BULL TRUSTWAY VPN APPLIANCE

ISO15408

Security Target

Version 1.6

TABLE OF CONTENTS

Acronyms 5
1 ST introduction 6
1.1 ST identification 6
1.2 ST overview 6
1.3 CC conformance 7
2 TOE DESCRIPTION 8
2.1 Introduction 8
2.2 TOE sub systems 8
2.2.1 General 8
2.2.2 TOE technical specifications 9
2.3 TrustWay VPN components 10
2.3.1 TVPN appliance 10
2.3.2 TVPN administration 11
2.3.2.1 TVPN administration station (TDM) 11
2.3.2.2 Local administration 11
2.3.3 TDM – TVPN communication 12
2.4 Security management 13
2.4.1 Network topology 13
2.4.2 Security domains 15
2.4.3 Tunnelling 15
2.4.4 Frames processing and filtering 16
2.4.5 Data securization systems keys 16
2.4.5.1 Systems keys renewal 16
2.4.6 TVPN operational states 17
2.5 TVPN audit capabilities 18
2.5.1 TVPN alarms 18
2.5.2 TVPN audit file 19
2.5.3 TVPN network supervision 19
3 TOE Security Environment 20
3.1 Assets to protect 20
3.2 Assumptions 20
3.3 Threats to Security 21
3.3.1 Threats to be countered by the TOE 21
3.4 Organisational Security Policies 22
4 Security Objectives 23
4.1 TOE Security Objectives 23
4.2 Security Objectives for the Operating Environment 25
5 IT Security Requirements 26
5.1 TOE Security Functional Requirements 26
5.1.1 SECURITY AUDIT (FAU) 26
5.1.1.1 FAU_ARP.1 Security alarms 26
5.1.1.2 FAU_GEN.1 Audit data generation 26
5.1.1.3 FAU_SAA.1 Potential violation analysis 27
5.1.1.4 FAU_SAR.1 Audit review 27
5.1.1.5 FAU_STG.1 Protected audit trail storage 28
5.1.2 CRYPTOGRAPHIC SUPPORT (FCS) 28
5.1.2.1 FCS_CKM.1 Cryptographic key generation 28
5.1.2.2 FCS_CKM.2 Cryptographic key distribution 28
5.1.2.3 FCS_CKM.4 Cryptographic key destruction 28
5.1.2.4 FCS_COP.1 Cryptographic operation 28
5.1.3 USER DATA PROTECTION (FDP) 29

5.1.3.1 FDP_ACC.2 (1) Complet access control....29
5.1.3.2 FDP_ACC.2 (2) Complet access control....29
5.1.3.3 FDP_ACF.1 (1) Security attribute based access control....29
5.1.3.4 FDP_ACF.1 (2) Security attribute based access control....29
5.1.3.5 FDP_IFC.1 Subset information flow control....30
5.1.3.6 FDP_IFF.1 Simple security attributes....30
5.1.3.7 FDP_RIP.1 Subset residual information protection....31
5.1.3.8 FDP_UCT.1 Basic data exchange confidentiality....31
5.1.3.9 FDP_UIT.1 Data exchange integrity....31
5.1.4 IDENTIFICATION AND AUTHENTICATION (FIA)....31
5.1.4.1 FIA_AFL.1 Authentication failure handling....31
5.1.4.2 FIA_ATD.1 User attribute definition....31
5.1.4.3 FIA_UAU.2 User authentication before any action....32
5.1.4.4 FIA_UID.2 User identification before any action....32
5.1.5 SECURITY MANAGEMENT (FMT)....32
5.1.5.1 FMT_MOF.1 Management of security functions behavior....32
5.1.5.2 FMT_MSA.1 Management of security attributes....32
5.1.5.3 FMT_MSA.3 Static attribute initialization....32
5.1.5.4 FMT_MTD.1 (1) Management of TSF data....33
5.1.5.5 FMT_MTD.1 (2) Management of TSF data....33
5.1.5.6 FMT_MTD.2 Management of limits on TSF data....33
5.1.5.7 FMT_SMR.1 Security roles....33
5.1.6 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)....33
5.1.6.1 FPT_STM.1 Reliable time stamps....33
5.1.6.2 FPT_TST.1 TSF testing....33
5.1.7 Trusted path (FTP)....34
5.1.7.1 FTP_TRP.1 Trusted path....34
5.1.8 Strength level for the Security Functional Requirements....34
5.2 TOE Security Assurance Requirements....34
6 TOE summary specification....35
6.1 TOE security functions....35
6.1.1 SF.CONFIDENTIALITY....35
6.1.1.1 SF.CONFIDENTIALITY.DATA....35
6.1.1.2 SF.CONFIDENTIALITY.ADDRESS....35
6.1.1.3 SF.CONFIDENTIALITY.CONFIGURATION....35
6.1.2 SF.INTEGRITY....36
6.1.2.1 SF.INTEGRITY.DATA....36
6.1.2.2 SF.INTEGRITY.TOE....36
6.1.2.3 SF.INTEGRITY.NETWORK....37
6.1.3 SF.CONTROL....37
6.1.3.1 SF.CONTROL.MESSAGE....37
6.1.3.2 SF.CONTROL.CORRESPONDANTS....37
6.1.3.3 SF.CONTROL.PORT....37
6.1.3.4 SF.CONTROL.LOCALFIREWALL....37
6.1.4 SF.KEYMANAGEMENT....38
6.1.5 SF.EVENT....38
6.1.6 SF.ACCESS PROTECTION....38
6.2 Assurance measures....38
7 PP claims....40
8 Rationale....41
8.1 Security Objectives Rationale....41
8.2 Security Requirements Rationale....44
8.3 TOE Summary specification rationale....47
8.4 Rationale for assurance requirements....52
8.5 Rationale for strength of function claim....52

References 53

Acronyms

ARP Address Resolution Protocol
CC Common Criteria
EAL Evaluation Assurance Level
ICMP Internet Control Message Protocol
IPSEC Internet Protocol Security
ISO International Standardization Organization
IT Information Technology
MTU Maximum Transmit Unit
PP Protection Profile
SF Security Function
SAR Security assurance requirements
SFP Security Function Policy
SFR Security functional requirements
SNMP Simple Network Management Protocol
SOF Strength of Function
ST Security Target
TCP Transmission Control Protocol
TOE Target of Evaluation
TSC TSF Scope of Control
TSF TOE Security Functions
TSFI TSF Interface
TSP TOE Security Policy
UDP User Datagram Protocol
VPN Virtual Private Network

1 ST introduction

1.1 ST identification

Title : BULL TrustWay VPN Appliance Security Target

Author : José Lavancier

Contributors : Nadine Fabiano , François Cunchon, René Martin, Ryo Watanabé

ST Version : 1.6, dated March 3rd , 2004

TOE Version : 3.01.06

TOE commercial name : BULL TrustWay VPN Appliance

1.2 ST overview

The aim of this document is to describe the Security Target of the BULL TrustWay VPN Appliance product.

With TrustWay, BULL has created a set of European network security products. The TrustWay Appliance family offers a range of custom designed "plug and play" devices targeted at specific security needs. Inside the Appliance range, TrustWay VPN is dedicated to providing a platform for creating trusted network infrastructures.

The TrustWay VPN Appliance rely on several elements (see figure 1). The TVPN (TrustWay Virtual Private NetWork) is a chassis which represents the linking points between the secured and open networks filtering and applying the security policy. The TDM (TrustWay Domain Manager) is a configuration and supervision tool necessary to define and apply the security policy on the different TVPNs by a secured proprietary protocol. The TDM also determines rules, checks the state of the virtual network and permits to up grade remotely the TVPN's and token 's softwares.

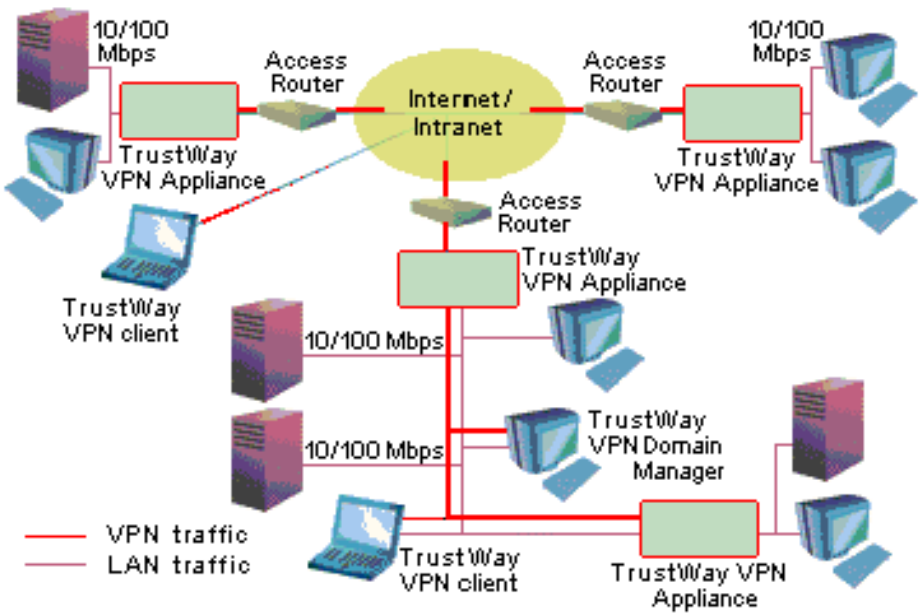


Fig1 : TrustWay VPN appliance : Architecture and Administration

The TOE is composed of the TrustWay VPN (TVPN) including the secured data exchange protocol with the network management utility (TDM TrustWay Domain Manager).

1.3 CC conformance

The ST is compliant to part 2 and part 3 of ISO 15408.

The assurance level for this ST is EAL2, augmented with ADV_HLD.2 (security enforcing high-level design), ALC_DVS.1 (identification of security measures), ALC_FLR.3 (systematic flow remediation), AVA_MSU.1 (examination of guidance), AVA_VLA.2 (independent vulnerability analysis), ADV_LLD.1 (descriptive low-level design), ADV_IMP.1 (subset of the implementation of the TSF) and ALC_TAT.1 (well-defined development tools).

Notes : ADV_LLD.1 (descriptive low-level design), ADV_IMP.1 (subset of the implementation of the TSF) and ALC_TAT.1 (well-defined development tools) are relative to TOE sub systems involved in cryptographic functions.

