BULL TRUSTWAY VPN LINE

ISO15408

Security Target

Version 2.9

TABLE OF CONTENTS

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 Line Security Target

Author : José Lavancier

Contributors : Nadine Fabiano, Liliana Cabalantti

ST Version : 2.9, dated February 27th , 2008

TOE Version : TVPN 4.05.02 and TCRX 4.05.01

TOE commercial name: BULL TrustWay VPN

1.2 ST overview

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

With TrustWay, BULL has created a set of European network security products. The TrustWay products family offers a range of custom designed "plug and play" devices targeted at specific security needs. Within the family, TVPN and TCRX are dedicated to provide a platform for creating trusted network infrastructures.

The TrustWay VPN offer relies on several elements (see figure 1). The TVPN (TrustWay Virtual Private NetWork) and the TCRX/TCRX2 (TrustWay Chiffreur routeur d'eXtrémité) are chassis which represent 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 TrustWay VPN equipments by a secured proprietary protocol. The TDM also determines rules, checks the state of the virtual network and permits to up grade remotely TrustWay VPNs and token 's softwares.

The SPC (Station de Personnalisation Client) is not mentioned on the schema but is necessary to perform customer personalization of the equipments. The SPC is used to inject specific secrets related to the particular equipment and to the particular user. The equipment receives then a cryptographic personalization and can be further introduced in the particular user network.

The TrustWay VPN offer also includes as options:

- the TrustWay Audit Manager (TAM) designed to monitor, supervise and audit the security policy implemented on the TrustWay appliances;

- the CEC (centre d'élaboration de clés) also called KGC (TrustWay Key Generation Center)creating and distributing all the encryption keys used by all TrustWay components.
- The TrustWay VPN client for nomadic users.

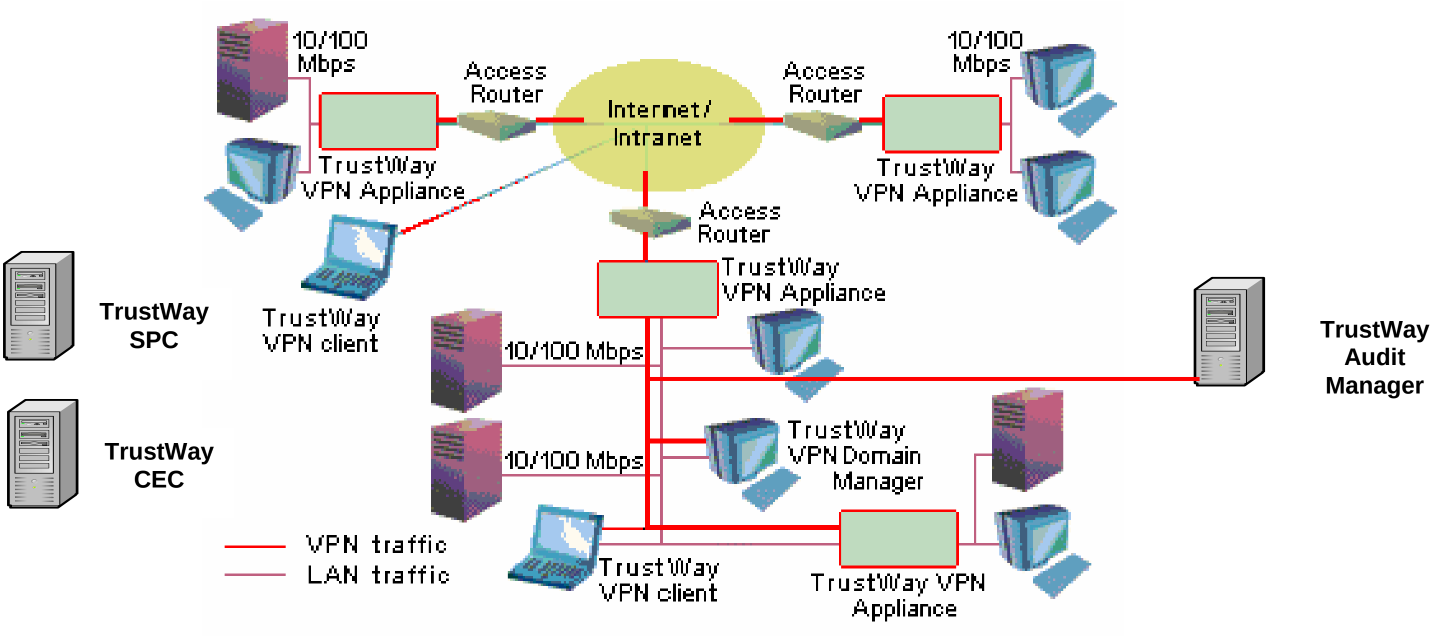


Fig1 : TrustWay VPN offer : Architecture and Administration

The TOE is composed of TrustWay VPN appliances, TVPN and TCRX, including the secured data exchange protocol with the network management utility (TDM TrustWay Domain Manager) and the Audit Manager (TAM)

Version TVPN 3.01.06 has been previously evaluated, certified (EAL2+) and qualified by DCSSI. The purpose is then a re evaluation of the TrustWay VPN offer including new VPN products CRX and CRX2.

It must be pointed out that the security target is not fully compliant to the protection profile edited by DCSSI (Profil de protection chiffreur IP version 1.5) but intends to take into account most of the DCSSI protection profile features.

1.3 CC conformance

The ST is compliant to part 2 and part 3 of ISO 15408 [1] and [2].

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 TOE does not implement any security function realized by non cryptographic probabilistic or permutational mechanism.

1.4 Standard Qualification conformance

The ST is compliant to the French qualification process [4] and thus conforms to the associated referential edited by DCSSI:

- Cryptographic referential [3];
- Key management architecture referential [5].

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):

- VPN Software (including secure administrative dialog) embedded in TVPN and TCRX,
- For TVPN
  - The hard disk part containing TVPN data (e.g. audit file)
  - The hardware token embedded software performing cryptographic operations
- For TCRX and TCRX2
  - Cryptographic software embedded in the cryptographic processor.
- The proprietary secured data exchange protocol (TDM - TrustWay VPN communication and TAM - TrustWay VPN communication)

The TOE concerns four operational modes of the TrustWay VPN equipments: the drop mode, forward mode, transport mode and tunnel mode (implementation of the IPSec protocol ESP).

