target

ST Version 1.0

28 April 2003

Prepared For:

Trend Micro Incorporated
10101 N. De Anza Blvd., 2nd Floor
Cupertino, CA., 95014 USA

Prepared By:

Science Applications International Corporation
7125 Gateway Drive
Columbia, MD 21046

1 Security Target (ST) Introduction

Trend Micro InterScan™ VirusWall™, henceforth referred to as InterScan VirusWall, is a suite of anti-virus programs that work at the Internet gateway to detect and clean virus-infected files before they enter the corporate network.

The suite monitors inbound and outbound email messages, all incoming HTTP traffic, checks for viruses and malicious Java and ActiveX applets, provides enterprise-wide Java and Authenticode standards, and ensures that all inbound file transfers made via FTP are virus-free.

InterScan VirusWall provides a high degree of user configurability and routine tasks such as virus alert notifications, virus pattern updates, and management of log files.

This section identifies the Security Target (ST), Target of Evaluation (TOE), specifies the ST conventions and ST conformance claims.

Security Target, TOE, Vendor, and CC Identification

ST Title – Trend Micro InterScan™ VirusWall™ Security Target

ST Version – 1.0

TOE Identification - Trend Micro InterScan™ VirusWall™ 3.52 for NT Version,

Trend Micro InterScan™ VirusWall™ 3.6 for Solaris, HP-UX, and Linux

Vendor – Trend Micro, Inc.

Evaluation Assurance Level (EAL) – EAL 4

Common Criteria Identification – Common Criteria for Information Technology Security Evaluation Version 2.1, August 1999, (International Standard – ISO/IEC 15408:1999)

Keywords – malicious code, virus

1.2 Common Criteria Conformance Claims

This TOE and ST are consistent with the following specifications:

- Common Criteria (CC) for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999.
    - Part 2 conformant
- Common Criteria (CC) for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999
    - Part 3 conformant
    - Evaluation Assurance Level 4(EAL4)

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations.
    - Assignment: allows the specification of an identified parameter.

  - Selection: allows the specification of one or more elements from a list.
  - Refinement: allows the addition of details.

  The conventions for the assignment, selection, refinement, and interaction operations are described in section 5.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

Terminology

- **ActiveX applet** – is a program written in Visual Basic that is included in web pages.
- **Audit** – The term audit is used to maintain consistency with the CC. Trend Micro's product literature uses the term log when referring to the audit record.
- **Authorized administrator / Administrator** – A user in the administrator role is an authorized user who 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 them. The term authorized administrator is taken from the CC and is used in the ST in those sections that are derived from the CC directly. Otherwise, the term administrator is used. These terms are used interchangeably.
- **HTTP traffic** – this is information enters the network via the Internet using web pages.
- **JAVA applet** – is a program written in the JAVA programming language that are include in web pages.
- **Malicious Code** – a hostile program that is able to access, alter or corrupt the user computer system and data.
- **Security Target (ST)** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
- **Target of Evaluation (TOE)** - An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Security Target Overview and Organization

This InterScan VirusWall security target is organized as follows:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by InterScan VirusWall and it environment and the organizational policy that the InterScan VirusWall must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the InterScan VirusWall and its environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for InterScan VirusWall and IT Environment that supports the TOE, and details the requirements for EAL 4.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the InterScan VirusWall that satisfy the security requirements.

- Section 7 – Rationale

  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

Target of Evaluation (TOE) Description

The TOE is the Trend Micro InterScan™ VirusWall™ product, henceforth referred to as InterScan VirusWall. The TOE is comprised of two product versions, 3.52 for the NT platform and 3.6 for the UNIX platform. The two versions are similar with the exception of the audit function.

Version 3.52 auditing provides three audit logs; virus, security and server. Additionally, a utility to manage the three logs is provided. Version 3.6 provides two audit logs, virus and system. Additionally, version 3.6 provides a utility to manage the virus log. The system log is viewed via an editor's tool provide by the environment. Henceforth, the term InterScan VirusWall is used to refer to TOE or product versions, unless otherwise specified.

InterScan VirusWall is a suite of anti-virus programs that work at the Internet gateway to detect and optionally pass, delete, quarantine or clean virus-infected files before they enter or leave the corporate network system. The TOE is installed on computers using Windows 2000 or Windows NT for version 3.52 and UNIX for version 3.6, (see the assumption A.Hardware for details of the underlying system the TOE must be installed upon).

The TOE is comprised of the following services:

- E-mail InterScan VirusWall - monitors and scans all inbound and outbound email messages (SMTP traffic).
- Web InterScan VirusWall - monitors all inbound HTTP traffic, checking for viruses and malicious Java and ActiveX applets, and providing enterprise-wide Java and Authenticode standards.
- FTP InterScan VirusWall - ensures that all inbound file transfers made via FTP are virus-free (FTP traffic).

All three InterScan VirusWall services provide a high degree of user configurability and routine tasks such as virus alert notifications, virus pattern updates, and management of the audit log files.

Additionally, each InterScan VirusWall service provides the capability for the administrator to determine which file types are scanned for viruses, the action InterScan VirusWall takes upon detecting a virus, and other program details.

In addition to detecting known viruses, InterScan VirusWall detects and intercepts previously unknown polymorphic or mutation viruses and detects both known and unknown macro viruses. Actions to be taken in the event that any of these viruses are detected are user configurable.

2.1 Scope of TOE

2.1.1 Physical Boundary

The TOE is the InterScan VirusWall software product. There is no difference between the TOE and the InterScan VirusWall product. The TOE runs on an operating system and relies on the operating system and the hardware in the IT environment for it to operate. The operating system and hardware is addressed by the IT Environment descriptions. The operating system and hardware is included by assumption and is not part of the TOE.

Logical Boundary

The TOE includes management interfaces provided to the administrator to primarily define the information flow policy and to review the logs, and the interfaces to utilize services provided by operating system.