The minimum strength level for the TOE security functions is SOF-high for all the TOE security functions.

2 TOE DESCRIPTION

2.1 Introduction

A VPN provides the ability to use a public network, such as the Internet, as if it were a secure, private network. A VPN is created through the use of devices that can establish secure communication channels over a common, untrusted (or less trusted) communications infrastructure, protecting data in-transit between two communicating entities.

The TrustWay VPN offer is designed to provide virtual private networks between a number of sites using a public network such as the Internet. Since each unit can establish several hundred simultaneous tunnels, it will ensure the transfer of data while preserving the data's security and integrity.

Based on the standards defined by the IETF and using a line cutoff architecture, the TrustWay VPN offer can be easily integrated into all IP V4 networks without having to modify the existing addressing plan.

2.2 TOE sub systems

2.2.1 General

The TOE is made up of (see figure 2) :

- TVPN Software (including secure administrative dialog),
- The hard disk part containing TVPN data (e.g. audit file)
- The hardware token embedded software performing cryptographic operations (including trusted path for authentication).

The TOE concerns four operational modes of the TVPN : the drop mode, forward mode, the transport mode and the tunnel mode (implementation of the IPSEC protocol ESP).

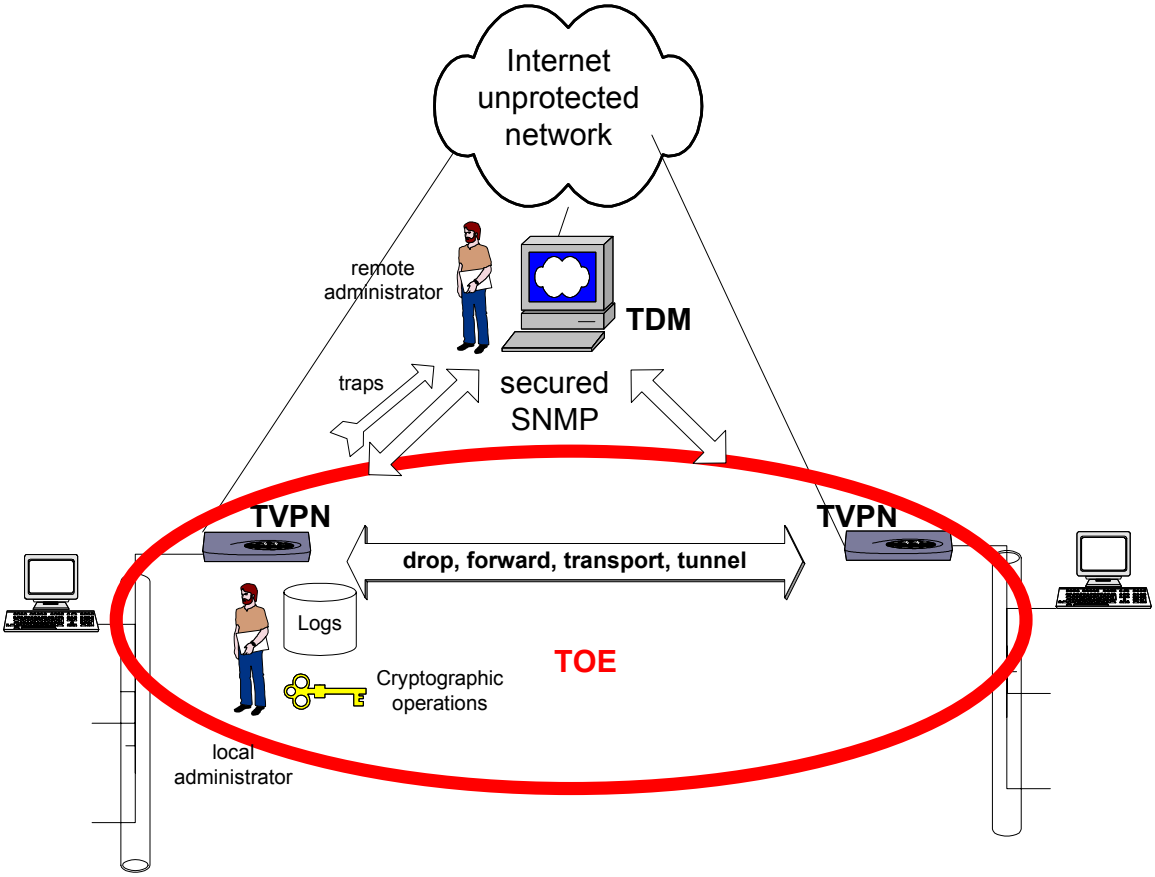


Fig2 : TOE boundaries

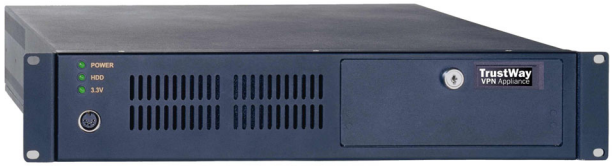
The following appliance part belongs to the TOE environment :

- the linux operating system (linx kernel 2.4.12)
- the filtering operations are managed by Netfilter utility (included in linux)
- Tripwire (version 2.2.1) product ensuring the integrity of files. TripWire is used to check the integrity according to 3 levels (3 frequencies). The first level checks the demons running on the TOE every minutes. The second level checks the configuration and permission files so as to the libraries. The third level checks TVPN, linux and Tripwire codes.
- The trusted channel (Safepad) to perform initial key distribution and authentication

2.2.2 TOE technical specifications

The TOE is physically represented by a chassis. This rack integrates the following elements :

- VIA C3 mainboard
- Celeron intel 800Mhz
- Hard disk fujitsu 20Go
- 128Mb SDRAM PC100
- hardware token (version 76677843-104A hardware – firmware)
- the power supplier



External interfaces :

- 2 ethernet interfaces PRO100 & REALTEK 8139
- Leds which indicate the chassis activity
- Serial port (used for local administration)

The hardware token indicates its state through the leds and provides a trusted path for authentication using a Safe Pad (a smart card reader).

Logical items included in the TOE are:

- The TVPN Software version 3.01.06
- The token embedded software performing cryptographic operations (version B005 software)
- The proprietary secured data exchange protocol (TDM - TVPN communication)
- Local administration means (through the serial port).

The TrustWay Domain Manager is not included in the TOE.

2.3 TrustWay VPN components

2.3.1 TVPN appliance

The appliance is based on a standard operating system: LINUX. The IPSec part is fully developed by BULL, thus offering complete control over the solution.

The chassis (including processor, hardware disk, CDROM, …) is manufactured by a supplier.

The cryptographic operations and the local authentication are performed by a high performance PCI interface based secure cryptographic hardware token developped by BULL.

Local access to the TVPN is protected by an authentication procedure. Authentification is performed on a trusted path using smart card technology.

2.3.2 TVPN administration

2.3.2.1 TVPN administration station (TDM)

The TDM (TrustWay Domain Manager) station acts as a remote TVPN administrator. It is based on a standard Windows operating system. A secure PCI hardware cryptographic token, developed by BULL, is plugged in the PCI bus.

The TDM configuration application is in charge of computing and sending TVPNs configuration. TDM offers a graphical view of both network topology and security rules (security policies) to apply between communicating systems.

TVPN configuration consists of:

- Security rules (security domains);
- Filtering options;
- TVPN network supervision configuration;
- Alerts management;
- Miscellaneous parameters (MTU, data compression, etc.).

TVPNs configuration is computed by TDM and conveyed to TVPNs using a secured SNMP link.

Access to TDM application is controlled through a smart card authentication procedure. Authentification itself is performed by the TDM hardware token, through a trusted path. The administration smart card is created by the TDM token during its installation phase. At this time the administrator can choose the PIN Code of the smart card.

Cryptographic operations relative to configuration are performed by TDM secure hardware cryptographic token.

2.3.2.2 Local administration

A local administrator role is defined for TVPN. The local administrator can access the audit file. This access is authorized by a secure Login via a serial port. The Login is protected by both a password (using the shadow password), and by a local smart card authentication with validation by PIN code (This is the only means of accessing and viewing the TVPN audit file).

TVPN secure installation is also performed by the local administrator using smartcard technology through the same trusted path (see below).

2.3.3 TDM – TVPN communication

TDM and TVPN communicate by way of a secure SNMP based proprietary protocol. This protocol, based on a shared secret, allows a mutual authentication between TDM and TVPN.

The shared secret is TVPN specific. It is generated by TDM token upon each TVPN object creation in graphical interface. This secret is securely stored in TDM token.

TDM generates a specific installation Smart Card for each configured TVPN. The TVPN associated secret is recorded on this Smart Card.
During TVPN installation procedure this secret is read from the smart card and stored into the TVPN cryptographic token.

Shared secrets never travel on the network.

Within each administrative dialog, the shared secred is used to transfer session keys, securizing configuration data transfer.

2.4 Security management

2.4.1 Network topology

The TVPN is oriented: it divides the topology of a network into a reliable network (safe and/or protected) and an unreliable network in the following way (see figure 3):

- Interface A: reliable network (unsecured traffic)

- Interface B: unreliable network (secured traffic)