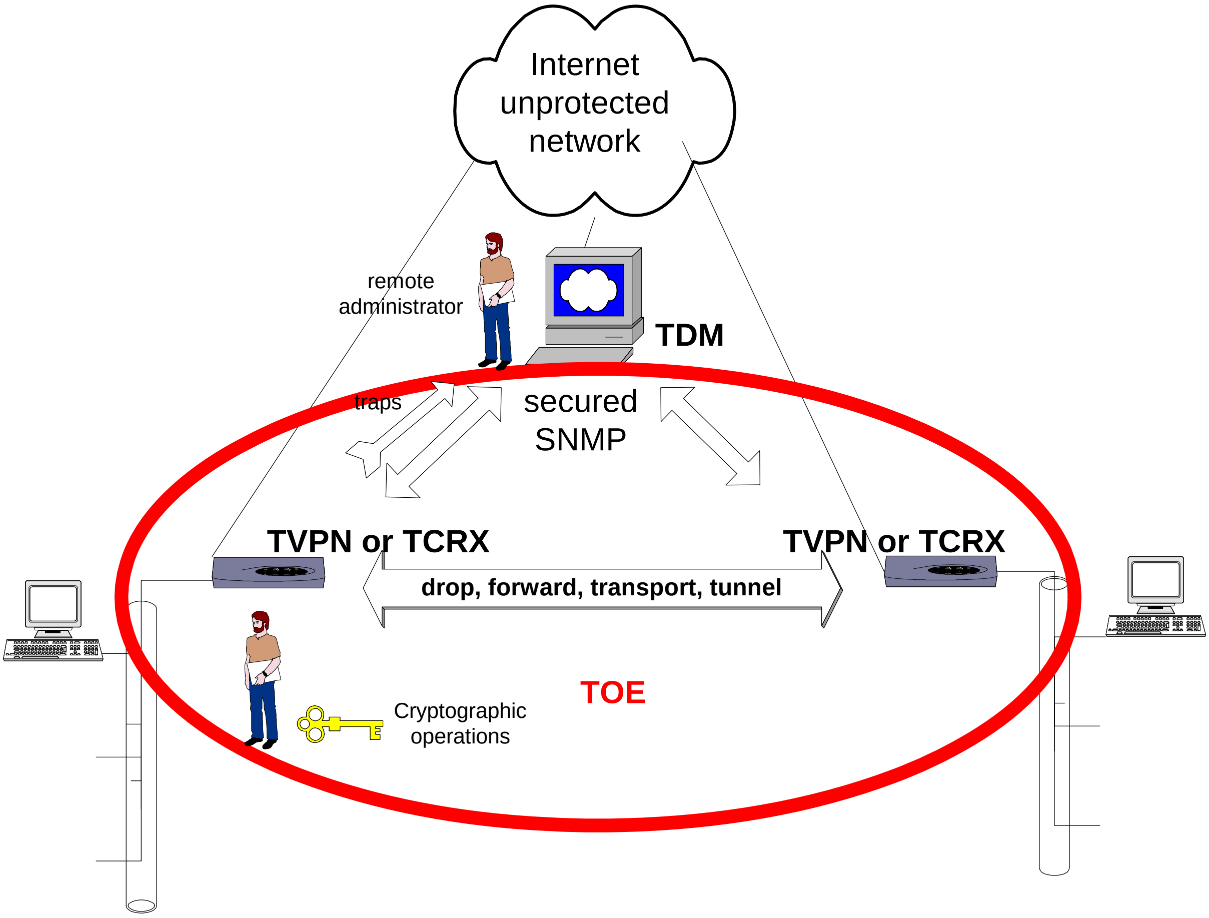


Fig2 : TOE boundaries

The following appliance part belongs to the TOE environment :

- the linux operating system (linux kernel 2.4.24)
- the filtering operations are managed by Netfilter utility (included in linux)
- Tripwire (version 1.2.2) 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 minute. The second level checks the configuration and permission files so as to the libraries. The third level checks TVPN, linux and Tripwire codes. Tripwire verification is based on a integrity pattern calculated and stored in the VPN software during software integration by Bull.
- The trusted channel (Safepad) to perform initial personalization of the TVPN.

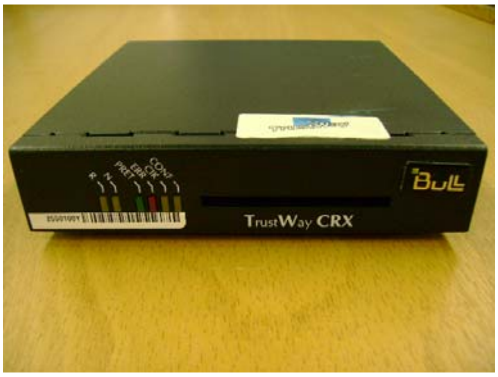
2.2.2 TOE technical specifications

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

- ASROCK I775 GV s775 FSB800 mother board
- Intel Celeron D 331 2.66Ghz s775
- Hard disk : 160go PATA Maxtor 8M
- Memory : 512 Mo 400Mhz CL3

- hardware token (version 76677843-309A hardware – firmware)
- the power supplier

The TCRX is a monocard system including a network processor (Intel EGLXT973QCA3V) and a cryptographic processor (Altera EP1C20F324C8N).



The TCRX2 contains the same monocard than the CRX (with a higher throughput) and the power supply is included into the box. Unless explicitly indicated, we will not distinguish the TCRX and TCRX2 in the present document (and we will simply indicate TCRX to refer to the two equipments).

External interfaces :

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

The hardware token of the TVPN indicates its state through the leds.

Logical items included in the TOE are:

- The TVPN Software version 4.05.02 and the TVPN token embedded software performing cryptographic operations (version B205 software)
- The TCRX Software version 4.05.01 (version c020 software)
- The proprietary secured data exchange protocol (TDM - TrustWay VPN communication and TAM - TrustWay VPN communication)
- Local administration facilities (through the serial port).

The TrustWay Domain Manager and the TrustWay Audit Manager are not included in the TOE, only the secured data exchange protocol between TrustWay VPN appliances, TVPN and TCRX and the TDM and TAM.

2.3 TrustWay VPN components

2.3.1 TVPN

TVPN 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 are performed by a high performance PCI interface based secure cryptographic hardware token developed by BULL.

2.3.2 TCRX

TCRX is a end-user version of the previous model, the IPSec part is common with the TVPN appliance.

TCRX contains an electronic card and a chassis integrated by a supplier.

The cryptographic operations are performed by a secure cryptographic processor developed by BULL and being the subject of a parallel evaluation relative to another TrustWay product.

2.3.3 TrustWay VPN administration

2.3.3.1 TrustWay VPN administration station (TDM)

The TDM (TrustWay Domain Manager) station acts as a remote TrustWay VPN administrator (and auditor). It is based on a standard Windows 2000 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 VPNs configuration. TDM offers a graphical view of both network topology and security rules (security policies) to apply between communicating systems.

TrustWay VPN configuration consists of:

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

TrustWay VPNs configuration is computed by TDM and conveyed to equipments 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.

2.3.3.2 Local administration

There is no possibility of Linux login on the TOE. The connection from a PC through the serial port leads to a local application, which give access to the following fonctionnalities:

- Display of TOE status
- Display of serial number
- Display and configuration of the initial IP parameters, allowing the first communication with the TDM
- Start the diagnostic tests
- Depersonalization of the TOE

2.3.3.3 CIK

The CIK (**C**rypto **I**gnition **K**ey) is an external element that is not stored in the cryptographic component of the TCRX. Without entering the CIK in the equipment, the system key is unusable since all the keys are wrapped. After equipment power on, the cryptographic component is waiting for the CIK (thus after power off the equipment is no more sensitive). A request for CIK is sent to the TDM. The TDM checks that the equipment is allowed to join the network (checking is based on the serial number, a blacklist is also handled by the TDM to refuse revocated equipments). The CIK is sent by the TDM through secure SNMP dialog.