The logical boundaries of the TOE can be described in the terms of the security functionalities that the TOE provides to the system that utilizes this product for the detection of viruses and malicious code.

Audit: The InterScan VirusWall provides an auditing mechanism that collects data with respect to the security risks associated with the information that is entering or leaving the network. For SMTP traffic the designated personnel that receives notification of security violations can additionally include an administrator specified recipient, while for HTTP and FTP traffic the designated personnel is fixed to only include the client and the administrator.

User Data Protection: The virus-detection, monitoring and managing capabilities of the TOE services ensures that the information received by the network is free of any potential risks.

Security Management: The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to provide the most efficient method of implementing the risk detection to ensure the steady flow of information through the network.

TSF Protection: The FTP, SMTP, and HTTP traffic are subjected to the information process flow policy before flowing through the TOE.

3 TOE Security Environment

The TOE security environment consists of the threats to the security of the TOE, organizational security policies, and usage assumptions as they relate to InterScan VirusWall. InterScan VirusWall provides for a level of protection that is appropriate for IT environments that require detection of virus infected files before they enter or leave the network system but is not designed to resist direct or hostile attacks. It is suitable for use in both commercial and government environments.

Assumptions

This section describes the security aspects of the environment in which the TOE will be utilized. This includes information about the physical, personnel, and system aspects of the environment.

3.1.1 Physical Assumptions

A.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

A.PROTECT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.1.2 Personal Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.

3.1.3 System Assumptions

A.CONFIG The TOE is configured to ensure all SMTP, HTTP and FTP traffic flow through the TOE.

A.HARDWRE The TOE will be installed on a hardware system that meets or exceeds the following constraints:

InterScan VirusWall 3.52:

- Windows 2000 server or Windows NT version 4.0 build 1381 with Service Pack 3.0,
- PC with a Pentium 200 or faster processor,
- 64 MB of memory; 128 MB recommended,
- 25 MB free disk space for program files; 100 to 500 MB is recommended for optimal performance on high-traffic systems,
- A 800x600 monitor; 1024x768 or higher resolution is recommended,

InterScan VirusWall 3.6:

Solaris Version

- Solaris 2.6 or above on Sun SPARC platform,

- 256 MB main memory (DRAM),
- Swap space should be 2 to 3 times the main memory,
- 20 MB disk space
- 9 GB or more disk space for operation

Linux Version

- OS: Linux kernel 2.2.x ONLY, glibc 2.1.x ONLY
- IBM/AT compatible PC with Intel Pentium® processor 133 MHz or faster
- 128 MB or more of memory
- Swap space should be 2 to 3 times the main memory
- 20 MB disk space
- At least 9 GB disk space for operation (processing emails)
- Package name: libstdc++-compat

HP-UX Version

- HP-UX 10.20 or later
- 128 MB RAM
- swap space should be 2 to 3 times the main memory
- 20 MB disk space for InterScan
- At least 9 GB disk space for operation (processing emails)

The following devices can be attached to either product version:

- Keyboard,
- Mouse,
- Floppy Disk Drive,
- CD-ROM Drive
- Tape Drive,
- Fixed Disk Drives,
- Printer, and
- Network Adapter

A.IDENT The operating environment will provide a method of administrative identification and authentication.

A.SYSPRCT The operating environment will provide protection to the TOE and its related data.

A.SYSTIME The operating environment will provide reliable system time.

3.2 Threats to Security

T.ACCESS_DATA

An unauthorized user may gain access to the TOE and alter and/or delete data contained in the TOE.

T.OVRLOAD

Overload of the TOE caused by excessive network traffic that exceeds the amount permissible by the TOE may allow malicious code to enter the network undetected.

T.UNAUTH An unauthorized user may gain access to the TOE and alter the TOE configuration, causing malicious code to enter the network undetected.

3.3 Organizational Security Policy

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to InterScan VirusWall.

P.ADMIN The TOE shall provide the tools to manage and monitor the TOE services and its related data.

P.TRAFFIC All network traffic that is related to email, web and ftp shall be able to be monitored for malicious code.

4 Security Objectives

This section describes the security for the InterScan VirusWall and its supporting environment. Security objectives, categorized as either security objectives of the TOE or security objectives of the environment, reflect the stated intent to counter identified threats and assumptions. All of the identified threats, assumptions and policy are addressed by the categories listed below.

4.1 Security Objectives of the TOE

O.ADMIN The TOE shall provide the authorized administrator with the tools to monitor and administer the TOE.

O.DETECT The TOE shall be able to detect all viruses and malicious code at the Internet gateway.

O.MONITOR The TOE shall be able to process all information received.

O.QUEUE The TOE shall establish an SMTP queue for the excessive information received.

4.2 Security Objective of the IT Environment

O.AUTH_ACCESS
The TOE operating environment must ensure that only authorized users gain access to the TOE and to the data contained in the TOE.

O.ENV_ADMIN The TOE operating environment must provide the authorized administrator with the tools to management the system logs generated by InterScan VirusWall 3.6.

O.TIME The TOE operating environment shall provide an accurate timestamp.

O.SEP The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.

4.3 Security Objective of the Non - IT Environment

O.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.

O.PERSON Authorized users of the TOE shall be properly trained in the configuration and usage of the TOE and will follow the guidance provided.

O.PHYCAL Those responsible for the TOE must ensure that the parts of the TOE critical to security policy are protected from physical attack that might compromise the TOE security objectives.