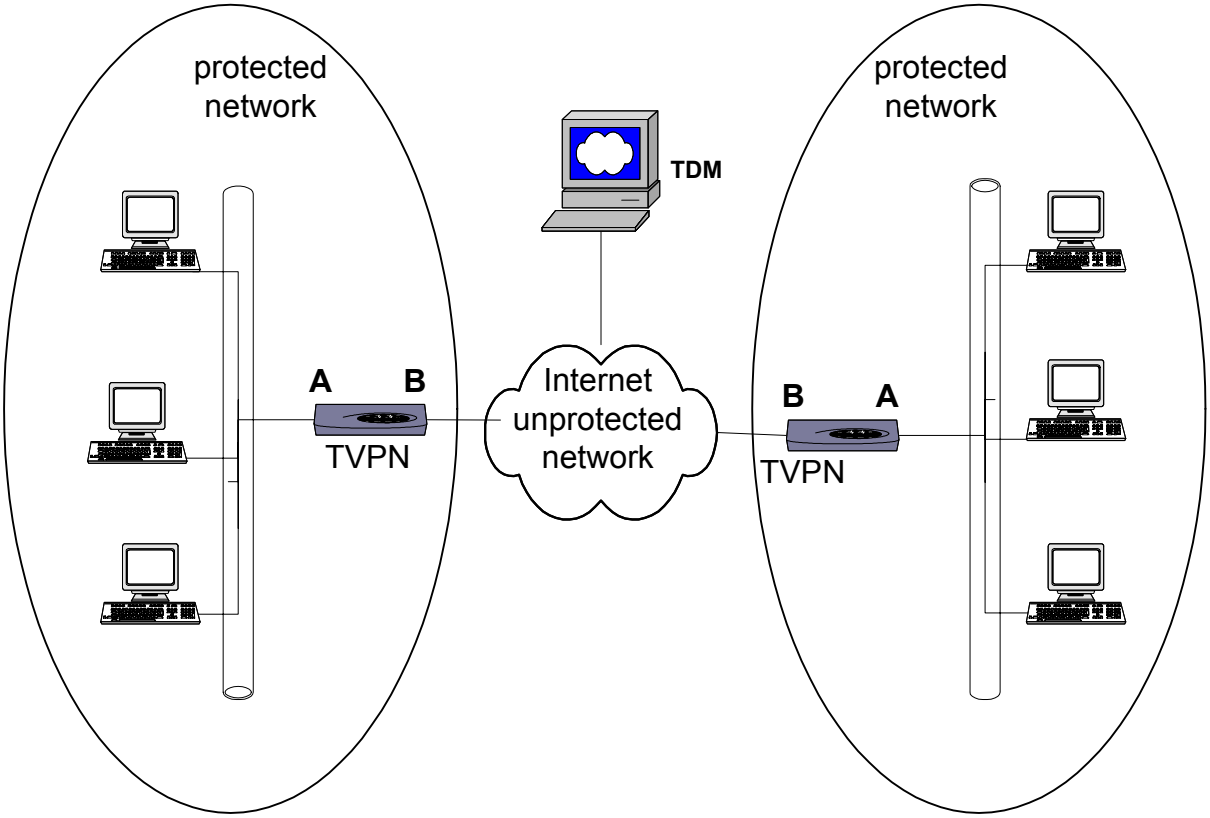


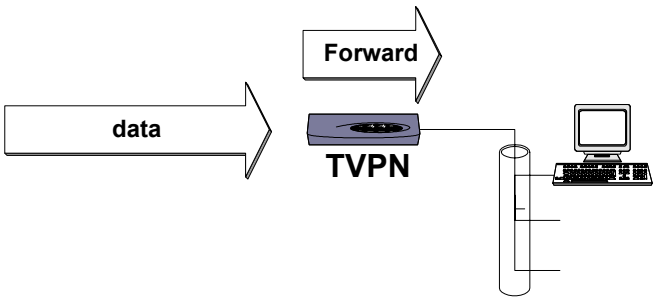
Fig 3 : General view of a network protected by TVPN boxes

The TVPNs will communicate in the mode corresponding to the security policy configured by TDM.

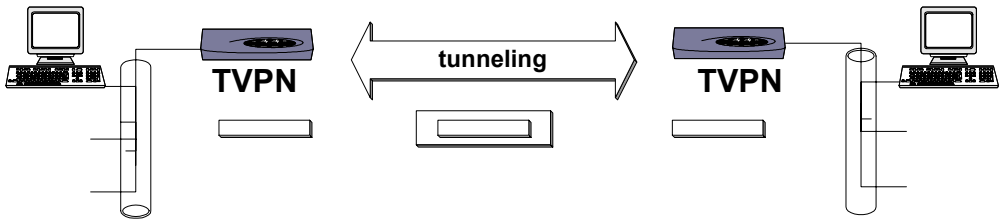
The following security policies are possible (from the least restricting to the most restricting) :

Security policy	Description
drop	Data dropped
Forward	Clear text communication
IPSEC-Authenticate	IPSEC tunnel (authentication only)
IPSEC-Transport	IPSEC transport (authentication and encryption)
IPSEC-Encrypt	IPSEC tunnel (authentication and encryption)

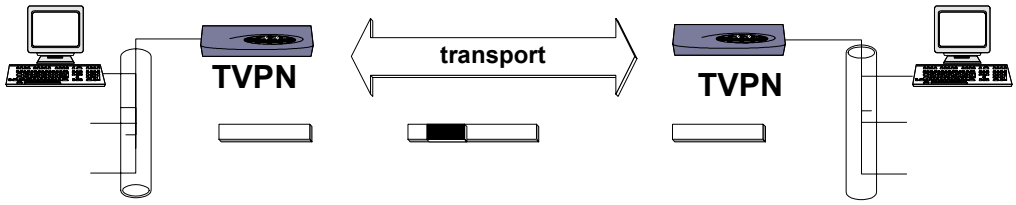
Forward mode : data are forwarded by configured TVPN equipments in clear text (clear text communication)



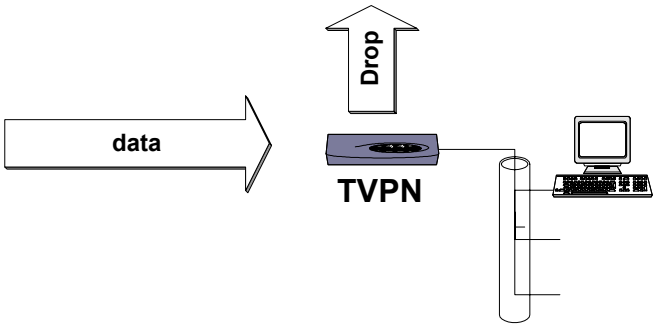
Tunnel mode : all the packets are encapsulated for the IPSEC exchange between TVPN equipments. So the packets are authenticated (and encrypted in the case of IPSEC-encrypted)



transport mode : all the packets for the IPSEC exchange between TVPN equipments are authenticated and encrypted (but not encapsulated).



Drop mode: when a packet arrives if no rule (about the source and destination) matches it (or if the drop rule is active) then the packet is dropped.



2.4.2 Security domains

The administrative view of security policies is obtained by defining security domains.

A security domain is a virtual space that groups a set of systems with the same security policy. The systems are necessarily machines or subnetworks installed on the reliable network (on the side of a TVPN where data appears in clear text) i.e. on interface A.

A TVPN only knows systems belonging to a security domain.

Only systems belonging to the same security domain are able to communicate. They communicate in the mode corresponding to the concerned domain security policy.

Systems protected by the same TVPN will communicate in clear text, whatever the domain's security policy.

2.4.3 Tunnelling

The TVPN implements the IPSEC protocol in tunnel mode.

The tunnels established between the various devices implement a 3DES CBC-mode encryption which ensures the flow's security, and a 128-bit HMAC MD5 signature for their integrity.

As opposed to the dynamic key negotiation technology, the mechanism involving a configuration by shared secret keys gives instant tunnel establishment times and supports architectures implementing load-balancing and backup mechanisms (VPNs 1.1.1 and 1.1.2 on figure 4).

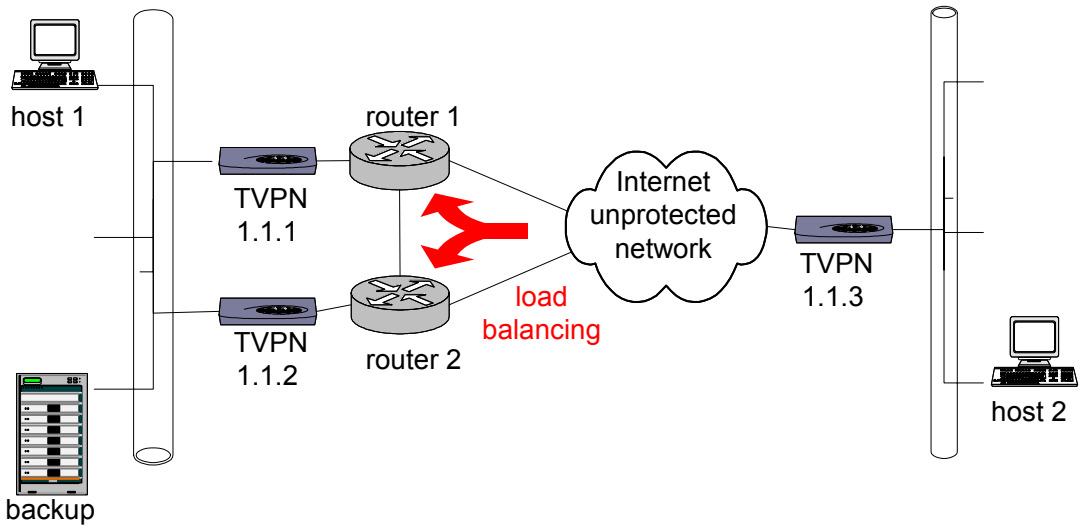


Fig 4 : General view of a network implementing load-balancing and backup

2.4.4 Frames processing and filtering

The configurated security policy is applied on TCP and UDP frames exchange between declared systems. An option regarding this flow can specify which action is to be performed (reject or transmit in clear text) on a frame when TVPN is unable to determine a security policy between the source and destination systems. It is the case when at least one system source or destination is not configured.

Additionnaly, given its line cutoff architecture [network interfaces in promiscuous mode], the unit has the capability to apply filters on all flows which traverse it. Frames sent specifically to TVPN are not concerned by filtering.

Filtering options are part of the configuration sent by TDM.

Following frames can be rejected or transmitted in clear text by the TVPN :

- ICMP
- TCP/BGP, UDP/RIP, UDP/BOOTP, UDP/DHCP
- Routing frames (GGP, EGP, IGP, HELLO, IGRP, OSPF)
- ARP and RARP

Furthermore an option can specify if these frames, when exchanged between configured systems, are encrypted or not (except for non IP frames ARP and RARP).

An option can specify which action is to be performed (reject or transmit in clear text) on a frame non-TCP, non-UDP and not listed above (for example ISO or IPX).

2.4.5 Data securization systems keys

Two keys are associated with each system created in the TDM configuration: the encryption key and the authentication key. These keys are generated by the TDM hardware token and are sent – in encrypted form –as part of TVPNs configuration.

The TVPN uses these systems keys to secure the flow between two systems.

2.4.5.1 Systems keys renewal

Two functions are available in TDM for systems keys renewal

Update configuration with new keys

It is possible to instantly modify current systems keys by updating configuration on TVPN.

TDM generates new systems keys and send the configuration with these new keys to all the TVPNs present in domains. Once TVPNs updated, news keys are immediately effective.