This feature is only available on TCRX.

2.3.4 TDM and TAM – TrustWay VPN communication

TDM (or TAM) and TrustWay VPN equipments communicate by way of a secure SNMP based proprietary protocol. This protocol, based on a shared secret, allows a mutual authentication between TDM (or TAM) and TrustWay VPN equipments.

The shared secret is specific to each equipment. It is either generated by TDM or CEC token and associated by TDM to each equipment during its registration phase. This secret is securely stored in TDM (or TAM) token.

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

2.3.5 Life cycle

Master secrets are generated :

- either by the CEC and loaded in the SPC and in the TDM
- or by the SPC and loaded in the TDM.

In the initial phase, the SPC is used to inject specific master secrets related to the particular equipment and to the particular user (cryptographic personalization of the VPN equipment). This secrets are injected through the Ethernet connection of the CRX or via a smart card for the TVPN (the smart card is generated by the SPC).

Following this personalization phase with the SPC, the equipment can only be introduced in the particular user network to establish dialog with the TDM (or TAM) that shares the same master secrets used to distribute cryptographic keys.

In the next phase, the basic IP configuration is loaded in the equipment (via the local consol port) and, after CIK activation by the TDM (CRX only), the equipment is then waiting for the TDM registration. The registration is performed under control of the TDM administrator and is intended to securely inject the shared secret (base keys) used by the secure administrative dialog.

The VPN equipment is then ready to securely receive the security policy defined by the administrator on the TDM and finally communicate according this policy.

2.4 Security management

2.4.1 Network topology

The TrustWay VPNis 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)

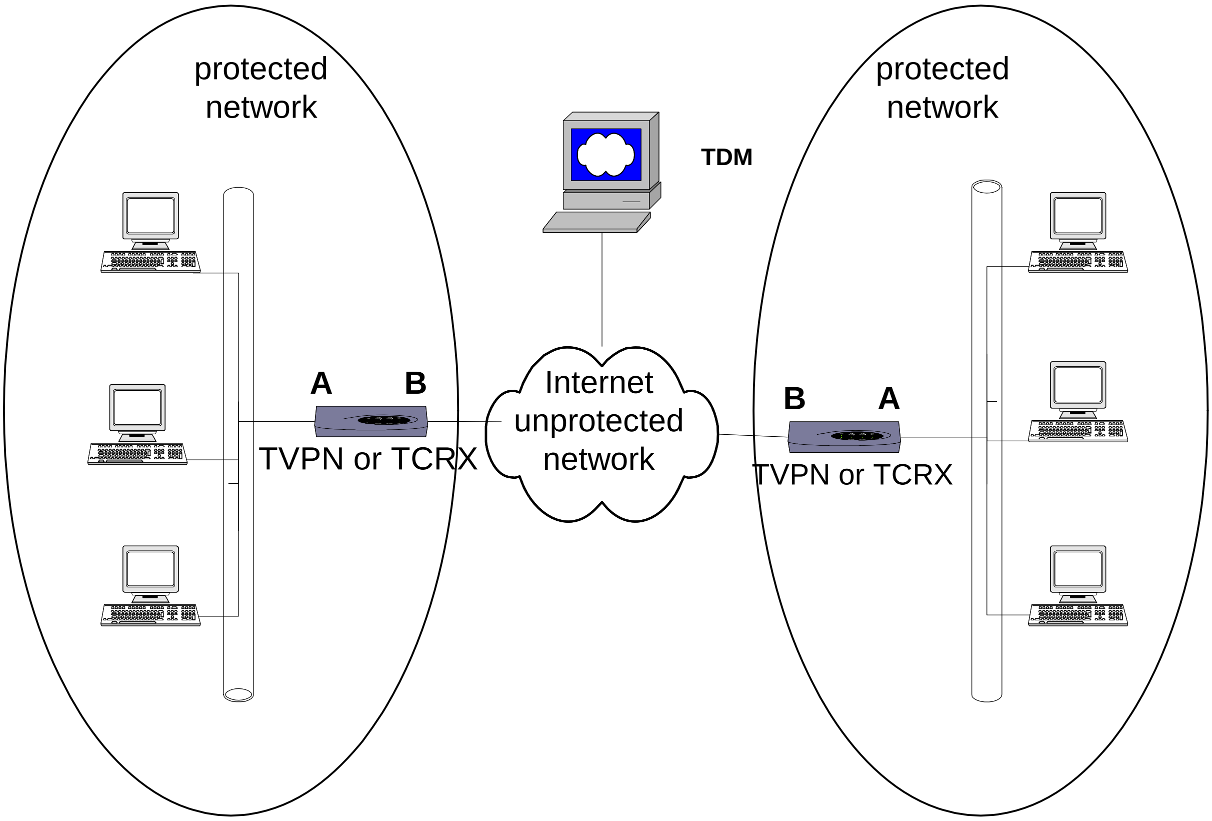


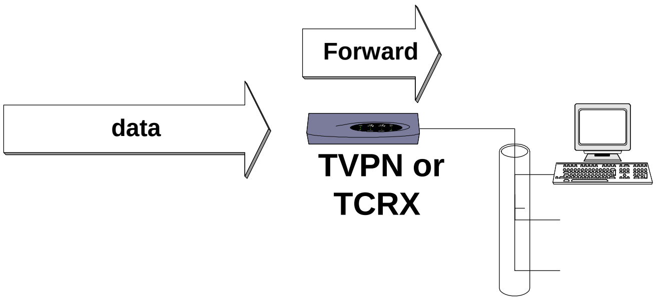
Fig 3 : General view of a network protected by TrustWay VPN boxes

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

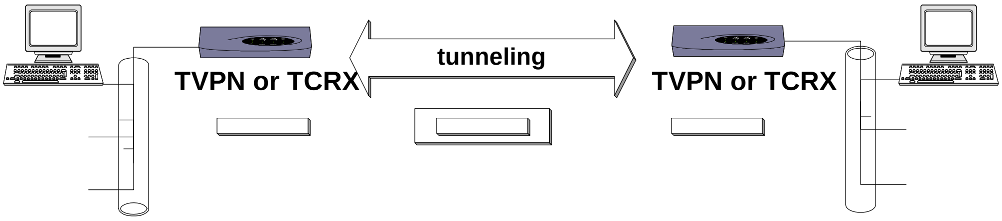
The following security policies are possible (from the least restricting to the most restricting) :

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

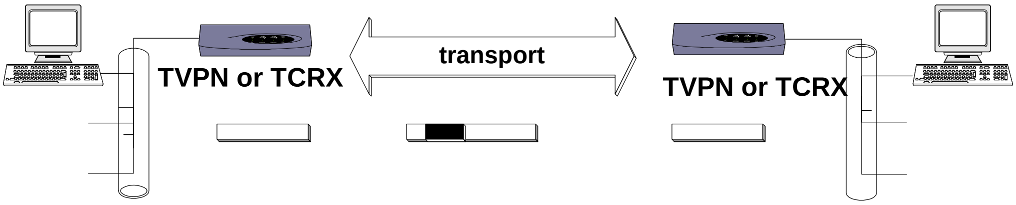
Forward mode : data are forwarded by configured VPN equipments in clear text (clear text communication)



