TNO report

PP-Software Based Personal Firewall-1.2

Low Assurance Protection Profile for a Software Based Personal Firewall for home Internet use

Version	1.2
Date	6th April 2005
Author(s)	Rob Hunter Dirk-Jan Out

Certification ID	BSI-PP-0014
Sponsor	TNO-ITSEF BV
File name	Software Based Personal Firewall Low Assurance Protection Profile 1.2.doc
No of pages	12

FINAL

Document information

Date of issue	6th April 2005
Author(s)	Rob Hunter Dirk-Jan Out
Version number report	1.2
Certification ID	BSI-PP-0014
Scheme	BSI
Sponsor	TNO-ITSEF BV
Sponsor address	Delftechpark 1 2628XJ Delft The Netherlands
Evaluation Lab	SRC
Evaluation Lab address	Graurheindorferstrasse 149a D-53117 Bonn Germany
Project leader	Rob Hunter
Target of Evaluation (TOE)	Software Based Personal Firewall
TOE reference name	Software Based Personal Firewall
CC-EAL number	1
Classification	Final
Report title	Low Assurance Protection Profile for a Software Based Personal Firewall for home Internet use
Report reference name	PP-Software Based Personal Firewall-1.2

Document history

Version	Date	Comment
0.1	7-04-04	Initial version
0.2	28-04-04	Review comments included
0.3	29-04-04	Second review round comments included
0.4	6-07-04	Comments from BSI included
1.0	3-09-04	Evaluation comments from SRC included
1.1	4-09-04	Lapp number changed from 2 to 3
1.2	6-04-05	Incorporation of Raised Interpretations, added certification ID

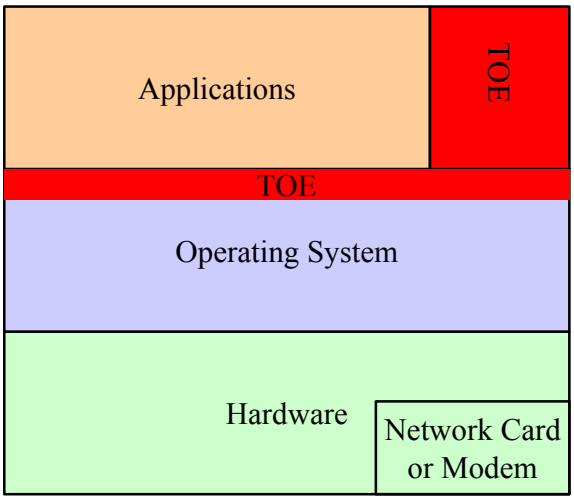
1. PP Introduction

1.1 PP Reference

This is the Low Assurance Protection Profile for a
Software Based Personal Firewall for home Internet use 1.2, TNO-ITSEF BV, 6th April 2005

1.2 TOE overview

The TOE is a software-based firewall, as is typically used in a typical home computing network environment to protect a personal computer that is connected to the Internet. The diagram below shows where the TOE can be placed in its environment: the TOE can operate as an application (from the home users point of view) or as part of the OS (from the computer applications point of view) and may also operate at both levels.



The TOE is used to regulate the flow of network traffic to and from the environment in which it is installed. As the TOE is connected to the Internet, the types of traffic that is regulated are:

- outgoing traffic: data that flows from the computing environment to the Internet
- incoming traffic: data that flows from the Internet to the computing environment.

The TOE intercepts, respectively, incoming and outgoing traffic that attempts to enter and exit the computing environment and applies a set of rules that define under which conditions network traffic is either allowed to proceed or is discarded.

The TOE may warn the user of the home PC when certain violations of the rules governing network traffic to and from the TOE occurs. A warning could relate to:

- A single violation of the rules, for example, an application attempts to make a outbound connection during installation in order to send customer information to a remote site
- A combination of violations of the rules, for example, a hacker runs a port scan on the computer in order to identify possible attack entry points.
- The TOE also keeps an event log of violations.

The TOE is not a stand-alone device, and requires a supporting computing platform with at least one network interface.

2. Conformance claims

2.1 Conformance claim

This Protection Profile:

- claims conformance to CC version 2.4 release 256 and v2.4Draft Interpretation[1] #1-#17
- is CC Part 2 conformant and CC Part 3 conformant.
- does not claim conformance to any other PP.
- is EAL 1 conformant

2.2 Conformance claim rationale

PP-related conformance claim rationale
This PP does not claim conformance to another PP, so there is no rationale related to this.