Change keys at specified date

It is possible to modify systems keys used by TVPN at a specified date. TDM generates new systems keys and sends them to all the TVPN. New keys are effective at the specified date.

2.4.6 TVPN operational states

As viewed from TDM application, a TVPN can have 3 distinct states.

The *installed* state corresponds to an operational TVPN which actions the rules issued according to domains security policies.

The *uninstalled* state corresponds to a TVPN temporary removed from network but which LAN is still connected to the network. In this case, its LAN can no longer communicate with LANs of other TVPN. This is the case, for example, of a TVPN sent to maintenance and which LAN flow shall be stopped because it is no longer securized. TDM no longer sends any configuration to this TVPN which can be considered as revoked.

The *transparent* state corresponds to a TVPN temporary removed from network but which LAN, still connected to the network, must communicate with LANs of other TVPNs. This is the case, for example, of a TVPN sent to maintenance and which LAN flow must continue in forward mode. In this case, its LAN communicate in clear text with LANs of other TVPN. TDM no longer sends any configuration to this TVPN but modifies other TVPNs configuration to apply a forward mode.

If a TVPN is removed from all security domains, then this TVPN will be revoked after updating configuration. Indeed all previous security rules on the TVPN are suppressed : then the action performed on any received frame is the one configured (drop or forward) in case of undetermined security policy. Furthermore the other TVPN don't have any rule applying to the systems protected by the revoked TVPN and so perform the default action (drop or forward) according to the configuration.

2.5 TVPN audit capabilities

2.5.1 TVPN alarms

Two types of alarms can be generated by TVPN:

- Alarms which triggering criteria can be configured

A threshold and a period are configured by TDM for each kind of alarm.

In TVPN, events related to the alarm are counted. When the counter becomes greater than or equal to a configured threshold TVPN triggers an alarm (sending of SNMP trap to TDM and supervisors) and the counter is reset to 0. At the end of the period the counter is also reset.

Events	Meaning
Frames in Overflow Eth.	Overflow in the number of Ethernet buffers, the frames will be dropped.
Unknown Protocol	Non TCP/IP or UDP/IP frames and frames never concerned by filtering(ex:ISO, IPX)
TCP and UDP checksum error (if checksum verification configured)	Checksum error for TCP or UDP frames.
MIB access	Attempt to access the secured MIB.
Frames in overflow DES	Overflow in the number of buffers for the DES encryption frames.
Dropped IP frames	IP frames dropped because of undefined security policy
Forbidden port	Attempt by an IP frame to access a destination port forbidden by configuration.
IPSEC authentication error	Error for IPSEC authentication.

TDM link events	Meaning
Authentication errors	Authentication errors between the TDM and the TVPN.
Failed Requests	Failed request due to an unauthorized access or a timeout overflow.
Integrity errors	Seal errors in the frames exchanged between the TVPN and the TDM.

- Alarms which are always sent when the associated event occurs

TDM link events	Meaning
TVPN Cold Start	Power on
TripWire alert	Error detected by TripWire (TVPN Functions survey)

2.5.2 TVPN audit file

Alarm sending is the way to signal that a particular event has occured and has been logged in the TVPN audit file.

Recorded events are :

- Start-up and shutdown of the audit functions;
- TVPN Cold Start
- Bad checksum from channel B
- IPSec authentication error
- Administrator authentication error
- Failed change key
- Unallowed port
- Error detected by TripWire (TVPN Functions survey)

Only the local TVPN administrator is allowed to access internal TVPN audit file through a secure path (see § Local administration).

2.5.3 TVPN network supervision

TDM offers the possibility to declare machines as network supervisors for a TVPN. These supervisors will receive TVPN SNMP traps.

If the option “Restrict MIB2 access to checked supervisors” is selected then only selected supervisors can query the non-secure MIB of this TVPN. Otherwise any machine can query the non-secure MIB of this TVPN.

TDM acts as a supervisor for all managed TVPNs. Received traps are logged by Windows SNMP trap service.

3 TOE Security Environment

3.1 Assets to protect

The primary assets that need to be protected by the TOE are the following:

TOE internal data:

- **R.USERDATA**: confidential exchanged user data have to be protected both in confidentiality and integrity.
- **R.KEYS** : session secret keys (encryption and authentication keys) and shared secrets have to be protected both in confidentiality and integrity.
- **R.MGMTDATA**: confidential configuration data (network configuration, security policy,audit files) have to be protected both in confidentiality and integrity.
- **R.SOFTWARE:** software parts of the TOE have to be protected in integrity.

Services ensured by the TOE:

- **R.SERVICES**: integrity and availability of the TOE services as well as protection against misuse is required.

3.2 Assumptions

A.CONFIGURATION

The TOE will be properly installed and configured according to the system administator's guide. Remote administrators are in charge of defining security domains and configure the TOE with the security policy. They are also in charge of securely stored and transmit the installation smart cards to the local administrators.

A.NO_EVIL

Authorized administrators are non-hostile, approprately trained and follow all administrator guidance.

A.CRYPTOGRAPHIC_DEVICE

Physical security mechanisms of the hardware token used by the TOE shall include hard opaque potting material, out-of-range voltage and temperature detection and tamper resistance.

3.3 Threats to Security

3.3.1 Threats to be countered by the TOE

The threats to be considered concern:

- information exchanged by users (peer TOEs)
- sensitive TOE configuration information (Security policy and network configuration)
- secret information (session keys, shared secrets)
- TOE security functions
- the client's addressing plan

The threat agents are unauthorized people (hackers for example) or external IT entities not authorized to access the TOE (in particular, administer the TOE).

T.DEFAULT_CONFIGURATION

A threat agent could send user-data while security policy of theTOE is not configured.

T.EXCHANGED_USER_DATA_DISCLOSURE

Disclosure of exchanged user data by IP address impersonation, attacks against confidentiality of exchanged data without knowledge of secrets (IPSEC-Transport and IPSEC-Encrypt security policies only), TOE theft in order to compromise the remainder of the secure network.

T.INTERNAL_USER_DATA_DISCLOSURE

Clear user data recorded in the TOE (hard disk) can be read by an attackant in case of TOE theft.

T.USER_DATA_FORGERY

Alteration of exchanged user data by modifying secure data transmitted (IPSEC-Authenticate, IPSEC-Transport and IPSEC-Encrypt security policies).

T.FALSE_FRAME_INJECTION

Injection of data by a hacker between the TOE and a remote TVPN (or the TDM) with a view to being delivered to the protected recipient (IPSEC-Authenticate, IPSEC-Transport and IPSEC-Encrypt security policies).

T.USER_ADDRESS_DISCLOSURE

Analysing secured data, disclosure of the addressing plan of protected networks to aid the preparation of attack scenarios (IPSEC-Encrypt security policy only).

T.KEYS_DISCLOSURE

Disclosure of session keys and shared secrets to disclose or alter secure data exchanged, or to inject false data to be received by the user, thru TOE theft or administration dialog analysis.

T.KEYS_FORGERY

Alteration of session keys and shared secrets to disclose or alter secure data exchanged, or to inject false data to be received by the user, thru TOE theft or administration dialog analysis.

T.SENSITIVE_DATA_DISCLOSURE

Disclosure of the security policy to aid the preparation of attack scenarios, thru TOE theft or administration dialog analysis.

T.SENSITIVE_DATA_FORGERY

Alteration of the security policy to alter secure data exchanged, or to inject false data to be received by the user, thru TOE theft or administration dialog analysis.

T.FUNCTIONS_FORGERY

Alteration of the software that implements the TOE security functions to alter the secure data exchanged, or to inject false data to be received by the user, thru Admininistration Card theft and Login password disclosure or TOE theft.

T.AUDIT

Attacks on secure elements not reported by the TOE. An attacker can access the audit files in order to read, modify or delete them, thru Admininistration Card theft and Login password disclosure or TOE theft.

3.4 Organisational Security Policies

P.ADMINISTRATION

Authorized Administrators shall administer the TOE locally or remotely (with the TDM) through protected communications channels.

P.AUDIT_REVIEW

The administrator shall analyse regularly the log files. He can detect any attack and check the coherence of the events logged (that is to say the events are well recorded).

4 Security Objectives

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

4.1 TOE Security Objectives

O.DEFAULT_SECURITY_POLICY

The default security policy is drop : all data are dropped on channel A and channel B.

O.CONFIDENTIALITY_EXCHANGED_USER_DATA

The TOE shall ensure the confidentiality of data exchanged by the users (IPSEC-Transport and IPSEC-Encrypt security policies only).

O.CONFIDENTIALITY_INTERNAL_USER_DATA

Clear flows only travel in the memory in the TOE (no file writing on the hard disk) in order not to compromise the remainder of the secure network in case of TOE theft.

O.INTEGRITY_EXCHANGED_USER_DATA

The TOE shall ensure that the data exchanged can not be altered (IPSEC-Authenticate, IPSEC-Transport and IPSEC-Encrypt security policies). If alteration of user data is detected, the corresponding data are dropped and the event is logged.

O.AUTHENTICATION_USER_DATA

The TOE shall ensure the authentication of secure data exchanged to guarantee that the remote peer TOE sending data is indeed the corresponding TOE (IPSEC-Authenticate, IPSEC-Transport and IPSEC-Encrypt security policies).

O.HANDLE

The TOE shall handle the flow of information between peer TOEs in accordance with its security policy.

O.CONFIGURATION_PROTECTION

The TOE's network behavior (routing of secure and clear flows) may only be viewed and/or modified by remote authorized administrators (IPSEC-Encrypt security policy only). Only remote authorized administrators can view and/or modify the security policy. The TOE shall hide the secure network's addressing plan.

O.KEY_PROTECTION

Keys (session keys and shared secrets) shall never be retrieved from the TOE or altered inside the TOE. For this reason, The keys are generated and stored in a hardware token. The TOE shall ensure the secure exchange of keys :

- by cryptographic functions for the session keys
- by a physical trusted path for the shared secrets.

O.SECURE_ADMINISTRATIVE_DIALOG

The TOE shall supply confidentiality and integrity services to ensure protection of the administrative dialog with the TDM.

O.TRIPWIRE

The TOE shall use Tripwire to perform software integrity verifications.

O.AUDIT

Security events will be recorded in an audit file. They will increment viewable statistic counters and can trigger alarms. Only authorized users can read audit files. The audit files are regularly analyzed.

