Low Assurance Protection Profile for a VPN gateway

Version:
1.4

Date:
29/04/2005

Filename:
lapp4_14

Product:
VPN gateway

Sponsor:
SRC Security Research & Consulting GmbH,
Graurheindorfer Straße 149a, D-53117 Bonn, Germany,
Phone: +49 (228) 2806-0, Fax: +49 (228) 2806-199

Certification ID:
BSI – PP-0013

Author(s):
Dirk Feldhusen
Sandro Amendola

No of pages:
12

Document Information

History of changes

Version	Date	Changes
0.1	30/08/2004	First Draft
0.2	03/09/2004	Updated version after internal revision
0.3	04/10/2004	Updated version after comments by BSI
0.4	08/10/2004	Updated version after further comments by BSI
0.5	12/10/2004	Updated version after some more comments by BSI
1.0	06/11/2004	Updated version after intermediate evaluation report by TNO
1.1	08/11/2004	Updated version after comments by TNO
1.2	09/11/2004	Updated version after one more comment by TNO
1.3	10/11/2004	Updated version after final comment by TNO
1.4	29/04/2005	Incorporated Raised Interpretations, added certification ID

Document Invariants

Name	Invariant (edit here)	Output value
Filename and size	calculated automatically	lapp4_14 (292864 Byte)
Last version	1.4	1.4
Date	29/04/2005	29/04/2005
Classification	Final	Final
TOE name (long)	VPN gateway	VPN gateway
TOE name (short)	VPN gateway	VPN gateway
Certification ID	BSI – PP-0013	BSI – PP-0013
Author(s)	Dirk Feldhusen Sandro Amendola	Dirk Feldhusen Sandro Amendola
Sponsor (long)	SRC Security Research & Consulting GmbH	SRC Security Research & Consulting GmbH
Sponsor (short)	SRC	SRC
Evaluation facility (long)	TNO-ITSEF BV Delftechpark 1 2628 XJ Delft The Netherlands	TNO-ITSEF BV Delftechpark 1 2628 XJ Delft The Netherlands
Evaluation facility (short)	TNO-ITSEF BV	TNO-ITSEF BV
Certification body (long)	Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185-189 53175 Bonn	Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185-189 53175 Bonn
Certification body (short)	BSI	BSI

Table of contents

1 PP Introduction

1.1 PP Reference

This is the Low Assurance Protection Profile for a VPN gateway, version 1.4, SRC Security Research & Consulting GmbH, 29/04/2005.

1.2 TOE overview

The TOE is a VPN gateway which is used to build up a virtual private network as depicted below. A Virtual Private Network, or VPN, is a private communication network communicating over a public network, i.e. the Internet. Normally, a local network is protected against unauthorised access from the public network by means of a firewall which limits the permitted types of traffic. The TOE provides a remote authorised users a full connection into the local network without bypassing this protection against unauthorised users.

This connection is established by a so called VPN tunnel between a VPN gateway on the side of the network and a VPN client on the side of the remote user, which is a reduced form of a gateway. Also two networks can be connected via two VPN gateways, in which case, one of the VPN gateways plays the role of the server and the other gateway plays the role of the client. There is no difference in the functionality offered by the VPN client irrespective of whether the remote VPN client is actually a single personal computer running a trusted VPN client software application or a VPN gateway device attached to a remote LAN.

The TOE provides the following functionality:

- identifying and authenticating remote VPN users or networks,
- building up VPN tunnels between the TOE and the VPN client by exchanging cryptographic keys and using agreed cryptographic algorithms and
- routing network traffic between the two sides of the VPN tunnel.

The VPN message traffic is carried on public networking infrastructure using standard protocols. VPNs use cryptographic tunnelling protocols to provide the necessary confidentiality (preventing snooping), sender authentication (preventing identity spoofing), and message integrity (preventing message alteration) to achieve the privacy intended. Such techniques can provide secure communications over possibly insecure networks.

Typical VPN protocols are:

- IPSec (IP security), the most common protocol specified by an IETF working group,
- OpenVPN, a SSL based encryption available for many operating systems,
- and proprietary protocols like
    - PPTP (point-to-point tunneling protocol) or
    - L2F (Layer 2 Forwarding) as well as
    - L2TP (Layer 2 Tunnelling Protocol).

The TOE requires a supporting computing platform equipped with a connection to the public network as well as the local network to provide its functionality.

Furthermore, the communication between the local network and the public network will be only through the TOE. This object will be supported by the use of a firewall that is configured to allow the minimum set of traffic to pass that is required for the operation of the TOE and any other services that are exposed to the outside world.

Further non-TOE hardware/firmware/software is not required by the TOE.

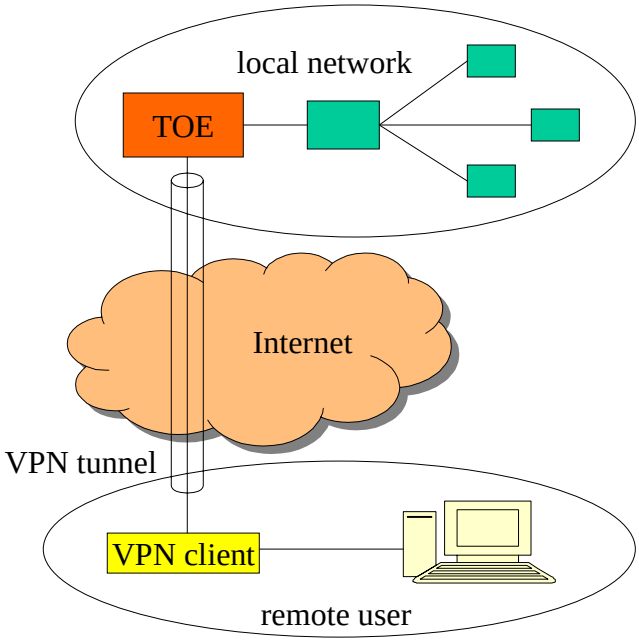

Figure 1 The TOE and its operational environment

2 Conformance claims

2.1 Conformance claim

This Protection Profile:

- claims conformance to CC version 2.4 release 256 and CC v2.4 Draft Interpretations #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

The conformance claim rationale consists in a PP-related conformance claim rationale and a package-related 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.