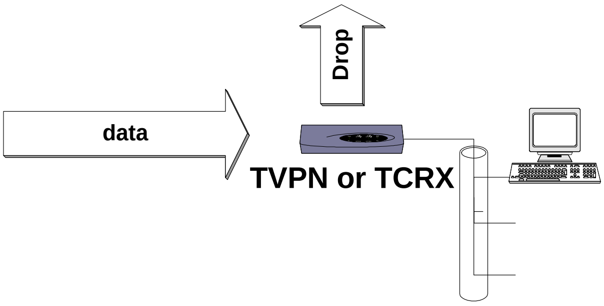
Tunnel mode : all the packets are encapsulated for the IPSEC exchange between VPN equipments. So the packets are authenticated and encrypted



transport mode : all the packets for the IPSEC exchange between VPN 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 TrustWay VPN where data appears in clear text) i.e. on interface A.

A TrustWay VPN 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 TrustWay VPN will communicate in clear text, whatever the domain's security policy.

2.4.3 Redondancy

Several TrustWay equipments protecting the same site can be put together to create a virtual equipment, provided that these equipments are identical (TVPN in router mode or CRX).

A single equipment, called the master, is responsible for relaying the traffic. The other equipments stay in waiting mode, ready to intervene. When a problem occurs that makes the master unoperational, the other equipments choose a new master responsible for relaying the traffic. The switch process has no effect on the other network elements.

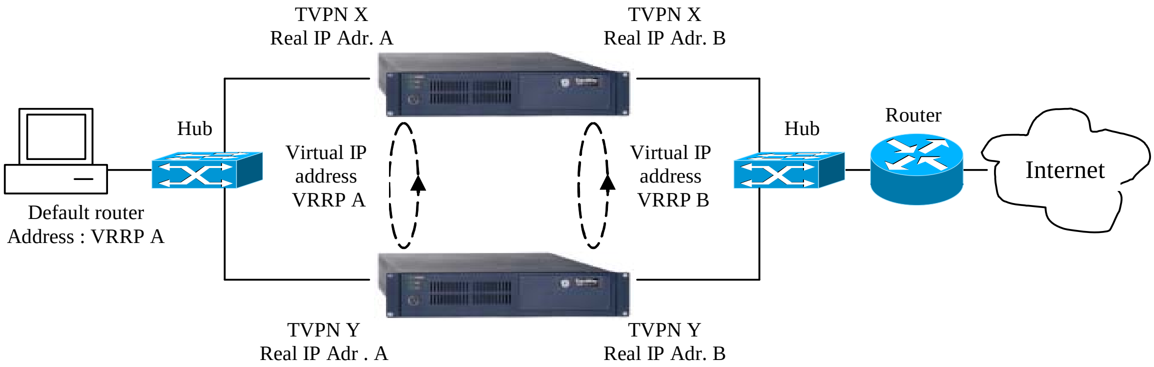


Fig 4 : General view of a network implementing VRRP

The TrustWay equipments belonging to a redundant group implements a mechanism compliant to VRRP protocol (RFC3768: « **V**irtual **R**outer **R**edundancy **P**rotocol) on each interface. A virtual IP VRRP address is then defined on each side of the equipment: the other network equipments (routers, extremity systems) are configured to use these virtual addresses. Moreover, the 2 VRRP instances of a redundantTrustWay equipment are coupled in order to switch in a coherent way the IP virtual address on each side. The master equipments is the equipments that owns the two IP virtual addresses at a given time.

The TrustWay administration stations (TDM) and the TrustWay audit stations (TAM) continue to address each equipments of a redundant group with the real IP addresses.

2.4.4 QoS marking

The TrustWay VPN equipments make possible to copy the QoS field of the initial frame in the QoS field of the IPSec frame or to position this field independently of the original frame.

2.4.4.1 DSCP field

The TrustWay VPN equipments configured in router mode make possible to mark the encrypted frames by positioning the DSCP field [RFC 2474 : Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers].
It is possible with the TDM to position any value in the DSCP field of the emitted IPSec frame. With this functionality, the network will apply a specific priority treatment based on the marking value.
The frame marking can be defined by :

- Source and destination IP/Mask address
- Port
- IP protocol

2.4.5 DHCP relay

The TrustWay VPN equipments configured in router mode propose the DHCP relay functionality. The networks on the clear secure side that are dynamically configured with DHCP can use the protecting VPN as DHCP relay. This implies that no DHCP request and response is emitted on the non secure network so as not to reveal the addresses of the equipments on the secure side.

2.4.6 Tunnelling

The TrustWay VPN implements the IPSec protocol in tunnel mode.

The tunnels established between the various devices implement an AES CBC-mode encryption which ensures the flow's security, and a 256-bit HMAC SHA 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 5).

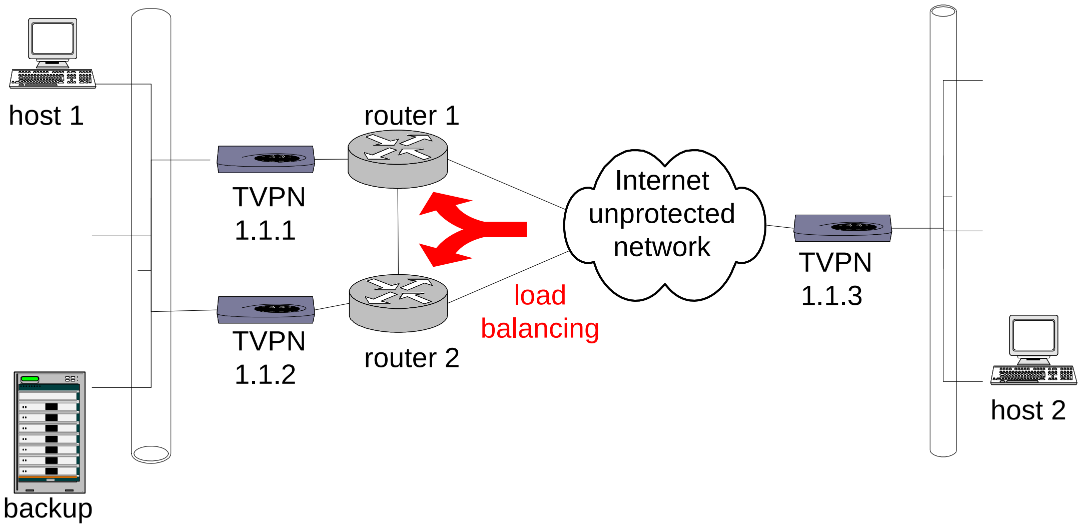


Fig 5 : General view of a network implementing load-balancing and backup

2.4.7 Frames processing and filtering

The configured 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 TrustWay VPN 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.

Additionally, 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 TrustWay VPN 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).

2.4.8 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 or CEC hardware token and are sent – in encrypted form –as part of TrustWay VPNs configuration.