4.2 Security Objectives for the Operating Environment

OE.CONFIGURATION

The TOE, including the underlying linux operating system and hardware, shall be installed, administered, and maintained (i.e., security-related hardware and software fixes) in a manner that preserves the integrity and confidentiality of TOE data (e.g., configuration data, administrative data, etc.) and data traversing the TOE.

OE.NO_EVIL

Authorized Administrators are non-hostile, appropriately trained and follow all administrator guidance.

OE.ADMINISTRATION

The TDM shall be protected by physical and logical protection measures and the TDM usage shall be restricted to authorised persons only. TOE installation smart cards shall be securely stored and securely sent to the TOE local administrators. The security policy of the general network shall be appropriatly defined and the TOE correctly configured with this policy. The TDM shall supply confidentiality and integrity services to ensure protection of the administrative dialog with the TOE.

OE.KEY_MANAGEMENT

The TOE shall use systems keys created in the TDM to secure the flow between itself and the other systems. All sensitive data shall be sent in encrypted form as part of the TOE and (of the other systems) configuration. Systems keys renewal can be performed at any time or at a specified date by configuration updating of the TOE (and of the other systems).

OE.INTEGRITY_FUNCTIONS

The TOE shall perform correct configuration of Tripwire which periodically verifies the integrity of the software applications that implement the TOE's security functions.

5 IT Security Requirements

This chapter gives the security functional requirements (SFR) and the security assurance requirements (SAR) for the TOE and the environment.

Security functional requirements components given in section 5.1 “TOE security functional requirements” are drawn from Common Criteria part 2 [1].

The TOE security assurance requirements statement given in section 5.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [2].

5.1 TOE Security Functional Requirements

5.1.1 SECURITY AUDIT (FAU)

5.1.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 – The TSF shall take [generate an SNMP trap (clear mode) towards the TDM] upon detection of a potential security violation.

5.1.1.2 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 *minimum* level of audit; and

c) - TVPN Cold Start
- Bad checksum from interface B
- IPSec authentication error
- Administrator authentication error
- failed key change
- Unallowed port
- Error detected by TripWire (TVPN Functions survey)

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 ST, [information specified in column two of Table 5.1].

Auditable Event	Additional Audit Record Contents
TVPN Cold Start	No additional content
Bad checksum from interface B	The address of the source and destination subject.
IPSec authentication error	The address of the source and destination subject.
Administrator authentication error	No additional content
failed change key	Reason code
Unallowed port	The port number and the address of the source subject.
Error detected by TripWire (TVPN Functions survey)	Reason code

Table 5.1 - Auditable Events

5.1.1.3 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 [
- Bad checksum from interface B
- IPSec authentication error
- Unallowed port]

known to indicate a potential security violation;

b) [no other rules].

5.1.1.4 FAU_SAR.1 Audit review

FAU_SAR.1.1 - The TSF shall provide [an Authorized Administrator] with the capability to read [all audit data] from the audit records.

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

5.1.1.5 FAU_STG.1 Protected audit trail storage

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

FAU_STG.1.2 - The TSF shall be able to *prevent* modifications to the audit records.

5.1.2 CRYPTOGRAPHIC SUPPORT (FCS)

5.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 - The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [random number hardware generator] and specified cryptographic key sizes [that are 192 binary digits in length] that meet the following: FIPS PUB 186-2 REV01 (05/10/2001), appendix 3.1.

5.1.2.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 - The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [secure key distribution method based on smart card] that meets the following: [none].

5.1.2.3 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 - The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization] that meets the following: [FIPS140-2, Section 4.7.6, Key Zeroization].

5.1.2.4 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 / ENCRYPT - The TSF shall perform [encryption] in accordance with a specified cryptographic algorithm [TDES CBC] and cryptographic key sizes [that are 192 binary digits in length] that meet the following: [RFC 2451 : The ESP CBC-Mode Cipher Algorithms (November 1998)].

FCS_COP.1.1 / DECRYPT - The TSF shall perform [decryption] in accordance with a specified cryptographic algorithm [TDES CBC] and cryptographic key sizes [that are 192 binary digits in length] that meet the following: [RFC 2451 : The ESP CBC-Mode Cipher Algorithms (November 1998)].

FCS_COP.1.1 / HMAC - The TSF shall perform [secure hash of network traffic] in accordance with a specified cryptographic algorithm [HMAC MD5] and cryptographic key sizes [128 bits] that meet the following: [RFC 2404 : Use of HMAC MD5 within ESP (November 1998)].

5.1.3 USER DATA PROTECTION (FDP)

5.1.3.1 FDP_ACC.2 (1) Complet access control

FDP_ACC.2.1 - The TSF shall enforce the [external IT entities access control SFP] on :

a) [subjects: external IT entities that send and receive information through the TOE to one another;

b) objects : customer data flow traffic through the TOE]

FDP_ACC.2.2 - The TSF shall ensure that all operations between any subject in the TSC and any object between the TSC are cevered by an access control SFP.

5.1.3.2 FDP_ACC.2 (2) Complet access control

FDP_ACC.2.1.- The TSF shall enforce the [remote administration access control SFP] on :

c) [subjects: remote administration;

d) objects : security policy].

FDP_ACC.2.2 - The TSF shall ensure that all operations between any subject in the TSC and any object between the TSC are cevered by an access control SFP.

5.1.3.3 FDP_ACF.1 (1) Security attribute based access control

FDP_ACF.1.1 - The TSF shall enforce the [external IT entities access control SFP] to object based on [information security attributes].

FDP_ACF.1.2 – The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [information security attributes verification].

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]

5.1.3.4 FDP_ACF.1 (2) Security attribute based access control

FDP_ACF.1.1 - The TSF shall enforce the [remote administration access control SFP] to object based on [secure proprietary authentication protocol].

FDP_ACF.1.2 – The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [authorize the remote administration].

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]

5.1.3.5 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 - The TSF shall enforce the [VPN access policy including drop, forward, IPSec_Authenticate, IPSec-Transport, IPSec-Encrypt] on:

e) [subjects: external IT entities that send and receive information through the TOE to one another;

f) information: customer data flow traffic through the TOE

g) operation: apply filters based on data flow types, pass encrypted information based on destination and source IP addresses and pass unencrypted (i.e., plain text) information based on destination and source IP addresses].

5.1.3.6 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 - The TSF shall enforce the [VPN access policy including drop, forward, IPSec_Authenticate, IPSec-Transport, IPSec-Encrypt] based on the following types of subject and information security attributes:

a) [Subject security attributes:

- external IT entities that send and receive information through the TOE to one another source address;

b) Information security attributes:

- address of source subject;

- address of destination subject; and

- data flow types (ISO, ARP, ICMP type, UDP port, IP protocol].

FDP_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:
[According to security attributes defined in FDP_IFF.1, data flow traffic can be :

- dropped (default security policy)
- forwarded
- secured].

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP_IFF.1.5 -The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules: [none].

5.1.3.7 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 – The TSF shall ensure that any previous information content of a resource is made unavailable upon [the deallocation of the resource] from the following objects : [Clear data flows].

5.1.3.8 FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 – The TSF shall enforce the [information flow control SFP] to be able to [transmit or receive] objects in a manner protected from unauthorized disclosure.

5.1.3.9 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 – The TSF shall enforce the [information flow control SFP] to be able to [transmit or receive] objects in a manner protected from [modification,insertion] errors.

FDP_UIT.1.2 – The TSF shall be able to determine on receipt of user data, whether [modification,insertion] has occured.

5.1.4 IDENTIFICATION AND AUTHENTICATION (FIA)

5.1.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 - The TSF shall detect when [1] unsuccessful authentication attempts occur related to [local authentication of Authorized Administrators].

FIA_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [generate an audit record].

5.1.4.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users : [identity and role]

5.1.4.3 FIA_UAU.2 User authentication before any action

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

5.1.4.4 FIA_UID.2 User identification before any action

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

5.1.5 SECURITY MANAGEMENT (FMT)

5.1.5.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 - The TSF shall restrict the ability to *determine and modify the behavior of* the functions:

- SF.CONTROL.CORRESPONDANTS;
- SF.CONTROL.PORT;
- SF.CONTROL.LOCALFIREWALL ;

to [an Authorized Administrator].

5.1.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 - The TSF shall enforce the [VPN access policy] to restrict the ability to *modify, delete* or [create] the security attributes [information flow rules in FDP_IFF.1] to [an Authorized Administrator].

5.1.5.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 - The TSF shall enforce the [VPN access policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 - The TSF shall allow the [Authorized Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.4 FMT_MTD.1 (1) Management of TSF data

FMT_MTD.1.1 - The TSF shall restrict the ability to *modify, delete* and [assign] the [authentication data in FIA_ATD.1] to [an Authorized Administrator].

5.1.5.5 FMT_MTD.1 (2) Management of TSF data

FMT_MTD.1.1 - The TSF shall restrict the ability to [set] the [time and date used to form the timestamps in FPT_STM.1] to [an Authorized Administrator].

5.1.5.6 FMT_MTD.2 Management of limits on TSF data

FMT_MTD.2.1 - The TSF shall restrict the specification of [the time interval used for self-testing] to [an Authorized Administrator].

FMT_MTD.2.2 - The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [Self testing].

5.1.5.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 - The TSF shall maintain the roles [Authorized Administrator].

FMT_SMR.1.2 - The TSF shall be able to associate users with the Authorized Administrator role.

5.1.6 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

5.1.6.1 FPT_STM.1 Reliable time stamps

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

5.1.6.2 FPT_TST.1 TSF testing

FPT_TST.1.1 - The TSF shall run a suite of self tests [during initial start-up, periodically during normal operation and at the request of the Authorized Administrator*]* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 - The TSF shall provide Authorized Administrators with the capability to verify the integrity of TSF data.

FPT_TST.1.3 - The TSF shall provide Authorized Administrators with the capability to verify the integrity of stored TSF executable code.

5.1.7 Trusted path (FTP)

5.1.7.1 FTP_TRP.1 Trusted path

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

FTP_TRP.1.2 – The TSF shall permit [local users] to initiate communication via the trusted path.

FTP_TRP.1.3 - The TSF shall require the use of the trusted path for [initial user authentication and TOE initialisation]

5.1.8 Strength level for the Security Functional Requirements

The minimum strength level for the FIA_UAU specific TOE Security Functional Requirements is SOF-high. This function strength is demonstrated in the document " Analyse des vulnérabilités de l'appliance TrustWay VPN v1.0".