3 Definition of terms

This section is added to define the terms like subjects, objects and operations, that are used in the Security Objectives of the Operational Environment and SFRs.

3.1 Subjects

S.USER	user of the TOE, typically a remote user or an administrator of a remote network. attribute: data used for the authentication like for instance public Diffie-Hellman key.
S.ADMIN	administrator, authorised to modify the list of authorised users and administrating the corresponding security attributes of S.USER.

3.2 Objects

O.NETWORK	local network to which the TOE provides the connection.

3.3 Operations

R.CONNECT	establish connection between S.USER and the O.NETWORK by a so-called VPN tunnel.

4 Security Objectives

Security Objectives for the operational environment

OE.PRIV_DATA The private data belonging to the security attributes of S.USER, typically a Diffie-Hellman key pair, are generated and handled in a secure manner.

OE.CLIENT The remote user S.USER utilise a trusted IT product (VPN client or another VPN gateway) for the connection to the TOE.

OE.ADMIN The security attributes of S.USER, typically a public Diffie-Hellman key or a X.509 certificate, are adequately imported and handled by S.ADMIN. In addition, S.ADMIN shall keep the computing platform of the TOE integer. For these purpose he shall:

- update the computing platform with the latest patches and updates for this environment and
- downloading and running only executable content which does not corrupt the integrity of the computing platform.

OE.ENVIRON[1] The operational environment of the TOE shall be a general office environment. This means low physical security measures.

OE.NETWORK There will be no direct connection between O.NETWORK and the public network. Communication between the two will be only through the TOE. This object will be supported by the use of a firewall that is configured to allow the minimum set of traffic to pass that is required for the operation of the TOE and any other services that are exposed to the outside world.

[1] 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 Security Requirements

5.1 Extended components definition

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

5.2 SFRs

Authentication and Identification

Informal explanation: Authentication and identification is one of the two main security functionalities of the VPN gateway. The user must identify and authenticate on behalf a security attribute like a public key known to the TOE before gaining access to the network

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

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

Dependencies: No dependencies

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes **which can be used to authenticate S.USER**]

Informal explanation: Security attributes can be e.g. pre-shared secrets in form of public Diffie-Hellman keys according to IPSEC or X.509 certificates which contain such public keys stored by a PKI. This depends on the implementation of the TOE and is therefore left to the ST.

Dependencies: No dependencies

Application note: The security mechanisms used for authentication like e.g. Diffie-Hellman key exchange algorithm, should be specified by the security target[2]. They should be of reasonable strength in order to support the security functionality of the TOE. For instance, cryptographic operations specified in the security target along with the recommended key length should be resistant against known cryptanalytic techniques.

[2] Since the required security functionality can be provided by several cryptographic algorithms or possibly even other security mechanisms, they are not specified in the protection profile.

Management

Informal explanation: This functionality supports the authentication by maintaining the list of security attributes. The access to the list of security attributes of authorised users is restricted to an administrator.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **SFP_VPN**[3] to restrict the ability to **modify** the security attributes [assignment: list of security attributes **which can be used to authenticate S.USER**] to **S.ADMIN**.

Dependencies: **FDP_ACC.1 Subset access control**

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **SFP_VPN**[3] on **{S.USER, O.NETWORK, R.CONNECT}**.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **SFP_VPN**[3] to objects based on the following **{security attributes of S.USER}**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.USER is only allowed to R.CONNECT to O.NETWORK if it is identified and authenticated on behalf of its security attribute**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **None**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **None**.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **SFP_VPN**[3] to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **S.ADMIN** to specify alternative initial values to override the default values when an object or information is created.

[3] The Security Function Policy SFP_VPN is identified by the elements FDP_ACC.1.1 and FDP_ACF.1.1 and consists in the rules defined by the elements FDP_ACF.1.2, FMT_MSA.1.1, FMT_MSA.3.1 and FMT_MSA.3.2.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **administrating the list of authorised users by adding and deleting the users along with their corresponding security attributes**.

Dependencies: No Dependencies

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **S.USER and S.ADMIN**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

Trusted channel

Informal explanation: The trusted channel is the second of the two main security functionalities.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **both the TSF and the remote trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **R.CONNECT**.

Dependencies: No dependencies

Application note: The security mechanisms used for the trusted channel, like e.g. triple DES encryption, should be specified by the security target[2]. They should be of reasonable strength in order to support the security functionality of the TOE. For instance, cryptographic operations specified in the security target along with the recommended key length should be resistant against known cryptanalytic techniques.

Self-protection

Informal explanation: The self-protection of the TOE supports the other security functionalities.

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.

Dependencies: No dependencies

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.

Dependencies: No dependencies

5.3 SARs

The SARs for this PP are the package EAL 1.