O.HARDWRE The TOE will be installed on a hardware system that meets or exceeds the following constraints:

InterScan VirusWall 3.52:

- Windows 2000 server or Windows NT version 4.0 build 1381 with Service Pack 3.0,

- PC with a Pentium 200 or faster processor,
- 64 MB of memory; 128 MB recommended,
- 25 MB free disk space for program files; 100 to 500 MB is recommended for optimal performance on high-traffic systems,
- A 800x600 monitor; 1024x768 or higher resolution is recommended,

InterScan VirusWall 3.6:

Solaris Version

- Solaris 2.6 or above on Sun SPARC platform,
- 256 MB main memory (DRAM),
- Swap space should be 2 to 3 times the main memory,
- 20 MB disk space
- 9 GB or more disk space for operation

Linux Version

- OS: Linux kernel 2.2.x ONLY, glibc 2.1.x ONLY
- IBM/AT compatible PC with Intel Pentium® processor 133 MHz or faster
- 128 MB or more of memory
- Swap space should be 2 to 3 times the main memory
- 20 MB disk space
- At least 9 GB disk space for operation (processing emails)
- Package name: libstdc++-compat

HP-UX Version

- HP-UX 10.20 or later
- 128 MB RAM
- swap space should be 2 to 3 times the main memory
- 20 MB disk space for InterScan
- At least 9 GB disk space for operation (processing emails)

The following devices can be attached to either product version:

- Keyboard,
- Mouse,
- Floppy Disk Drive,
- CD-ROM Drive
- Tape Drive,
- Fixed Disk Drives,
- Printer, and
- Network Adapter

5 IT Security Requirements

This section of the ST details the security functional requirements (SFR) for the TOE and the IT Environment that will support the TOE. The SFR were drawn from the CC Part 2.

CC defined operations for assignment, iteration, selection, and refinement were used to tailor the requirements to the level of detail necessary to meet the stated security objectives. These operations are indicated through the use of underlined text (assignments and selections), italicized text (refinements) and iteration is denoted with a letter added to the component.

In addition to the TOE requirements that apply to both TOE versions, there are specific requirements that apply to the 3.52 TOE only and other requirements that apply to the 3.6 TOE only. Additionally, there are specific requirements that apply only to the environment of the 3.6 TOE. The TOE requirements are presented in the following manner to clarify the differences between the TOE versions:

Section 5.1:	TOE requirements for both TOE versions
Section 5.2:	3.52 TOE requirements only
Section 5.3:	3.6 TOE requirements only
Section 5.4:	TOE requirements for the environment of both TOE versions
Section 5.5:	TOE requirements for the environment of the 3.6 TOE only

There are no SFRs for which an explicit strength of function (SOF) claim is appropriate. Therefore, there is no minimum SOF claim made for the TOE. The TOE does not include any functions or mechanism that are of a probabilistic or permutation nature.

The following table lists the security functional requirements for the TOE and the IT environment. The security functional requirements of the IT Environment address the dependency of the TOE requirements on the environment.

Security Functional Requirements	
TOE	
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FAU_SAR.3a	Selectable audit review of Virus Logs
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simply security attributes
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_RVM.1	Non-bypassability of the TSP
(Version 3.52 only)	
FAU_SAR.1a	Audit Review of Virus, Security, and Sever Logs
FAU_SAR.3b	Selectable audit review of Security Logs
FAU_SAR.3c	Selectable audit review of Server Logs
(Version 3.6 only)	
FAU_SAR.1b	Audit Review for the Virus Log
[redacted]	

IT Environment	
FIA_UID.1	Timing of identification
FMT_SMR.1	Security Roles
FPT_SEP.1	TSF Domain separation
FPT_STM.1	Reliable time stamps
(Version 3.6 only)	
FAU_SAR.1c	Audit Review for the System Log

Table 1: Security Functional Requirements

5.1 TOE Security Functional Requirements

5.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take action to notify the administrator's designated personnel via email and generate an audit record upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions,
b) All auditable events for the not specified level of audit, and
c) Detection of information process flow policy violation,
d) Requested URLs and IP Address,
e) System updates,
f) Start-up and shutdown of the TOE services.

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, no other information.

Environment Dependency: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

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

Environment Dependency: FIA_UID.1 Timing of identification

FAU_SAA.1 Potential violation analysis

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 detection of information process flow policy violation known to indicate a potential security violation;
b) No additional rules.

5.1.5 FAU_SAR.3a Selectable audit review *of the Virus Logs*

FAU_SAR.3.1 The TSF shall provide the ability to perform searches, and sorting of *the Virus* audit data based on the service, date, user and/or virus.

FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the information process flow policy on subjects (sender, and recipient) and the information (information structure) and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.1.7 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the information process flow policy based on the following types of subject and information security attributes: information structure types.

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

1. Monitoring option is not enabled for the service and information structure type
2. Monitoring option is enabled for the service and information structure type and:
    a. No malicious code is detected,
    b. Malicious code is detected and the following actions are configured:
        i. Forward as received,
        ii. Attempt to clean and:
            1. If cleanable then forward clean, else
            2. If uncleanable,
                a. Forward as received

FDP_IFF.1.3 The TSF shall enforce no additional information flow control SFP rules.

FDP_IFF.1.4 The TSF shall provide the following no additional SFP capabilities.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: no explicit authorization rules.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: no explicit denial rules.

5.1.8 FMT_SMF.1 Specification of Management Functions[1]

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: disable, enable, and modify the services and information structure types that will be monitored by the information process flow policy.

5.1.9 FPT_RVM.1 Non-bypassability of the TSP

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

[1] Added requirement to conform to Interpretation RI #65

Additional TOE Security Functional Requirements for InterScan VirusWall 3.52

5.2.1 FAU_SAR.1a Audit review *for Virus, Security, and Server Logs*

FAU_SAR.1.1 The TSF shall provide the authorized administrator with the capability to read all information from the audit records.

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

5.2.2 FAU_SAR.3b Selectable audit review *of the Security Logs*

FAU_SAR.3.1 The TSF shall provide the ability to perform searches, and sorting of *the Security* audit data based on the security type, and/or date.

5.2.3 FAU_SAR.3c Selectable audit review *of the Server Logs*

FAU_SAR.3.1 The TSF shall provide the ability to perform searches, and sorting of *the Server* audit data based on the service, and/or date.