5.2 TOE Security Assurance Requirements

The assurance requirements for EAL2, augmented with ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2, ADV_LLD.1, ADV_IMP.1, ALC_TAT.1 are listed in the Table 5.2 below.

Notes : ADV_LLD.1, ADV_IMP.1 and ALC_TAT.1 are relative to TOE sub systems involved in cryptographic functions.

Table 5.1 Assurance Requirements: EAL 2 augmented

Assurance Class	Assurance Components
ACM	ACM_CAP.2
ADO	ADO_DEL.1 ADO_IGS.1
ADV	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 ADV_RCR.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1, ALC_FLR.3 ALC_TAT.1
ATE	ATE_COV.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.1, AVA_SOF.1 AVA_VLA.2

6 TOE summary specification

6.1 TOE security functions

6.1.1 SF.CONFIDENTIALITY

6.1.1.1 SF.CONFIDENTIALITY.DATA

SF.CONFIDENTIALITY.DATA.PROTOCOL

The TOE shall support the IETF *Internet Protocol Security Encapsulating Security Payload* (IPSEC ESP) in Tunnel Mode as specified in RFC2406. The TOE shall utilize, at a minimum, the Triple DES (3DES) algorithm as specified in ESP CBC-Mode Cipher Algorithms (RFC 2451). The Key used is a 192-bit length key.

SF.CONFIDENTIALITY.DATA.NOFILE

Clear flows only travel in the memory in the TOE (no file writing).

SF.CONFIDENTIALITY.DATA.PROTECTION

3DES cryptographic operations (along with HMD5 operations) are performed in a hardware token including hard opaque potting material and out of range voltage and temperature detections.

6.1.1.2 SF.CONFIDENTIALITY.ADDRESS

The secure network's addressing is hidden by the use of IPSEC tunnels and by the fact that the TOE can be configured so that the flows are encrypted or dropped.

6.1.1.3 SF.CONFIDENTIALITY.CONFIGURATION

Secret elements (keys) are stored in a hardware token.

Sensitive elements (security configuration) are stored in an encrypted 192-bit 3DES file and signed by 128-bit HMAC-MD5. The encryption and signature are performed by the hardware token.

6.1.2 SF.INTEGRITY

6.1.2.1 SF.INTEGRITY.DATA

SF.INTEGRITY.DATA.PROTOCOL

The TOE shall support the IETF Internet Protocol Security Encapsulating Security Payload (IPSEC ESP) in Tunnel Mode as specified in RFC2406. Sensitive information transmitted to a peer TOE shall apply integrity mechanisms as specified in *Use of HMAC-MD5 within ESP* (RFC 2404). The Key used is a 128-bit length key. The signature used in IPSEC is 128 bits long.

SF.INTEGRITY.DATA.FAILURE

Failure to authenticate a message initiates:

- the destruction of the message;
- the recording of the event in the audit file ;
- the incrementation of a statistic counter;
- the sending of an alarm (SNMP trap) if the configuration requests

SF.INTEGRITY.DATA.CHECKSUM

The TOE can be set up so as to verify the checksum of TCP/UDP/ICMP frames.

The verification's failure initiates:

- the destruction of the message;
- the recording of the event in the audit file ;
- the incrementation of a statistic counter ;
- the sending of an alarm (SNMP trap) if the configuration requests.

6.1.2.2 SF.INTEGRITY.TOE

Software applications that implement the TOE's functions and that handle sensitive data are checked on a regular basis during operation. This is done by Tripwire which is configured and launched by the TOE. The detection of any alteration triggers an alarm and an entry in the log file.

The TOE's operational events that handle secret data (keys) are implemented in a hardware token.

Functions that check the use of the memory are included in the elements with sensitive operational security to prevent attacks via the network. If an anomaly is detected in the memory's use, the TOE is rebooted.

Still with a view to counter network attacks, only essential Linux functions are present or enabled. In particular, the TCP flow is stopped upstream of the IP layer.

6.1.2.3 SF.INTEGRITY.NETWORK

The TOE does not allow unauthorized users to modify its network behavior (routing tables). In particular, the ICMP Redirect message is not accepted. The TOE does not contain any dynamic routing mechanisms.

6.1.3 SF.CONTROL

6.1.3.1 SF.CONTROL.MESSAGE

The TOE can be configured to disable the transmission of non encrypted data.

6.1.3.2 SF.CONTROL.CORRESPONDANTS

Secure communications will only be possible between systems authorized to communicate with one another.

This ban is ensured by the integrity and security afforded by the IPSEC Tunnel mode and by the security domain concept (set of systems authorized to communicate and sharing the same security policy).

If the security policy is not configured, the TOE dropped all the user data.

6.1.3.3 SF.CONTROL.PORT

The TOE can apply a filter on the recipient ports of the TCP/UDP frames after decryption. The check's failure initiates:

- the destruction of the message;
- the recording of the event in the audit file ;
- the incrementation of a statistic counter;
- the sending of an alarm (SNMP trap) if the configuration requests.

6.1.3.4 SF.CONTROL.LOCALFIREWALL

The TOE is equipped with an internal firewall which limits its access via the network only to machines whose addresses are configured and to ports necessary for the TOE's operation. This does not concern the flows that pass via the TOE.

6.1.4 SF.KEYMANAGEMENT

TOE correspondents use one different encryption key per pair of corresponding protected systems.

The TOE provides functions for changing encryption keys and authentication on request. There are no limits as to the number of changes required.

The keys are generated and stored in a hardware token (keys are generated according an approved generation method, are stored in a protected memory and cannot be retrieved in clear) .

The TOE unit is fitted with an opening detection device. If opened, the secret data (keys) in the TOE are destroyed. This is done via a contact between the opening detection device and the hardware token.

6.1.5 SF.EVENT

Counters representing the TOE's activity are maintained by the TOE and enable the sending of alarms if the configuration requires. The event is traced in a log file.

6.1.6 SF.ACCESS PROTECTION

Access to internal TOE data (including audit data) is authorized by a secure Login via a serial port. This Login is protected at the same time by password (using the shadow password), and by the insertion - in the reader - of an administration smart card with validation by PIN code. This is the only means of accessing and viewing the TOE's internal sensitive data.

The strength of the function is SOF-high.

6.2 Assurance measures

Appropriate assurance measures will be employed to satisfy the security assurance requirements. The evaluation will confirm whether the assurance measures are sufficient to satisfy the assurance requirements. The assurance measures will consist of the set of evaluation evidence listed in Table 6.1, below. The documents listed in the table will be used as to satisfy assurance evaluation requirements.

Table 6-1 Assurance evaluation evidence

Components	Delivrables
ACM_CAP.2	Environnement de développement du TVPN et de la carte PCA3 v1.2 Processus de développement du TVPN v1.1 Processus de développement de la carte PCA3 v1.1 Procédure documentation pour les cartes PCA3 v5.0 TVPN 3.01.06 Outillage et paquetage linux Liste de configuration de l'appliance TrustWay VPN v1.0
ADO_DEL.1	Processus de livraison de l'appliance TrustWay VPN v1.0 Création du TrustWay VPN à l'usine d'angers v5.0 Personnalisation des cartes CC2000 à l'usine d'Angers v4.0
ADO_IGS.1	Manuel d'installation et d'utilisation TrustWay Domain Manager v8.0 Manuel d'installation et d'utilisation TrustWay VPN/devices v3.1
ADV_FSP.1	Spécifications fonctionnelles de sécurité de l'appliance TrustWay VPN v1.1
ADV_HLD.2	Spécifications globales de l'appliance TrustWay VPN v1.1
ADV_LLD.1	Architecture du logiciel de la carte PCA3 v1.1 Carte PCA3 : Spécifications matérielles v1.3 Carte PCA3 : Visibilité micrologicielle v1.3
ADV_IMP.1	Implémentation de la carte PCA3 v1.0
ADV_RCR.1	Spécifications fonctionnelles de sécurité de l'appliance TrustWay VPN v1.1 Spécifications globales de l'appliance TrustWay VPN v1.1 Implémentation de la carte PCA3 v1.0
AGD_ADM.1	Manuel d'installation et d'utilisation TrustWay Domain Manager v8.0
AGD_USR.1	Manuel d'installation et d'utilisation TrustWay VPN/devices v3.1
ALC_DVS.1	Procédure de sécurité pour le développement des appliances TrustWay v1.0
ALC_FLR.3	Environnement de développement du TVPN et de la carte PCA3 v1.2 Processus de développement du TVPN v1.1
ALC_TAT.1	Environnement de développement du TVPN et de la carte PCA3 v1.2
ATE_COV.1	Tests de la carte PCA3 v1.0 TVPN 3.01.06 Tests de sécurité v2.0 Tests du chiffrement et de l'authentification IPSEC TVPN v1.0
ATE_FUN.1	Tests de la carte PCA3 v1.0 TVPN 3.01.06 Tests de sécurité v2.0 Tests du chiffrement et de l'authentification IPSEC TVPN v1.0
ATE_IND.2	Performed by the evaluator
AVA_MSU.1	Manuel d'installation et d'utilisation TrustWay Domain Manager v8.0 Manuel d'installation et d'utilisation TrustWay VPN/devices v3.1
AVA_SOF.1	Analyse des vulnérabilités de l'appliance TrustWay VPN v1.0
AVA_VLA.2	Analyse des vulnérabilités de l'appliance TrustWay VPN v1.0

7 PP claims

This security target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

DEFAULT_SECURITY_POLICY

This component ensures that a security policy is always configured in theTOE. This component is met by the following objectives : O.DEFAULT_SECURITY_POLICY.

T_ EXCHANGED_USER_DATA _DISCLOSURE

This component protects against disclosure of exchanged user data. This component is met by the following objectives : O.CONFIDENTIALITY_EXCHANGED_USER_DATA (user data protection), O.HANDLE (security policy application), O.CONFIGURATION_PROTECTION (security policy protection) and O.KEY_PROTECTION (keys protection)

T_ INTERNAL_USER_DATA _DISCLOSURE

This component ensures that clear user data recorded in the TOE cannot be read by an attackant. This component is met by the following objective : O.CONFIDENTIALITY_INTERNAL_USER_DATA.

T_ USER_DATA _FORGERY

This component protects against alteration of exchanged user data. This component is met by the following objectives : O.INTEGRITY_USER_DATA (user data protection), O.HANDLE (security policy application), O.CONFIGURATION_PROTECTION (security policy protection), O.KEY_PROTECTION (keys protection), O.TRIPWIRE and OE.INTEGRITY_FUNCTIONS (software applications aprotection).