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

2.4.8.1 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 TrustWay VPNs.
>
> TDM uses new systems keys (generated by the TDM or the CEC) and send the configuration with these new keys to all the TrustWay VPNs present in domains. Once updated, news keys are immediately effective.

Change keys at specified date

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

Furthermore whenever TDM imports a configuration from .xml script files, new system keys are generated and sent to TrustWay VPNs upon next configuration update.

2.4.9 TVPN operational states

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

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

The *uninstalled* state corresponds to a TrustWay VPN 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 TrustWay VPN. This is the case, for example, of a TrustWay VPN sent to maintenance and which LAN flow shall be stopped because it is no longer securized. TDM no longer sends any configuration to this TrustWay VPN which can be considered as revoked.

The *transparent* state corresponds to a TrustWay VPN temporary removed from network but which LAN, still connected to the network, must communicate with LANs of other TrustWay VPNs. This is the case, for example, of a TrustWay VPN 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 TrustWay VPN. TDM no longer sends any configuration to this TrustWay VPN but modifies other TrustWay VPNs configuration to apply a forward mode.

If a TrustWay VPN is removed from all security domains, then this TrustWay VPN will be revoked after updating configuration. Indeed all previous security rules on the TrustWay VPN 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 TrustWay VPN don’t have any rule applying to the systems protected by the revoked one and so perform the default action (drop or forward) according to the configuration.

2.5 TrustWay VPN audit capabilities Alarms

2.5.1 TVPN alarms

Two types of alarms can be generated by TrustWay VPN:

- ❑ Alarms which triggering criteria can be configured

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

In TrustWay VPN, events related to the alarm are counted. When the counter becomes greater than or equal to a configured threshold the equipment 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 other than routing protocols OSPF, RIP, IGRP and EGP.
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 encryption of 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	VPN functions starting
TripWire alert	Error detected by TripWire (Functions survey)
Change Keys alert	Error detected during Change Systems Keys operation
TCRX Software Update alert	Error detected during Software Update operation (TCRX only)
TVPN Cryptographic token alert	Error detected on Cryptographic token (TVPN only)

These alarms are reviewed by authorized auditor on supervisor stations.

2.5.2 Syslog

Syslog messages are sent to the syslog servers declared in the TDM configuration. Each alarm has an equivalent syslog message.

According to TDM configuration, Syslog messages can be IPSec encapsulated. They provide more detailed information that alarms.

These alarms are reviewed by authorized auditors on syslog stations.

2.5.3 TrustWay VPN network supervision

TDM offers the possibility to declare machines as network supervisors for a TrustWay VPN and to define the security policy applied to supervision flow. These supervisors will receive TrustWay VPN SNMP traps and can query the non-secure MIB of this equipment.

TDM acts as a supervisor for all managed TrustWay VPNs. Received traps are logged by Windows Event viewer.

2.6 TOE users

TOE users are the following:

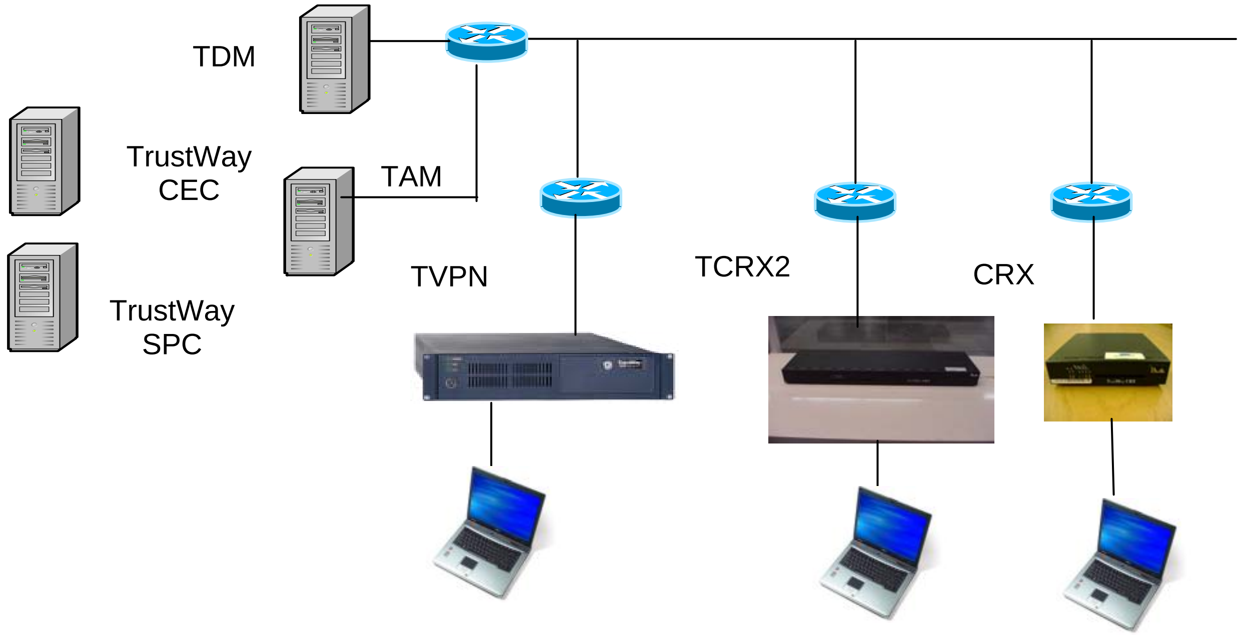
- Auditors on syslog stations and supervisor stations in charge of analysing the security events to detect any attack.
- Administrator on the TAM in charge of verifying the coherency of the security policy.
- Administrator on the TDM in charge of defining, configuring and distributing the security policy. They are also in charge of managing all the security features such as CIK blacklist, key renewal …
- Administrator in charge of generating the keys on the CEC
- Administratror in charge of (de)personalizing the equipments.

2.7 Evaluation platform

The evaluation platform will include (see figure 6):

- A TDM station (version 4.06.02)
- A TAM station (version 1.06.01)
- A SPC station (version 1.03.04)
- A CEC station (version 1.02.05)
- A TVPN, a CRX and a CRX2
- PC (Windows XP) protected by TVPN equipments
- Routers

Fig 6: Evaluation platform



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,) and sensitive audit data (syslog messages) 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.LOCAL
All the administrative equipments (TDM, CEC, TAM, SPC …) including all the associated data media (e.g. CDROM with keys, smart cards …) and the TVPN must be placed in secure environments whose access is strictly restricted to authorised administrators only. In particular the CEC or the SPC in charge of generating the keys are not connected to any network. The TCRX and the TCRX2 which are placed at end points are not concerned by this assumption.

A.TDM_PROTECTION
The robustness of TDM operating system will be assured by logical means before its first use.

A.SECURE_OPERATION
The TOE will be configured in order to assure a secure operation, that is securization of all frames and use of IPSec Tunnel for this securization.

A.CRYPTO
The cryptographic keys generated outside the TOE (CEC, SPC and TDM) and distributed to the TOE must have been generated according to recommendations specified in the DCSSI cryptographic referential [3] for the standard strength level.