Package-related conformance claim rationale
This PP is EAL1 conformant. The EAL1 package contains no uncompleted operations. As no SARs were added to EAL1, the SARs in this PP are consistent with EAL1.

2.3 Conformance statement

Security targets or other PPs wishing to claim conformance to this PP can do so as *strict-PP-conformance*. Demonstrable-PP-conformance is not allowed for this PP.

[1] V2.4 Draft Interpretation #n are interpretations that are made during the v2.4 Trial Period. They address problems with CC v2.4 as they occur.

3. Security Requirements

3.1 Extended components definition

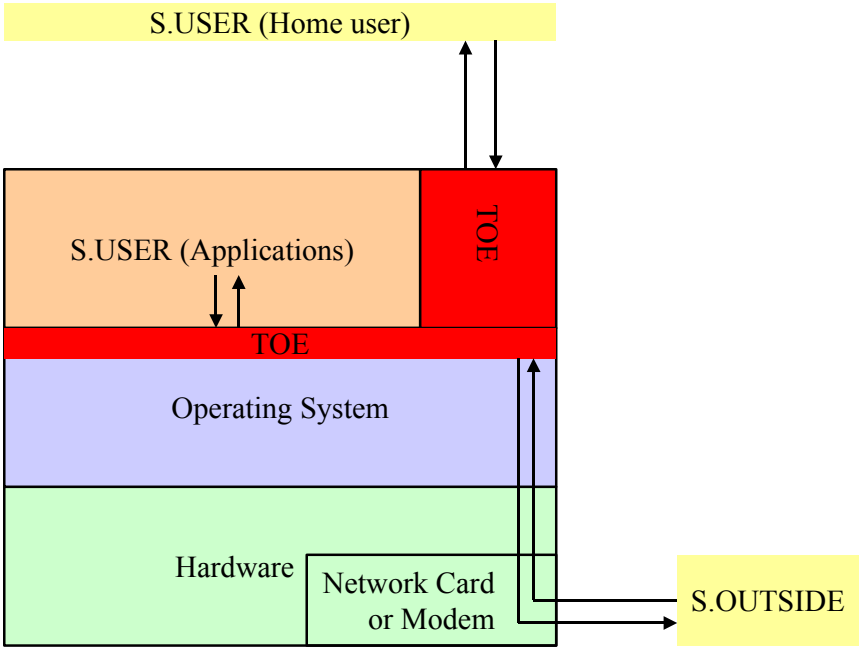
As this PP does not contain extended security requirements, there are no extended components.

3.2 Definition of subjects, information, operations and objectives for the environment

This section is added to define the terms that are used in the SFRs.

3.2.1 Subjects

The following diagram indicates the subjects as seen from the perspective of the TOE.



S.USER	A person or entity that uses the TOE.
S.OUTSIDE	Any entity on the “Internet” side of the TOE.

All subjects have a single security attribute, which is identical to its name.

3.2.2 Objects

D.RULE_SET	Object containing TSF data that defines how the firewall handles incoming and outgoing data.
D.INBOUND_TRAFFIC	User data that enters the TOE from S.OUTSIDE. This object has the following security attributes: • Source Address, • Destination Address, • Source Port, • Destination Port, • Packet type.
D.OUTBOUND_TRAFFIC	User data that leaves the TOE to S.OUTSIDE. This object has the following security attributes: • Source Address, • Destination Address, • Source Port, • Destination Port, • Packet type.

3.2.3 Operations

The operations that are performed by the TOE are (in alphabetical order):

R.ENTER	The TSF allows D.INBOUND_TRAFFIC to enter the TOE.
R.EXIT	The TSF allows D.OUTBOUND_TRAFFIC to leave the TOE.

4. Security Objectives for the Operational Environment

The operational environment of the TOE shall conform to the following objectives:

OE.USER	S.USER shall keep the computing environment on which the TOE installed integer. To this end he shall: • Install anti-virus software and ensure it is kept up-to-date. • Update his entire computing environment with the latest patches and updates for this environment • Use his judgment when downloading and running executable content such as programs, scripts and macros etc in order to prevent attacks on the integrity of the computing environment.
OE.ENVIRONMENT	The computing environment on which the TOE is installed shall communicate with S.OUTSIDE only through the TOE.
OE.HOME[2]	The operational environment of the TOE shall be a general home-type environment. This means low physical security measures.