T_FALSE_FRAME_INJECTION

This component protects against injection of data by a hacker between the TOE and a remote**.** This component is met by the following objectives : O.AUTHENTICATION_USER_DATA (user data protection), O.HANDLE (security policy application) and O.KEY_PROTECTION (keys protection).

T_ USER_ADDRESS_DISCLOSURE

This component protects against disclosure of the addressing plan. This component is met by the following objectives : O.CONFIGURATION_PROTECTION (security policy protection), O.TRIPWIRE and OE.INTEGRITY_FUNCTIONS (software protection).

T_ KEYS_DISCLOSURE

This component protects against disclosure of session keys. This component is met by the following objectives : O.KEY_PROTECTION (keys protection in the hardware token) and O.SECURE_ADMINISTRATIVE_DIALOG (secure administrative dialog).

T_KEYS_FORGERY

This component protects against alteration of session keys. This component is met by the following objectives O.KEY_PROTECTION (keys protection in the hardware token) and O.SECURE_ADMINISTRATIVE_DIALOG (secure administrative dialog).

T_SENSITIVE_DATA_DISCLOSURE

This component protects against disclosure of the security policy. This component is met by the following objectives : O.CONFIGURATION_PROTECTION (security policy protection), O.TRIPWIRE, OE.INTEGRITY_FUNCTIONS (software protection) and O.SECURE_ADMINISTRATIVE_DIALOG (secure administrative dialog).

T_SENSITIVE_DATA_FORGERY

This component protects against alteration of the security policy. This component is met by the following objectives : O.CONFIGURATION_PROTECTION (security policy protection), O.TRIPWIRE , OE.INTEGRITY_FUNCTIONS (software protection) and O.SECURE_ADMINISTRATIVE_DIALOG (secure administrative dialog).

T_FUNCTIONS_FORGERY

This component protects against alteration of the software that implements the TOE security functions. This component is met by the following objective : O.TRIPWIRE and OE.INTEGRITY_FUNCTIONS.

T_AUDIT

This component protects against attacks on secure elements not reported by the TOE. This component is met by the following objective : O.AUDIT.

P_ADMINISTRATION

This component ensures that TOE is securely administered through protected communications channels. This component is met by the following objectives : O.HANDLE (security policy application), OE.ADMINISTRATION (secure administrative station) and OE.KEY_MANAGEMENT (secure key management).

P_AUDIT_REVIEW

This component ensures that log files are regularly analysed. This component is met by the following objective : O.AUDIT.

A.CONFIGURATION

This component ensures that TOE will be properly installed and configured. This component is met by the following objectives : OE.CONFIGURATION (secure configuration)and OE.KEY_MANAGEMENT (secure key distibution).

A.NO_EVIL

This component states that administrators are non-hostile This component is met by the following objectives : OE.NO_EVIL**.**

A.CRYPTOGRAPHIC_DEVICE

This components ensures that TOE used an hardware token implementing security mechanisms. This component is met by the following objectives : O.KEY_PROTECTION**.**

A summary of the threats to security objectives mapping is contained in the Table 8.1 below.

Table 8-1 Security environment to Security Objectives mapping

	O_DEFAULT_SECURITY_POLICY	O_CONFIDENTIALITY_EXCHANGED_USER_DATA	O_CONFIDENTIALITY_INTERNAL_USER_DATA	O_INTEGRITY_USER_DATA	O_AUTHENTICATION_USER_DATA	O_HANDLE	O_CONFIGURATION_PROTECTION	O_KEY_PROTECTION	O_TRIPWIRE	O.SECURE_ADMINISTRATIVE_DIALOG	O_AUDIT	OE.CONFIGURATION	OE.NO_EVIL	OE.ADMINISTRATION	OE.KEY_MANAGEMENT	OE.INTEGRITY_FUNCTIONS
T.DEFAULT_SECURITY_POLICY	x															
T_ EXCHANGED_USER_DATA _DISCLOSURE		x				x	x	x								
T_ INTERNAL_USER_DATA _DISCLOSURE			x													
T_ USER_DATA _FORGERY				x		x	x	x	x							x
T_FALSE_FRAME_INJECTION					x	x		x								
T_ USER_ADDRESS_DISCLOSURE							x		x							x
T_ KEYS_DISCLOSURE								x		x						
T_KEYS_FORGERY								x		x						
T_SENSITIVE_DATA_DISCLOSURE							x		x	x						x
T_SENSITIVE_DATA_FORGERY							x		x	x						x
T_FUNCTIONS_FORGERY									x							x
T_AUDIT											x					
P_ADMINISTRATION						x								x	x	
P_AUDIT_REVIEW											x					
A.CONFIGURATION												x			x	
A.NO_EVIL													x			
A.CRYPTOGRAPHIC_DEVICE								x								

8.2 Security Requirements Rationale

O.DEFAULT_SECURITY_POLICY

This objective addresses security policy when the TOE has not been configured yet. FDP_IFF.1 ensures that defaut security policy is "drop".

O.CONFIDENTIALITY_EXCHANGED_USER_DATA

This objective addresses confidentiality of user exchanged data. FDP_UCT.1 ensures that inter TOEs user data flows are protected from disclosure. This is also guarantied by FCS_CKM.1 and FCS_CKM.4 ensuring secure key handling associated with secure encryption/decryption operations (FCS_COP.1).

O.CONFIDENTIALITY_INTERNAL_USER_DATA

This objective guaranties that no sensitive data are written on the hard disk. FDP_RIP.1 ensures that clear data flows are unavailable in case of TOE theft.

O.INTEGRITY_USER_DATA

This objective addresses integrity of user exchanged data. FDP_UIT.1 ensures that inter TOEs user data flows are protected from alteration. This is also guarantied by FCS_CKM.1 and FCS_CKM.4 ensuring secure key handling associated with secure HMAC operations (FCS_COP.1).

O.AUTHENTICATION_USER_DATA

This objective addresses authentication of secure exchanged data. This is ensured by Ipsec protocol (HMAC control with FCS_CKM.1, FCS_CKM.4 and FCS_COP.1) and by the security domain concept described in FDP_ACC.2.

O.HANDLE

This objective guaranties that exchanged information between peer TOEs are handled in accordance with the security policy. FDP_IFC.1 and FDP_IFF.1 describe the rules permiting information flow between peer TOEs.

O.CONFIGURATION_PROTECTION

This objective addresses security policy and addressing plan protection. FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 ensure cryptographic protection of sensitive elements. FDP_ACF.1 describes the rules of the access control policy. The authentication policy is described by FIA_AFL.1 (generation of audit record after authentication failure), FIA_ATD.1 (to distinguish authorized administrators), FIA_UAU.2 and FIA_UID.2 (administrator authentication and idnetification before any action).
FMT_MOF.1 lists and defines the security function controlled by the administrator.
The security attributes affecting the VPN access policy are handled according to FMT_MSA.1 and FMT_MSA.3. FMT_MTD.1 and FMT_MTD.2 ensures user attributes management and self test tunning performed by the authorized administrator (maintained by FMT_SMR.1).

O.KEY_PROTECTION

This objective addresses secure key distribution. FCS_CKM.2 ensures a secure key distribution method based on smart card and performed through a trusted path (FTP_TRP.1).

O.TRIPWIRE

This objective guaranties that the TOE use some tools (namely Tripwire) to verify integrity of sensitive software parts. FPT_TST.1 ensures that integrity tests are periodically performed.

O.SECURE_ADMINISTRATIVE_DIALOG

This objective addresses protection of the administrative dialog. This is guarantied by FCS_CKM.4 and FCS_CKM.2 ensuring secure key destruction (key generation is performed on the TDM) and distribution (through a trusted path guarandied by FTP_TRP.1) and by FCS_COP.1 ensuring secure cryptographic operations for confidentiality and integrity protections.

O.AUDIT

This objective deals with security events handling. FAU.ARP.1 ensures that snmp traps are sent towards the TDM. The audit file is managed according to FAU_GEN.1 (list of auditable events), FAU_SAA.1 (events indicating a potential violation analysis) and FAU_SAR.1 (audit review by an authorized administrator). FAU_STG.1 ensures protection of the audit records.

A summary of the security requirements to security objectives mapping is contained in the Table 8.2 below.

Table 8-2 Functional and Assurance requirements to Security Objective mapping

	O.DEFAULT_SECURITY_POLICY	O.CONFIDENTIALITY_EXCHANGED_USER_DATA	O.CONFIDENTIALITY_INTERNAL_USER_DATA	O.INTEGRITY_USER_DATA	O.AUTHENTICATION_USER_DATA	O.HANDLE	O.CONFIGURATION_PROTECTION	O.KEY_PROTECTION	O.TRIPWIRE	O.SECURE_ADMINISTRATIVE_DIALOG	O.AUDIT
FAU_ARP.1											x
FAU_GEN.1											x
FAU_SAA.1											x
FAU_SAR.1											x
FAU_STG.1											x
FCS_CKM.1		x		x	x		x				
FCS_CKM.2								x		x	
FCS_CKM.4		x		x	x		x			x	
FCS_COP.1		x		x	x		x			x	
FDP_ACC.2					x						
FDP_ACF.1							x				
FDP_IFC.1						x					
FDP_IFF.1	x					x					
FDP_RIP.1			x								
FDP_UCT.1		x									
FDP_UIT.1				x							
FIA_AFL.1							x				
FIA_ATD.1							x				
FIA_UAU.2							x				
FIA_UID.2							x				
FMT_MOF.1							x				
FMT_MSA.1							x				
FMT_MSA.3							x				
FMT_MTD.1							x				
FMT_MTD.2							x				
FMT_SMR.1							x				
FPT_STM.1											x
FPT_TST.1									x		
FTP_TRP.1								x		x	

8.3 TOE Summary specification rationale

FAU_ARP.1 Audit alarms

This component aids in the detection of attacks and provides a function to alert the authorized administrator. This component is met by the following security function : SF.EVENT.

FAU_GEN.1 Audit Data Generation

This component outlines the data that must be included in audit records and the events that must be audited. This component is met by the following security functions : SF.INTEGRITY.DATA.CHECKSUM, SF.INTEGRITY.DATA.FAILURE, SF.CONTROL.PORTS and SF.EVENT.