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.

A.NO_EVIL
Authorized administrators and auditors are non-hostile, approprately trained and follow all administrator guidance. In particular, authorized administrators are authenticated before performing any action on the TDM or TAM. Authentification is performed by the TDM or TAM hardware token, through a trusted path based on a smart card authentication procedure.

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 :
- external profile : external unauthorized people (hackers for example) or external IT entities not authorized to access the TOE (in particular, administer the TOE)
- internal profile : Hostile people (belonging to maintenance or cleaning personnel for example) with access to internal network.
- malfunction profile (software dysfunction causing security failure).

T.DEFAULT_CONFIGURATION
Threat agents with internal profile
A threat agent could send user-data while security policy of theTOE is not configured.

T.INTERNAL_USER_DATA_DISCLOSURE
Threat agents with internal and external profile
Sensitive clear user data recorded in remanent memory of the TOE (CRX or CRX2) can be read by an attackant in case of TOE theft.

T.FALSE_FRAME_INJECTION
Threat agents with external profile

Injection of data by a hacker between the TOE and the TDM with a view to being delivered to the protected recipient.

T.KEYS_DISCLOSURE
Threat agents with internal and external profile
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
Threat agents with internal and external profile
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
Threat agents with internal and external profile
Disclosure of the security policy to aid the preparation of attack scenarios, thru TOE theft or administration dialog analysis.

T.SENSITIVE_DATA_FORGERY
Threat agents with internal and external profile
Alteration of the security policy to enable clear flows exchange between peer TOE and disclosure of secure data exchanged thru TOE theft or administration dialog analysis.

T.MISUSE
Threat agents with external profile
Buying a TVPN equipment or stealing it after personnalisation or buying a TDM station in order to enter the user network and exchange sensitive data with the user equipments.

T.FUNCTIONS_FORGERY
Threat agents with malfunction profile
Alteration of the software (internal error) that implements the TOE security functions causing alteration of the secure data exchanged or false data received by the user.

T.AUDIT
Threat agents with external profile
Attacks on secure elements not reported by the TOE. An attacker can access the audit alarms in order to read sensitive information reported by the syslog message, modify the message content or delete it.

T.COHERENCE_POL

Threat agents with external profile
The security policy applied at the level of a subnet IP is different from the one expected as defined by the administrator after administration dialog analysis and modification (from tunnel AES to forward for example in order to send clear flows).

T.ADMIN_REPLAY
Threat agents with external profile
Capture of administration IP packets sequence in order to play them again

3.4 Organisational Security Policies

P.SERVICES

The TOE must apply the VPN security policies defined by the security administrator.

The TOE must provide all the security services necessary to implement the protections that are specified in these security policies.

- Confidentiality protection of applicative user data
- Authenticity protection of applicative user data
- Confidentiality protection of topological data (addressing plan)
- Authenticity protection of topological data

P.CRYPTO

The DCSSI cryptographic referential [3] and [5] must be applied for key management (generation, destruction, usage and distribution) and cryptographic functions used by the TOE and relative to the standard strength level.

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
IPSec-Transport and IPSec-Tunnel security policies shall ensure the confidentiality of data exchanged by the users.

O.CONFIDENTIALITY_INTERNAL_USER_DATA
Clear flows only travel in the memory in the TOE (no file writing on the hard disk for example) in order not to compromise the remainder of the secure network in case of TOE theft. Also after power off for maintenance, new affectation purpose or any other context modification, all sensitive data are made unavailable

O.INTEGRITY_EXCHANGED_USER_DATA
IPSec-Transport and IPSec-Tunnel security policies shall ensure that the data exchanged can not be altered. 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-Transport and IPSEC-Tunnel 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. 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 secure proprietary SNMP dialog for the shared secrets.

Keys are generated, deleted, managed and distributed according to the DCSSI cryptographic referential.

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. The TOE is rebooted after anomaly detection.

O.AUDIT
Security events will be sent to remote audit servers protected by a VPN equipment on a link applying the configured security policy. They will increment viewable statistic counters and can trigger alarms.

O.ADMIN_REPLAY
The TOE shall ensure protection against replay of administration data sequences.

O.COHERENCE_POL
The TOE shall guaranty the coherency between the VPN security policy definitions on the TDM (with associated contexts) with the real applied security policies on the remote VPNs.

4.2 Security Objectives for the Operating Environment

OE.CONFIGURATION

The TOE 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. . In particular, authorized administrators are authenticated before performing any action on the TDM or TAM. Authentification is performed by the TDM or TAM hardware token, through a trusted path based on a smart card authentication procedure.

OE.ADMINISTRATION

All the administrative equipments (TDM, CEC, TAM, SPC …) including all the associated data media (e.g. CDROM with keys, smart cards …) and the TVPN shall be protected by physical and logical protection measures with access strictly restricted to authorised administrators only. In particular the CEC or the SPC in charge of generating the keys are not connected to any network. The security policy of the general network shall be appropriatly defined and the TOE correctly configured with this policy. The TDM and TAM shall supply confidentiality and integrity services to ensure protection of the administrative dialog with the TOE.

OE.KEY_MANAGEMENT

The TOE shall be personalized by the user SPC in order to inject specific secrets related to the particular equipment and to the particular user. In this process, the equipment receives a cryptographic personalization and will be authenticated when further introduced in the particular user network .

The TOE shall use systems keys supplied by 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.

OE.CRYPTO

Cryptographic keys distributed to the TOE must have been generated according to recommendations specified in the DCSSI cryptographic referential [3] for the standard strength level.

OE.AUDIT_REVIEW

The auditors on TDM, syslog stations and supervisor stations must analyse regularly the log files. They are in charge of managing the log files and detecting any attack.

OE.REVOCATION

The administrator must manage a blacklist on the TDM in order to control (accept or forbid) equipments introduction into the network.

OE.MAINTENANCE

Upon suppression of an equipment from the network (e.g. for maintenance purpose), the administrator must depersonalize this equipment before returning it to the producer and must include it in the revocation list of the TDM and TAM stations.

OE.TDM_PROTECTION

The appropriate logical measures must be taken to strengthen the operating system of TDM before its first use (for example, apply the security patches delivered by the operating system vendor, use a firewall).

OE.SECURE_OPERATION

In accordance with the security recommendations mentioned in “TrustWay Domain Manager – Installation and User’s Guide”, some rules must be followed when configuring TrustWay devices to obtain the best security. Secure operation implies the following:

- no frame is transmitted in clear text,
- the frames are secured by an encrypted IPSec tunnel.

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 the following actions [generate an SNMP trap (clear mode) towards the TDM , an SNMP trap towards configured supervisors (mode conforming with security policy) and a syslog message towards the configured syslog servers (mode conforming with security policy)] 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
-
- failed key change
- Unallowed port
- Error detected by TripWire(Functions survey)
- TCRX Software Update failure
- TVPN Cryptographic token alert

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.
failed change key	Reason code
Unallowed port	The port number and the address of the source subject.
TCRX Software Update failure	Reason code
Error detected by TripWire(Functions survey)	Reason code
TVPN Cryptographic token alert	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 trap and syslog audit records in a manner suitable for the Authorized Administrator to interpret the information.