[2] *Application Note: The goal of this security objective is to ensure that any PP or ST claiming compliance to this PP cannot add objectives for the operational environment that are inconsistent with this objective, such as "The TOE shall be guarded for 24 hours a day".*

5. SFRs

The SFRs in this PP can be divided into three groups according to the three main functionalities:

- filtering
- management
- logging and auditing

5.1 SFRs for filtering

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **FIREWALL_POLICY**[3] on:

- **D.INBOUND_TRAFFIC,**
- **D.OUTBOUND_TRAFFIC.**

FDP_ACF.1 Security attribute based access control[4]

FDP_ACF.1.1 The TSF shall enforce the **FIREWALL_POLICY** to objects based on**:**

- **Source address,**
- **Destination address,**
- **Source port,**
- **Destination port,**
- **Packet type.**

FDP_ACF.1.2[5,6] The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The TOE performs R.ENTER on D.INBOUND_TRAFFIC if**

  "Destination Port(D.INBOUND_TRAFFIC)" and
  "Source Address(D.INBOUND_TRAFFIC)" and

[3] The firewall policy consists of the elements FDP_ACF.1.1 and FDP_ACF.1.2

[4] The third and fourth element were empty and therefore refined away.

[5] In the rule definition, the words 'matches a rule defined' is used to indicate that the S.USER has created a rule that tells the TSF how to handle the network traffic when a particular condition is met.

[6] This SFR presents a logical view on D.RULE_SET: D.RULE_SET is the set of all that is allowed. Developers typically implement D.RULE_SET with ALLOW and DENY rules or a combination of both. However, logically, DENY rules are excluded from the set of permitted traffic operations and are therefore not permitted to pass through the TSF.

"Packet Type(D.INBOUND_TRAFFIC)"

matches a rule defined in D.RULE_SET.

- **The TOE performs R.EXIT on D.OUTBOUND_TRAFFIC if**

  "Source Port(D.OUTBOUND_TRAFFIC)" and
  "Destination Address(D.OUTBOUND_TRAFFIC)" and
  "Packet Type(D.OUTBOUND_TRAFFIC)"

  matches a rule defined in D.RULE_SET.

5.2 SFRs for management

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1. The TSF shall restrict the ability to **modify** the **D.RULE_SET and the rules for FAU_SAA** to **S.USER.**

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1. The TSF shall ensure that **D.RULE_SET has no rules for D.INBOUND traffic on installation.**[7]

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:
- **S.USER,**
- **S.OUTSIDE.**

FMT_SMR.1.2 The TSF shall be able to associate the users with roles **by the interface they use to communicate with the TOE**[8].

---

[7] This requirement was refined to show that it only applies to the TSF data "D.RULESET" and not to the TSF data "rules for FAU_SAA". It was also refined to show that it also applies only directly after installation.

The reason for this is that recent research has shown that unprotected PCs survive only a few minutes on the Internet. Therefore the firewall (and the platform) needs to be protected against these attacks immediately. S.USER can then customise the firewall rules and alarms as he wishes, but he is still protected while doing so.

FMT_MTD.3 will allow S.USER to configure the TOE to modes generally considered to be unsafe (e.g. allow everything and report nothing). This is covered by the AGD_ADM.1 component in EAL1. The administrator guidance will tell S.USER what the consequences of his modifications are and what modifications he should / should not make.

5.3 SFRs for logging and auditing

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) -[9]

c) All attempted violations of FDP_ACF.1

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

a) Date and time of the event[10], 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, **the following information will be recorded:**

- **Source address,**
- **Destination address,**
- **Source port,**
- **Destination port,**
- **Packet type.**

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:

- Accumulation or combination of [assignment: **user definable** subset of auditable events[11]] known to indicate a potential security violation;

---

[8] Typically S.USER will be associated with some sort of application or management interface, while S.OUTSIDE will use the network interface. Because of this requirement, FIA_UID has not been included.

[9] This element was first completed with "**not specified**" and subsequently refined away (editorial refinement).

[10] The TSF will obtain time-stamp information from the OS. This time information is not trusted since it is easy to modify on many computing environments.

- [assignment: any other rules].

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall[12] **warn S.USER** upon detection of a potential security violation **as indicated by FAU_SAA.1[13].**

5.4 SARs

The SARs for this PP are the package EAL 1.

[11] This requirement has been refined to show that the list is not static, but can be set by S.USER.

[12] Editorial refinement for readability

[13] This refinement shows the relation between FAU_SAA and FAU_ARP in this PP.