FAU_SAA.1 Potential Violation Analysis

This component ensures that repeated failed attempts to authenticate or to encrypt data are monitored and alarmed if a threshold is reached. This component is met by the following security functions: SF.INTEGRITY.DATA.CHECKSUM, SF.INTEGRITY.DATA.FAILURE, SF.CONTROL.PORTS and SF.EVENT.

FAU_SAR.1 Audit Review

This component ensures that the audit is understandable by an Authorized Administrator. This component is met by the following security function : SF.EVENT.

FAU_STG.1 Protected Audit Trail Storage

This component ensures that the audit trail is always protected from tampering. Only the Authorized Administrator is permitted to access the audit trail. This component is met by the following security function : SF.ACCESS_PROTECTION.

FCS_CKM.1 Cryptographic Key Generation

This component ensures that the keys and key management data generated are of adequate strength to protect the confidentiality and integrity of data transmitted between peer TOEs. This component is met by the following security functions : SF.CONFIDENTIALITY.DATA.PROTOCOL, SF.CONFIDENTIALITY.ADDRESS, SF.CONFIDENTIALITY.CONFIGURATION and SF.INTEGRITY.DATA.PROTOCOL.

FCS_CKM.2 Cryptographic Key Distribution

This component ensures that the keys and key management data are distributed securely to provide confidentiality and integrity of data transmitted between peer TOEs. This component is met by the following security functions : SF.KEYMANAGEMENT.

FCS_CKM.4 Cryptographic Key Destruction

This component ensures that the keys and key management data are correctly destroyed to protect the confidentiality and integrity of data transmitted between peer TOEs. This component is met by the following security functions : SF.CONFIDENTIALITY.DATA.PROTOCOL and SF.KEYMANAGEMENT.

FCS_COP.1 Cryptographic Operation

This component ensures that all data sent between peer TOEs are encrypted using Triple Data Encryption Standard (3DES) and authenticated using HMAC MD5. This component is met by the following security functions : SF.CONFIDENTIALITY.DATA.PROTOCOL, , SF.CONFIDENTIALITY.ADDRESS, SF.CONFIDENTIALITY.CONFIGURATION, SF.INTEGRITY.DATA.PROTOCOL. and SF.INTEGRITY.DATA.CHECKSUM

FDP_ACC.2 Complete access control

This component defines the scope of control of the policies that form the identified access control portion of the SFP. This component is met by the following security function : SF.CONTROL.CORRESPONDANTS.

FDP_ACF.1 Security attribute based access control

This component describes the rules of the access control policy. This component is met by the following security function : SF.CONTROL.CORRESPONDANTS.

FDP_IFC.1 Subset Information Flow Control

This component identifies the entities involved in the AUTHENTICATED information flow control SFP. This component is met by the following security functions : SF.CONFIDENTIALITY.DATA.PROTOCOL and SF.INTEGRITY.DATA.PROTOCOL.

FDP_IFF.1 Simple Security Attributes

This component identifies the attributes of the subjects sending and receiving the information in the VPN access policy, as well as the attributes for the information itself. Then the operations identify under what conditions information is permitted to flow through the TOE. This component is met by the following security functions : SF.CONFIDENTIALITY.DATA.PROTOCOL and SF.INTEGRITY.DATA.PROTOCOL.

FDP_RIP.1 Subset residual information protection

This component ensures that deleted clear data flows are no longer accessible in the TOE . This component is met by the following security functions : SF.CONFIDENTIALITY.DATA.NOFILE.

FDP_UCT.1 Basic data exchange confidentiality

This component ensures that inter TOEs user data flows are protected from disclosure. This component is met by the following security function : SF.CONFIDENTIALITY.DATA.PROTOCOL.

FDP_UIT.1 Data exchange integrity

This component ensures that inter TOEs user data flows are protected from modification. This component is met by the following security function : SF.INTEGRITY.DATA.PROTOCOL.

FIA_AFL.1 Authentication Failure Handling

This component ensures that human users who are not Authorized Administrators cannot endlessly attempt to authenticate. After some number of failures, defined by the Authorized Administrator, the user is unable from that point on to authenticate. This component is met by the following security function : SF.ACCESS_PROTECTION.

FIA_ATD.1 User Attribute Definition

This component exists to provide attributes to distinguish Authorized Administrators from one another for accountability purposes and to associate the role in FMT_SMR.1 with a user. This component is met by the following security function : SF.ACCESS_PROTECTION.

FIA_UAU.2 User Authentication Before Any Action

This component ensures that the Authorized Administrator is authenticated before any action is allowed by the TSF. This component is met by the following security function : SF.ACCESS_PROTECTION.

FIA_UID.2 User Identification Before Any Action

This component ensures that the Authorized Administrator identity is identified to the TOE before anything occurs on behalf of the Authorized Administrator. This component is met by the following security function : SF.ACCESS_PROTECTION.

FMT_MOF.1 Management of Security Functions Behavior

This component ensures that the TSF restricts the ability to modify the behavior of functions (e.g., audit trail management, replay detection, self-test, authentication failure) to an Authorized Administrator. This component is met by the following security functions : SF.INTEGRITY.NETWORK, SF.CONTROL.MESSAGE , SF.CONTROL.CORRESPONDANTS, SF.CONTROL.PORTS, SF.CONTROL.LOCALFIREWALL and SF.EVENT.

FMT_MSA.1 Management of Security Attributes

This component ensures that the TSF restricts the ability to add, delete, and modify the security attributes that affect the VPN access policy to only the Authorized Administrator. This component is met by the following security function : SF.ACCESS_PROTECTION.

FMT_MSA.3 Static Attribute Initialization

This component ensures that there are restrictive default values implemented in the VPN access policy which the Authorized Administrator can change. This component is met by the following security function : SF.ACCESS_PROTECTION.

FMT_MTD.1 (1) Management of TSF Data

This component ensures that the TSF restricts the ability to modify, delete, and assign user attributes (as defined in FIA_ATD.1.1) to only the Authorized Administrator. This component is met by the following security function : SF.ACCESS_PROTECTION.

FMT_MTD.1 (2) Management of TSF Data

This component ensures that the TSF restricts the ability to set the time and date used to form timestamps (as defined in FPT_STM.1) to only the Authorized Administrator. This component is met by the following security functions :.

FMT_MTD.2 Management of TSF Limits on TSF Data

This component ensures that the TSF restricts the specification of the time interval for self-testing to the Authorized Administrator. This component is met by the following security function : SF.EVENT.

FMT_SMR.1 Security Roles

This component was chosen because each of the FMT components depends on the assignment of a user to the Authorized Administrator role. This component is met by the following security function : SF.ACCESS_PROTECTION.

FPT_STM.1 Reliable Time Stamps

This component was included because FAU_GEN.1 depends on having the date and time accurately recorded in the audit records. This component is met by the following security functions : SF.EVENT and SF.ACCESS_PROTECTION.

FPT_TST.1 TSF Testing

This component ensures the integrity of the operation of the TSF and to provide the Authorized Administrator a means to verify the integrity of the TSF code and data. This component is met by the following security function : SF.INTEGRITY.TOE.

FPT_TRP.1 Trusted Path

This component ensures that authentication process is performed through a secure path logically and physically independant from user data path. This component is met by the following security functions : SF.KEYMANAGEMENT and SF.ACCESS_PROTECTION.

A summary of the security requirements to security functions mapping is contained in the Table 8.3 below.

Table 8-3 Security Functions to Requirements mapping

	SF.CONFIDENTIALITY.DATA.PROTOCOL	SF.CONFIDENTIALITY.DATA.NOFILE	SF.CONFIDENTIALITY.DATA.PROTECTION	SF.CONFIDENTIALITY.ADDRESS	SF.CONFIDENTIALITY.CONFIGURATION	SF.INTEGRITY.DATA.PROTOCOL	SF.INTEGRITY.DATA.CHECKSUM	SF.INTEGRITY.DATA.FAILURE	SF.INTEGRITY.TOE	SF.INTEGRITY.NETWORK	SF.CONTROL.MESSAGE	SF.CONTROL.CORRESPONDANTS	SF.CONTROL.PORTS	SF.CONTROL.LOCALFIREWALL	SF.KEYMANAGEMENT	SF.EVENT	SF.ACCESS_PROTECTION
FAU_ARP.1																x	
FAU_GEN.1							x	x					x			x	
FAU_SAA.1							x	x					x			x	
FAU_SAR.1																x	
FAU_STG.1																	x
FCS_CKM.1	x			x	x	x											
FCS_CKM.2															x		
FCS_CKM.4	x														x		
FCS_COP.1	x			x	x	x	x										
FDP_ACC.2												x					
FDP_ACF.1												x					
FDP_IFC.1	x					x											
FDP_IFF.1	x					x											
FDP_RIP.1		x															
FDP_UCT.1	x																
FDP_UIT.1						x											
FIA_AFL.1																	x
FIA_ATD.1																	x
FIA_UAU.2																	x
FIA_UID.2																	x
FMT_MOF.1										x	x	x	x	x		x	
FMT_MSA.1																	x
FMT_MSA.3																	x
FMT_MTD.1																	x
FMT_MTD.2																x	
FMT_SMR.1																	x
FPT_STM.1																x	x
FPT_TST.1									x								
FTP_TRP.1															x		x

8.4 Rationale for assurance requirements

The EAL2 assurance level augmented with ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1, AVA_VLA.2, ADV_LLD.1, ADV_IMP.1, ALC_TAT.1 (these last 3 classes are relative to TOE sub systems involved in cryptographic functions) was chosen because it imposes :

- Independant testing performed by the evaluator (the final user is then ensured that the TOE security functions are implemented as specified)
- Independant vulnerability analysis by the evaluator (the final user is then ensured that the TOE is resistant to penetration attacks performed by attackers possessing a low attack potential).
- A high level design and a low level design including implementation analysis (cryptographic functions only) evaluation to verify any security malfunctions ;
- Software developpment good practices (the final user is then ensured that the product was correctly and securely designed and developped and that any discovered security flaw is tracked and corrected).

8.5 Rationale for strength of function claim

"strength of function" is the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels : SOF-basic, SOF-medium and SOF- high.

SOF-high is the strength of function level chosen for this SP. SOF-basic states, "a level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a high attack potentiall.. The rationale for choosing SOF-high was based on the TOE security objectives documented in Section 4 of this ST and on cryptographic requirements from french DCSSI .

References

[1] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[2] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.