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 256 binary digits in length] that meet the following: FIPS PUB 186-2 REV01 (05/10/2001), appendix 3.1 and DCSSI cryptographic referential [3].

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 [master keys are distributed by the SPC during the personalisation phase, CIK and shared secrets are distributed by the TDM through a proprietary secure key distribution method] 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 [AES CBC] and cryptographic key sizes [that are 256 binary digits in length] that meet the following: [FIPS PUB 197 REV01 26/11/2001 and DCSSI cryptographic referential]

FCS_COP.1.1 / DECRYPT - The TSF shall perform [decryption] in accordance with a specified cryptographic algorithm [AES CBC] and cryptographic key sizes [that are 256 binary digits in length] that meet the following: [FIPS PUB 197 REV01 26/11/2001 and DCSSI cryptographic referential].

FCS_COP.1.1 / HMAC - The TSF shall perform [secure hash of network traffic] in accordance with a specified cryptographic algorithm [HMAC SHA] and cryptographic key sizes [256 bits] that meet the following: [RFC2104 and DCSSI cryptographic referential.].

5.1.3 USER DATA PROTECTION (FDP)

5.1.3.1 FDP_ACC.2 / Security Policy complete access control

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

a) [subjects: part of the administration software that allows a security administrator to define, distribute and display VPN security policies and their security context;

b) 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 covered by an access control SFP.

5.1.3.2 FDP_ACF.1 / Security Policy 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 :

- The display of VPN security policies is authorized to be performed by an authenticated security administrator and in accordance with access rights defined by security administrators.

The distribution of VPN security policies is authorized only if performed on behalf of a remote security administrator and if the VPN security policies are protected from modification and disclosure during the distribution.

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]

5.1.3.3 FDP_IFC.1/Config audit subset Information flow control

FDP_IFC.1.1/Config_audit The TSF shall enforce the configuration and audit policy on

- **a)** [subjects: subjects of administration software that consults or modifies this information;
- **b)** information : configuration parameters, audit events and security alarms;
- **c)** Operations: all remote operations that cause this information to flow]

5.1.3.4 FDP_IFC.1/Key policy subset Information flow control

FDP_IFC.1.1/Key policy The TSF shall enforce the key policy on

- **d)** [subjects: administrator in charge of key management policy;
- **e)** information : master keys, administration keys and session keys;
- **f)** Operations: all remote operations perform from the TDM and that cause this information to flow]

5.1.3.5 FDP_IFC.1/VPN_Access_Policy Subset information flow control

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

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

b) information: customer data flow traffic through the TOE

c) 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 / VPN Access policy Simple security attributes

FDP_IFF.1.1 - VPN_Access_Policy The TSF shall enforce the [VPN access policy including drop, forward, IPSec-Transport, IPSec-Tunnel] 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 - VPN_Access_Policy 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 - VPN_Access_Policy The TSF shall enforce the [none].

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

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

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

5.1.3.7 FDP_IFF.1/Key policy simple security attributes

FDP_IFF.1.1/Key_policy The TSF shall enforce the key management policy based on the following types of subject and information security attributes:

a) AT.key_type attribute that indicates if the key is public, private or secret.

b) [assignment: other security attributes].

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

a) Remote key injection operation is authorized only if performed on behalf of a remote security administrator and if the imported keys are protected from modification and the private and secret imported keys are protected from disclosure during the injection.

FDP_IFF.1.3/Key_policy The TSF shall enforce the [none].

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

FDP_IFF.1.5/Key_policy The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.6/Key_policy The TSF shall explicitly deny an information flow based on the following rules: export (in plain text) of sessions keys and administrative shared secrets is forbidden.

5.1.3.8 FDP_IFF.1 / Config audit simple security attributes

FDP_IFF.1.1/Config_audit The TSF shall enforce the configuration and audit policy based on the following types of subject and information security attributes: none.

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

a) Remote administration operations on configuration parameters are authorized if this information is protected from modification and disclosure when flowing between the administration equipment and the IP encrypter.

b) Remote administration operations on audit events and security alarms are authorized if this information is protected from modification when flowing between the administration equipment and the IP encrypter.

FDP_IFF.1.3/Config_audit The TSF shall enforce the [none].

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

FDP_IFF.1.5/Config_audit The TSF shall explicitly authorise an information flow based on the following rules: [none].

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

5.1.3.9 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].

5.1.4 SECURITY MANAGEMENT (FMT)

5.1.4.1 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.MESSAGE;
- SF.INTEGRITY.NETWORK;
- SF.CONTROL.LOCALFIREWALL ;

to [an Authorized Administrator].

5.1.4.2 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/VPN _Access_Policy] to [an Authorized Administrator].

5.1.4.3 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.

5.1.4.4 FMT_MTD.1 / Authentication data - Management of TSF data

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

Refinement :

Authentication data are used for secure administration dialog and are based on shared secret keys allowing authentication between the TOE and the TDM through HMAC operations.

5.1.4.5 FMT_MTD.1 / Time stamping - 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].

5.1.4.6 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].

5.1.4.7 FMT_SMR.1 Security roles

FMT_SMR.1.1 - The TSF shall maintain the roles [Authorized Administrator based on remote TDM].

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

5.1.5 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

5.1.5.1 FPT_ITT.1/administration Basic internal data transfert protection

FPT_ITT.1.1/Administration The TSF shall protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

5.1.5.2 FPT_ITT.3/Administration TSF data intergrity monitoring

FPT_ITT.3.1/Administration The TSF shall be able to detect [modification of data, substitution of data, re-ordering of data, deletion of data] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2/Administration Upon detection of a data integrity error, the TSF shall take the following actions : [drops the frame and send an alarm trap and a syslog message].

5.1.5.3 FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities:

- sequences of administration data exchanged between a VPN and the TDM.

FPT_RPL.1.2 The TSF shall perform [frame dropped] when replay is detected.

5.1.5.4 FPT_STM.1 Reliable time stamps

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

5.1.5.5 FPT_TRC.1/VPN_policy Internal TSF consistency

FPT_TRC.1.1/VPN_policy - The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2/VPN_policy - When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [data exchange with the remote VPNs].

5.1.6 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

5.2 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 the AES algorithm as specified in FIPS PUB 197 REV01 26/11/2001 and DCSSI cryptographic referential. The Key used is a 256 bit length key.

SF.CONFIDENTIALITY.DATA.NOFILE

Clear flows only travel in the memory in the TOE (in particular no file writing on the hard disk of the VPN appliance).

6.1.1.2 SF.CONFIDENTIALITY.ADMIN

The administration dialog (including secure network's addressing and VPN policies) is hidden by the use of a secure proprietary snmp dialog 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 256-bit AES file and signed by 160-bit HMAC-SHA. 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 (HMAC SHA) as specified in RFC2104 and DCSSI cryptographic referential. The Key used is a 256-bit length key. The signature used in IPSEC is 160 bits long.