5.3 Additional TOE Security Functional Requirements for InterScan VirusWall 3.6

5.3.1 FAU_SAR.1b Audit review *for the Virus Logs*

FAU_SAR.1.1 The TSF shall provide the authorized administrator with the capability to read all information from the audit records.

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

IT Environment Security Functional Requirements

5.4.1 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow no actions on behalf of the user to be performed before the user is identified.

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

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the *role* of authorized administrator.

FMT_SMR.1.2 The TSF shall be able to associate *a user* with *the role*.

5.4.3 FPT_SEP.1 TSF domain separation

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

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

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.5 Additional IT Environment Security Functional Requirements for InterScan VirusWall 3.6

5.5.1 FAU_SAR.1c Audit review *for the System Logs*

FAU_SAR.1.1 The TSF shall provide the authorized administrator with the capability to read all information from the audit records.

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

Security Requirements Dependencies

The table below maps the TOE security functional requirements to the corresponding requirements they are dependent on. Note: the requirement iterations have the same dependencies and therefore the iterations are not individually identified in the table (e.g. FAU_SAR.1c).

Dependencies

	CC Identifiers	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FDP_IFC.2	FDP_IFF.1	FMT_SMR.1	FIA_UID.1	FPT_STM.1
Requirements	FAU_ARP.1		X						
	FAU_GEN.1								X
	FAU_GEN.2	X						X	
	FAU_SAA.1	X							
	FAU_SAR.1	X							
	FAU_SAR.3			X					
	FDP_IFC.2					X			
	FDP_IFF.1				X				
	FMT_SMF.1								

Table 2: SFR mapping to SFR Dependencies

The dependencies of the TOE security functional requirements are, for the most part, met through the functionality of the TOE and/or by the security functionality of the IT environment. The only requirements that are dependencies and are not included as TOE or environment functional requirements are FMT_MSA.3 and FMT_MSA.1. These requirements are direct and indirect dependencies of FDP_IFF.1 and address the management of security attributes used in the policy defined in FDP_IFF.1. There is only one security attribute upon which the FDP_IFF.1 policy is based upon, and that is the object security attribute “information structure type”. The TOE does not provide the capability to manage the information structure type associated with the information structure (e.g. cannot change the file type of attached files being sent through the TOE). Therefore, these requirements are not applicable to the TOE. All other requirements identified as dependencies in the table above are included within the ST.

5.7 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the components included in Evaluation Assurance Level (EAL) 4 as specified in Part 3 of Common Criteria. No operations of refinements or iterations were applied to the assurance components.

The assurance requirements were modified, when necessary, to confirm to National and International Interpretations. The modifications are identified as follows:

- Additions of details are indicated using bold, (e.g. “…**all** objects…”)
- Deletions are indicated using strike-through (e.g. “… ~~some~~ objects…”)

Assurance Class	Assurance Components
Class ACM: Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Class ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Class 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
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class 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
Class 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
Class AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

Table 3: Assurance Components for EAL 4

5.7.1 Class ACM: Configuration Management

5.7.1.1 ACM_AUT.1: Partial CM automation

ACM_AUT.1.1D: The developer shall use a CM system.

ACM_AUT.1.2D: The developer shall provide a CM plan.

ACM_AUT.1.1C: The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_CAP.4 Generation support and acceptance procedures

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

International Interpretation RI #3 The configuration list shall uniquely identify all configuration items that comprise the TOE[2]

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

[2] New assurance element added to conform with Interpretation RI #3

ACM_SCP.2.1D The developer shall provide ~~CM documentation~~ **a list of configuration items for the TOE**.[3]

ACM_SCP.2.1C ~~The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.~~ **The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.**[4]

~~ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.~~[5]

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Class ADO: Deliver and Operation

5.7.2.1 ADO_DEL.2 Detection of modification

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C ~~The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.~~ **The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.**[6]

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Class ADV: Development

[3] Modification made to conform with Interpretation RI #4

[4] Modification made to conform with Interpretation RI #4

[5] Deletion made to conform with Interpretation RI #4

[6] Modified to conform with Interpretation RI #51

5.7.3.1 ADV_FSP.2 Fully defined external interfaces

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.1 Subset of the implementation of the TSF

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.7.3.6 ADV_SPM.1 Informal TOE security policy model

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Class AGD: Guidance Documents

5.7.4.1 AGD_ADM.1Administrator guidance

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Class ALC: Lifecycle

5.7.5.1 ALC_DVS.1 Identification of security measures

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Class ATE: Tests

5.7.6.1 ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: high-level design

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

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

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing – sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

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

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

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.7.7 Class AVA: Vulnerability Assessment

5.7.7.1 AVA_MSU.2 Validation of analysis

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.2 Independent vulnerability analysis

AVA_VLA.2.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.2.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.2.1C ~~The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.~~ **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.**[7]

AVA_VLA.2.2C ~~The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.~~ **The**

[7] Modified to conform with Interpretation RI #51

vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.[8]

AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.[9]

AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.[10]

AVA_VLA.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

[8] Modified to conform with Interpretation RI #51

[9] Added to conform with Interpretation RI #51

[10] Added to conform with Interpretation RI #51

6 TOE Summary Specification

6.1 TOE Security Functions

The below described security functions fulfill the security requirements that are illustrated in Section 5.1. Supporting rationale that the functions fulfill the security requirements is located in Section 7.4, Toe Summary Specification Rationale.

The security functions performed by the InterScan VirusWall are as follows:

- Audit
- User Data Protection
- Security Management
- TSF Protection

6.1.1 Audit Function

Generation

The InterScan VirusWall generates a daily audit log of their activities. Each auditable event that occurs is complied into a record, which is written into the log. The events are as follows:

- Start and stop of the InterScan VirusWall services,
- Virus pattern file and scanning engine update,
- Violation detected and the policy action performed

Each audit record consist of the following information:

- The transport service,
- Date and time of the event,
- Sender identification,
- Recipient identification,
- File processed,
- The violation that occurred,
- The actions taken in response.

Additionally, there are optional events that can be monitored and audited at the discretion of the authorized administrator. The HTTP service provides an option to monitor and record all URLs that are requested. The resulting audit record created includes the IP address of client and URL requested, which is written into the daily audit log.

In InterScan VirusWall 3.52, the daily audit logs are a composite of two types of logs;

- Virus log – contains the details that surround the occurrences of information process flow policy violations and the actions taken,
- System log – is a composite of two types of logs, security and server.
  - Security log– contains information about the violations to the information process flow policy that are related to Java Applets and,
  - Server logs – contains the recording of administrative actions that are taken, such as the start-up and shutdown of the InterScan VirusWall services.

In InterScan VirusWall 3.6, the daily audit logs are composed of two types of logs;

- Virus log – contains the occurrences of the information process flow policy violations
- System log – contains the details of the transactions performed by the TOE, the system error messages and the start-up and shutdown of the TOE.

Management

The InterScan VirusWall provides the authorized administrator with a log-viewing utility that provides the administrator with the capability to monitor, manage, and view the audit logs. The utility is used to view the two logs of InterScan VirusWall 3.52 and the virus log of InterScan VirusWall 3.6.

The utility allows to the administrator to view the number of violations that occur on a specific day, based on the service type. Additionally, in InterScan VirusWall 3.52, the Email InterScan VirusWall (SMTP) service provides a real-time activity monitor, that tracks, in real-time, the progress of the violation detected. The data tracked includes the number of messages processed, number of violations detected, and the status of the policy.

The log viewing utility allows the administrator to perform queries and sorting on the audit log using the criteria given for the type of log information that is requested.

In both InterScan VirusWall 3.52 and 3.6:

- virus logs are queried using the service, date, virus and/or user.

In InterScan VirusWall 3.52:

- In the System log; the security log is queried using the security type, Java applets and the date, and while server logs are queried by the service type and date. It organizes the queried information is organized into a format that can be exported into a standard tool for further analysis.

In InterScan VirusWall 3.6:

- the system logs are viewed by an editor's tool provided by the environment.

Notification

Notifications are specific to each service. Email InterScan VirusWall (SMTP) inserts a warning message into the original message; Web InterScan VirusWall (HTTP) sends an HTML message to the requesting browser, and FTP InterScan VirusWall issues an ASCII text alert to the requesting client.

The InterScan VirusWall provides a notification utility that provides the administrator with the ability to automatically send messages via email to the designated personnel about each violation and the actions taken. The designated personnel vary with the service. For the Email InterScan VirusWall (SMTP) service, the designated personnel can include but not be limited to the sender, recipient, and the administrator. For the Web InterScan VirusWall (HTTP) service and FTP InterScan VirusWall service, the designated personnel are the client and administrator

Additionally, the Web InterScan VirusWall (HTTP) service has an added capability to issue violation notifications. The Web InterScan VirusWall (HTTP) provides a window option that will alert the client to the status of their requests and the violations that have been noted and rectified based on configured actions.

6.1.2 User Data Protection

Information Process Flow Policy

The TOE implements an information process flow policy, which determines the procedures utilized to process information entering the system and the action taken when a security violation occurs. The security violations are viruses, which include macros, file, boot, multi-partite and polymorphic viruses, malicious code in the form of JAVA applets

The policy is configurable by the authorized administrator. It can be configured to perform virus scanning on selected or all information structure types with respect to selected services (HTTP, FTP, or SMTP). The actions taken at the occurrence of a violation is also configurable.

The information structure types are all files types that are capable of becoming infected and carrying a virus or malicious code. These files include, but are not limited to, document, compressed, media, and html files.

With the enabling of the policy, the InterScan VirusWall utilizes a scanning engine that creates a copy of the information file to a temporary location and opens the copy for virus checking. If the information is clean, InterScan VirusWall deletes the copy and releases the original for delivery by the appropriate service. The service refers to one of the three protocols, SMTP, HTTP, and FTP.

If a violation is found, a notification is issued and InterScan VirusWall takes the actions configured. The actions that can be taken are as follows:

- Pass – forwards information with violation included.
- Move – moves the information to a designated file for the services.
- Delete – removes the information from the system.
- Auto Clean – the information is cleaned and then delivered to recipient.

For the above actions a notification can be issued to the specified recipients in a format that is relative to the service that processed the information.

6.1.3 Security Management

Roles

The TOE implements only one role, which performs all functionalities. This role is considered to be the authorized administrator. The authorized administrator is the user that has been given the administrative rights to the TOE by the system administrator of the underlying operating system.

Functions

The InterScan VirusWall supports policies and features that require appropriate management. The policies and features are as follows:

- **Audit** – the audit function permits the authorized administrator to manage and view the audit logs. Make selection of additional information to be audited. Perform manually deletions and set up a scheduled deletion of the audit logs.

- **Information Process Flow Policy** – the policy functions permit the authorized administrator to enable the violation processing capability with respect to selected services (SMTP, HTTP, and FTP), select the information structure type that would be processed, configure the actions that would be taken at the occurrence of a violation and if notification is issued and to whom.

- **System Services –** the system services provides the authorized administrator with the capability to automatically or manually update the scanning engine and virus pattern files to ensure the current information is available for the information process flow.

6.1.4 TSF Protection

The Implementation of the InterScan VirusWall services integrates the services into the system network as a vital and transparent part of the overall network. The implementation configuration ensures that all SMTP, HTTP and FTP traffic flows thru the services. The configurable options that are modifiable by the authorized administrator ensure that all information is subjected to the information process flow policy.

The InterScan VirusWall runs as an underlying system service that is started and stopped with the operating system or at the discretion of the authorized administrator.

6.2 Assurance Measures

The assurance measures address in this section applies to the EAL 4 requirements.

Configuration Management

The Configuration Management Plan and Security Flaw Records/Documentation describes the CM measures utilized by Trend Micro that ensure that the configuration items are uniquely identified and changes are accurately tracked. The documentation describes the processes and procedure followed and automated tools that are utilized in the tracking and monitoring the changes to the CM items and the generation of the TOE.

This measure satisfy the following requirements:

- ACM_AUT.1
- ACM_CAP.4
- ACM_SCP.2

Delivery and Operation

Delivery and Operation describes the methods and procedures used to distribute and identify the TOE that is obtained by electronic and non-electronic means. Quick Start Guide for Solaris, HP, and Linux describe the various installation configuration topologies and methods to set-up and operate the TOE.

The administrative guidance describes the interfaces and procedures that are used by the administrator to operated and administer the TOE in a secure manner. The guidance documents. the security functions and the interfaces that are utilized to configure the functions. Administrative guidance is as follows:

- Trend Micro InterScan VirusWall 3.6 Administrator Guide For Solaris, HP-UX, and Linux,
- Trend Micro InterScan VirusWall 3.5 Administrator's Guide For NT version, and
- Administering Your Trend Micro Security Product.

This measure satisfy the following requirements:

- ADO_DEL.2
- ADO_IGS.1
- AGD_ADM.1
- AGD_USR.1

Development Documentation

The following documentation describes the functional specification of the TOE. It includes a description of the aspects of the TOE security design, architecture and interfaces.

- Functional Specification – details the interfaces and the functions of the TOE.
- High-Level Design – provides a high level description of the TOE and it's security functions in terms of subsystems
- Low-Level Design – provides a detailed description of the TOE in terms of modules.
- Representation Correspondence – provides a mapping of the security functions and requirements to the descriptions provide in the design documentation.
- Trend Micro InterScan VirusWall Security Policy Model – presents an informal model of the security polices associated with the security requirements.
- Source Code – sample of the implementation of the security functions in the TOE.

This measure satisfy the following requirements:

- ADV_SPM.1
- ADV_RCR.1
- ADV_LLD.1
- ADV_IMP.1
- ADV_HLD.2
- ADV_FSP.2

Lifecycle Support

The NIAP Life-Cycle Documentation describes the adequacy of the procedures used during the development and maintenance of the TOE. The manual documents the security measures utilized in the development environment to ensure confidentiality and the integrity of the TOE design and generation.

This measure satisfy the following requirements:

- ALC_DVS.1
- ALC_LCD.1
- ALC_TAT.1

Tests

The following documentation describes how the security relevant functions are tested. The document describes the test practices utilized to test the security functionality of the TOE.

- Test Plan InterScan VirusWall Unix
- Tests Cases InterScan VirusWall for Unix 3.6
- Test Plan InterScan VirusWall NT 3.52
- Tests Cases InterScan VirusWall for NT 3.52
- Test Coverage Analysis for InterScan VirusWall

This measure satisfy the following requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

Vulnerability Assessment

Vulnerability Assessment identifies the vulnerabilities in the TOE. The assessment provides the status of each identified vulnerability and demonstrates that each one cannot be exploited in the intended environment and that the InterScan VirusWall is resistant to obvious penetration attacks.
Misuse Analysis shows that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

This measure satisfy the following requirements:

- AVA_MSU.2
- AVA_SOF.1
- AVA_VLA.2

7 Rationale

This section provides the rationale for completeness and consistency of the ST.

7.1 Security Objectives Rationale

This section shows that all threats, secure usage assumptions, and organizational security policies are completely covered by security objectives.

The following table shows the assumptions, threats and organizational policy that each IT security objective addresses.

Security Objectives

	TOE				IT Environ				Non - IT Environ			
	O.ADMIN	O.DETECT	O.MONITOR	O.QUEUE	O.AUTH_ACCESS	O.ENV_ADMIN	O.SEP	O.TIME	O.INSTALL	O.PERSON	O.PHYCAL	O.HARDWRE
Assumptions												
A.LOCATE											x	
A.PROTECT									x	x	x	
A.MANAGE										x		
A.NOEVIL										x		
A.CONFIG									x	x		
A.IDENT					x							
A.SYSPRCT					x						x	
A.HARDWRE												x
A.SYSTIME								x				
Threats												
T.ACCESS_DATA					x		x				x	
T.OVRLOAD				x								
T.UNAUTH					x		x			x	x	
Policy												
P.ADMIN	x					x						
P.TRAFFIC	x	x	x	x				x	x	x		

Table 4: Mapping of Threats and Organizational Policies to Security Objectives

The following describe how the Security Objectives for the TOE and the Environment completely and effectively counters the threats and fulfill the organizational policies that are implemented:

O.ADMIN This objective ensures that interfaces provide the administrator with the ability to configure the TOE, enable the auditing capabilities, manage and query the audit logs, while providing other tools for the performance monitor for the SMTP services, providing real-time activity monitoring of the enforcing of the SFP. Thus the TOE enforces P.ADMIN, supports the enforcement of P.TRAFFIC.

O.DETECT This objective ensures that the administrator is provided with tools and the capability to enable the information process flow policy, perform regular maintenance to ensure the system is able to detect all familiar and unfamiliar virus and malicious code, and supports the enforcement of P.TRAFFIC.

O.MONITOR This objective ensures that all information that is capable of carrying malicious code is checked, before entering or leaving the network, thus supporting the enforcement of P.TRAFFIC.

O.QUEUE This objective will ensure that all information flowing into the system is monitored, regardless of the volume of the information. Thus, countering T.OVRLOAD and supporting the enforcement of P.TRAFFIC.

O.AUTH_ACCESS

This objective ensures that only authorized administrators have access to the TOE, thus supporting the countering T.ACCESS_DATA and T.UNAUTH and assuring that A.IDENT and A.SYSPRCT are addressed.

O.ENV_ADMIN This objective supports P.ADMIN by ensuring that the InterScan VirusWall 3.6 is provided with the tools needed to view the system logs.

O.TIME By ensuring that accurate timestamp is provided; accurate record information on a time/date basis can be generated, queried and tracked. This objective addresses A.SYSTIME, and supports P.TRAFFIC.

O.SEP This objective provides the support needed by the TOE to counter threats T.UNAUTH and T.ACCESS_DATA by ensuring that the TOE cannot be tampered with or bypassed.

O.INSTALL By ensuring that the TOE is delivered, installed, managed, and operated in a secure manner, the assumptions A.PROTECT and A.CONFIG are addressed, and P.TRAFFIC is supported. This objective ensures that the TOE is managed and administered in a secure manner by a competent and security aware individual in accordance with the administrator documentation.

O.PERSON This objective ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. Thus, addressing A.CONFIG, A.NOEVIL, A.MANAGE, and A.PROTECT. Additionally, this objective supports the countering T.UNAUTH and supports the enforcement of P.TRAFFIC.

O.PHYCAL This objective ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated. This objective addresses A.LOCATE, A.PROTECT, A.SYSPRCT and supports the countering of T.ACCESS_DATA and T.UNAUTH.

O.HARDWRE This objective ensures that the TOE is operating on the hardware, operating system, and associated software that would ensure the TOE operates correctly and has sufficient space to execute the security functions correctly. This objective addresses A.HARDWRE.

7.2 Security Requirements Rationale

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

Objectives	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1a	FAU_SAR.1b	FAU_SAR.1c	FAU_SAR.3a	FAU_SAR.3b	FAU_SAR.3c	FDP_IFC.2	FDP_IFF.1	FMT_SMF.1	FPT_RVM.1	FMT_SMR.1	FIA_UID.1	FPT_SEP.1	FPT_STM.1
TOE																		
O.ADMIN	x	x	x	x	x	x		x	x	x			x		x	x		
O.DETECT											x	x	x		x	x	x	
O.MONITOR		x	x														x	x
O.QUEUE											x	x		x			x	
IT Environment																		
O.AUTH_ACCESS															x	x		
O.ENV_ADMIN							x											
O.SEP																	x	
O.TIME																		x

Table 5: SFR mapping to Security Objectives

The following text describes how each security objective is satisfied by the SFRs:

O.ADMIN *The TOE shall provide the authorized administrator with the tools to monitor and administer the TOE.*

FAU_ARP.1 provides a notification capability, which is utility to keep the administrator updated on SFP violations.

FAU_GEN.1, FAU_SAA.1, FAU_GEN.2, FAU_SAR.1a, FAU_SAR.1b, FAU_SAR.3a, FAU_SAR.3b, FAU_SAR.3c defines an auditing capability, which records all information that flows into the system and the actions taken.

FMT_SMR.1, FIA_UID.1 ensures that the authorized administrator role is defined, based on identification and authentication.

FMT_SMF.1 ensures that the TOE provides the tools the authorized administrator use to perform the security management of the information process flow policy.

The above-mentioned requirements provide the tools and capabilities that are utilized by the administrator to monitor and administer the TOE.

O.DETECT *The TOE shall detect all viruses and malicious code at the Internet gateway.*

FDP_IFC.2, FDP_IFF.1 defines the SFP that ensures that all inbound and outbound information is analyzed for SFP violations and that appropriate action is taken.

FPT_SEP.1 protects the TOE from disruption caused by untrusted subjects.

FMT_SMR.1, FIA_UID.1 ensures that the authorized administrator role is defined.

FMT_SMF.1 ensures that the TOE provides the tools the authorized administrator use to perform the security management of the information process flow policy.

The above-mentioned requirements ensure that all SFP violations are detected and appropriate actions are taken.

O.MONITOR The TOE shall process all information received.

FAU_GEN.1, FAU_GEN.2, and FPT_STM.1 provide the means to record all information received by the TOE and the results of the SFP with respect to the received information.

FPT_SEP.1 protects the TOE for disruption caused by untrusted subjects.

The above-mentioned requirements ensure all information that enters the network system is checked for SFP violations.

O.QUEUE The TOE shall establish a queue for the excessive information received.

FDP_IFC.2, FDP_IFF.1 ensures that all information is monitored, provides a method to continue the processing when the large amount of information for the TOE to handle.

FPT_RVM.1 ensures that all the inbound and outbound information cannot bypass the SFP.

FPT_SEP.1 protects the TOE for disruption caused by untrusted subjects.

The above-mentioned requirements ensure that all SFP violations are detected and appropriate actions are taken and that any attempt to bypass the system is not possible.

O.AUTH_ACCESS
The TOE operating environment must ensure that only authorized users gain access to the TOE and to the data contained in the TOE.

FMT_SMR.1, FIA_UID.1 ensures that TOE operating environment defines the administrator role and provides the identification mechanism to ensure that only authorized administrators have access to the TOE and its associated data.

The abovementioned requirements ensure that only authorized administrator has access to the TOE and the data associated and generated by the TOE.

O.ENV_ADMIN The TOE operating environment must provide the authorized administrator with the tools to management the system logs generated by the InterScan VirusWall 3.6.

FAU_SAR.1c ensures that the TOE environment provides the administrator with the capability to view the system logs of InterScan VirusWall 3.6.

The abovementioned requirement ensures IT environment provides the administrator with the editor tool required to view the system logs.

O.TIME The TOE operating environment shall provide an accurate timestamp.

FPT_STM.1 ensures that the environment provides accurate and reliable time mechanism, which may be utilized by the TOE.

The abovementioned requirement ensures that the environment has a timing mechanism which accurate and reliable.

O.SEP *The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.*

FPT_SEP.1 ensures that the environment protects the TOE from intrusions from untrusted process.

The abovementioned requirement ensures that the environment protects the TOE from untrusted process that could attempt to tamper with or bypass the TOE.

Rationale of Internal Consistency and Support

The selected functional requirements for the TOE and IT Environment are internally consistent. All the operations performed are in accordance with the CC. The ST does not include any instances of a requirement that conflicts with or contradicts another requirement. In instances where multiple requirements apply to the same functions, the requirements and their operations do not cause a conflict between each other.

The selected requirements are mutually supportive by supporting the dependencies as demonstrated in the Table 2, the rationale of the suitability of the requirements to meet the objectives; the inclusion of architectural requirements, FPT_RVM.1 and FPT_SEP.1, to protect the TOE; the inclusion of audit requirements to detect attacks and the inclusion of management requirements to provide a means to properly configure and manage the other security requirements

Security Assurance Requirements Rationale

The EAL chosen is based on the statement of the security environment (assumptions, threats and organizational policy) and the security objectives defined in this ST. The sufficiency of the EAL chosen (EAL4) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative staff is conscientious, non-hostile and well trained (A.NOEVIL, A.MANAGE, O.PERSON). The TOE is physically protected (O.PHYCAL), and properly and securely configured (O.INSTALL). Given these aspects, a TOE based on good commercial development practices is sufficient. The CC states that EAL 4 permits a developer to gain the maximum assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills and other resources. Given the amount of assurance deemed necessary to meet the security environment and objectives of the TOE and the intent of EAL 4. EAL 4 is an appropriate level of assurance for the TOE described in this ST.

TOE Summary Specification Rationale

This section in conjunction with section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The security functions described are necessary for the required functionality in the TSF.

	Security Functions			
Requirements	Audit	User Data Protection	Security Management	TSF Protection
FAU_ARP.1	x	x		
FAU_GEN.1	x			
FAU_GEN.2	x			
FAU_SAR.1a	x			
FAU_SAR.1b	x			
FAU_SAR.3a	x			
FAU_SAR.3b	x			
FAU_SAR.3c	x			
FDP_IFC.2		x		
FDP_IFF.1		x		
FMT_SMF.1			x	
FPT_RVM.1				x

Table 6: Security Functional Requirements vs. Security Functions

FAU_ARP.1 Security alarms
The audit function and the user data protection function are suitable to meet this requirement. The TOE provides a method of alerting the select personnel of the occurrence of the policy violation and the actions taken. It then records the incident in the daily audit log. The notification is triggered by the user protection function that invokes the information process flow policy.

FAU_GEN.1 Audit data generation
The audit function generates a record of the auditable events that is stored in the audit log which is created on a daily bases. The record generated includes the date and time of the event, event type, the information structure type, the sender/requester and/or recipients and the action taken.

FAU_GEN.2 User identity association
The audit records of the virus and security portion of the audit log include the identity sender/requester and/or recipient.

FAU_SAA.1 Potential violation analysis
The log viewing utility and the real-time activity monitor of the Email InterScan VirusWall give the authorized administrator the ability to review the number of violation occurrences. The log viewing utility

gives the total number of violations per service type and per date, while the activity monitor is real-time information about violations.

FAU_SAR.3a Selectable audit review of Virus Logs,
The log viewing log utility provides the administrator with the capability to query and view the virus logs based on the selected criteria.

InterScan VirusWall 3.52:
FAU_SAR.1a Audit review,
FAU_SAR.3b Selectable audit review of Security Logs,
FAU_SAR.3c Selectable audit review of Server Logs
The log viewing utility provides the administrator with the capability to query the audit logs and view the results of the logs. The utility gives the option to view all available data in the virus, server or security portion of the logs or limit the data based on certain criteria.

InterScan VirusWall 3.6:
FAU_SAR.1b Audit review of the Virus Logs
The utility in the Audit function provides the means to view all available data in the virus log.

FDP_IFC.2 Complete information flow control,
FDP_IFF.1 Simple security attributes
The User Data Protection function utilizes the information process flow policy to monitor and process the information entering into the system. The policy encourages the analysis of the information for potential violations and takes appropriate steps to rectify the presence of a violation, based on the administrator configuration.

FMT_SMF.1 Specification of Management Functions
The Security Management function provides administrator the capability to enable, and disable the information process flow policy, select the actions that would be taken upon the violation of the policy and select the method and type of notification of violations. It provides the capability for the administrator to select the type of information structure with respect to selected services to be monitored and processed, and the ability to install and configure the InterScan VirusWall services to ensure that the information entering the system is subjected to the information process flow policy.

FPT_RVM.1 Non-bypassability of the TSP
The TSF Protection function ensures through the implementation and the configuration of the TOE that all information traffic is subjected to the information process flow policy.

Strength of Function Rationale

The TOE does not identify functional requirements for which an explicit SOF is appropriate and does not identify any functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

Notes on Deviations

Note 1: In FIA_UID.1.2, corrected “successfully” for spelling error.

Note 2: In FMT_SMR.1.1, and FMT_SMR.1.2 changed the word “roles” to role” for grammatical sentence structure

References

Common Criteria for Information Technology Security Evaluation Part 1, CCIMB-99-031, Version 2.1, August 1999.

Common Criteria for Information Technology Security Evaluation Part 2, CCIMB-99-032, Version 2.1, August 1999.

Common Criteria for Information Technology Security Evaluation Part 3, CCIMB-99-033, Version 2.1, August 1999.

Trend Micro InterScan VirusWall 3.5 Administrative Guide for NT Version, July 2000

Trend Micro InterScan VirusWall 3.6 Administrative Guide for Solaris, HP-UX, and Linux, August 2001

Trend Micro InterScan VirusWall 3.6 for Solaris Readme.txt, September 2001

Trend Micro InterScan VirusWall 3.6 for Linux Readme.txt, September 2001

Acronyms

CC - Common Criteria

EAL - Evaluation Assurance Level

FTP – File Transfer Protocol

HTTP – Hypertext Transfer Protocol

IT - Information Technology

SFP - Security Function Policy

SFR - Security Function Requirement

SMTP – Simple Mail Transfer Protocol

ST - Security Target

TOE - Target of Evaluation

TSC - TSF Scope of Control

TSF - TOE Security Functions

TSP - TOE Security Policy