SF.INTEGRITY.DATA.FAILURE

Failure to authenticate a message initiates:

- the destruction of the message;
-
- the incrementation of a statistic counter;
- the sending of an alarm (SNMP trap and syslog message) 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 incrementation of a statistic counter ;
- the sending of an alarm (SNMP trap and syslog message) 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, launched and driven by the TOE. Results of Tripwire operations are delivered to the TOE. Then the detection of any alteration triggers the sending of an alarm (SNMP trap and syslog message).

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.ADMIN

The administration dialog (including secure network's addressing and VPN policies) is integrity protected by the use of a secure proprietary snmp dialog.

6.1.2.4 SF.INTEGRITY.NETWORK

Static routing tables are sent by the TDM as part of the VPN configuration. The tables are then transmitted by the TOE (VPN application) to the underlying linux. 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.AUTHENTICATION.ADMIN

TDM and TAM communicate with the TOE by way of a secure SNMP based proprietary protocol. This protocol, based on a shared secret and HMAC SHA-1 algorithm, allows a mutual authentication between TDM (or TAM) and the TOE.

The shared secret is specific to each TOE. It is either generated by TDM or CEC token and associated by TDM (or TAM) to each equipment during the registration phase.

6.1.4 SF.CONTROL

6.1.4.1 SF.CONTROL.MESSAGE

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

6.1.4.2 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.

6.1.4.3 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 incrementation of a statistic counter;
- the sending of an alarm (SNMP trap and syslog message) if the configuration requests.

6.1.4.4 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. This is done by netfilter which is configured, launched and driven by the TOE. Results of netfilter operations are delivered to the TOE.

6.1.4.5 SF.CONTROL.REPLAY

The TOE administration dialog supports an anti-replay mechanism .

6.1.5 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 keys on request. There are no limits as to the number of changes required.

The keys are generated :
- either by the CEC dedicated station (master secrets and session keys). When the number of session keys loaded in the TDM becomes low, the TDM administrator is alerted. When there is no more session keys loaded in the TDM, the session keys are automatically generated by the TDM (automatic mode) and the administrator is alerted by a permanent message on the graphical view ;
- or by the SPC (master secrets) and the TDM (session keys).

The keys are stored in the hardware token of the VPN appliance (keys are generated according an approved generation method, are stored in a protected memory and cannot be retrieved in clear) or are wrapped when stored outside the cryptographic component of the CRX.

6.1.6 SF.TDM

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

The TDM configuration application is in charge of computing and sending TrustWay VPNs configuration under the administrator control.

TrustWay VPN configuration consists of:

- ❑ Security rules (security domains);
- ❑ Filtering options;
- ❑ TVPN network supervision configuration;
- ❑ VPN network configuration (QOS, VRRP, etc.)
- ❑ Alerts management;
- ❑ Miscellaneous parameters (MTU, data compression, etc.).
- ❑ Date and Time for synchronizaton

6.1.7 SF.EVENT

6.1.7.1 Traps

SNMP traps (or alarms) are sent to the TDMs and declared supervisors.

On the supervisors, the MIB must first be installed. This MIB is described by the TW-public-MIB.txt file on the installation CD of the TDM.

The transmission of some traps is determined by thresholds configured on the TDM

List of Traps of the TVPN and TCRX

- Ethernet Overflow A:
  Channel A Ethernet Saturation
- Ethernet Overflow B:
  Channel B Ethernet Saturation
- SNMP Session Wrong Status:
  Message not expected in this state of the SNMP session
- SNMP protocol error:
  Error in the SNMP administrative protocol
- SNMP seal error:
  Signature error in the SNMP administrative protocol
- Non IP frames dropped (due to U= drop) from channel A:
  Non IP frames destroyed by U = Drops received on channel A
- Cryptographic overflow from channel A:
  Frames destroyed by saturation of the cryptography at encryption
- IP frames dropped from channel A:
  IP frames received on channel A destroyed by the "Drop" action (parameter X = Drop) or ICMP message not sent
- MIB unauthorized access:
  Attempt to modify a read only object or access by an unauthorised SNMP Manager

- Non IP frames dropped (due to U= drop) from channel B:
  Non IP frames destroyed by U = Drops received on channel B
- Bad checksum from channel B:
  Bad Transport checksum (TCP, UDP, ICMP) (checked when parameter S = Verify)
- IPSec authentication error:
  Frame destroyed by IPSEC authentication error
- Cryptographic overflow from channel B:
  Frames destroyed by saturation of the cryptography at deciphering
- IP frames dropped from channel B:
  IP frames received on channel B destroyed by the "Drop" action (parameter X = Drop) or ICMP message not sent
- Unallowed port:
  Connection attempt at an unauthorised port (filtering of ports configured on the TDM)
- Error detected by TripWire:
  Error in TVPN/TCRX integrity detected by TripWire
- Error detected by ChangeKeys:
  Error in the systems key change process
- PCA3 Cryptographic card Alarm:
  Error fed back by the TVPN encryption module

6.1.7.2 Syslog

Syslog messages are sent to the syslog servers declared in the TDM configuration. Each SNMP Trap has an equivalent syslog message. Date and time synchronized by the TDM (during configuration first sending and subsequent updates) are part of the syslog message.

List of Syslog Messages

The following messages are added to the list of traps:
(The following messages only contain the “information” part of the message; the fields <...> indicate the variable parts)

kernel:

1. ip dst authentication failed, ip src = <...>, = <...>
   (Authentication failed for this frame)
2. PORT not allowed for = <...>, ip src = <...>
   (Attempt to access an application <...> not allowed by port filtering)
3. checksum failed (<...>), ip src = <...>, ip dst = <...>
   (Verification of the transport layer checksum failed)
4. Open Session cipher failed – rv = <...>

(Failure to open the cryptography session)

5. Open Session decipher failed – rv = <...>
   (Failure to open the cryptography session)

6. SignEncrypt(): driver error <...>
   (Driver problem for this request)

7. SignEncrypt() failed: RC = <...>
   (SignEncrypt error described by the RC, Return Code)

8. VerifyDecrypt(): driver error <...>
   (Driver problem for this request)

9. VerifyDecrypt() failed: RC = <...>
   (VerifyDecrypt error described by the RC, Return Code)

10. Open Session: driver error <...>
    (Failure to open the cryptography session at the driver)

11. Open Session failed: RC = <...>
    (Failure to open the cryptography session described by RC, Error Code)

12. Close Session(): driver error <...>
    (Failure to close the cryptography session at the driver)

13. Destroy Object(<...>,<...>): driver error <...>
    (Destroy Object failed (parameter 1 = session, parameter 2 = object)

snmpd:

14. PDU rejected code = <...> src IP addr = <...>

15. Unauthorized access to MIB (<...>) from IP addr <...>

16. snmp exchange error - code (<...>)

17. Verify seal failed code (<...>) src IP addr = <...>

18. Unexpected SNMP variable, magic= <...>, code = <...>

19. VpnAutomatStatus != E2_STATE (<...>) , src IP address = <...>

changekeys:

20. Fatal: Can't start crypto (keys not changed)
    (initialisation of the cryptographic card failed)

21. Fatal: Can't open MIB file (keys not changed)
    (MIB file inaccessible or locked)

22. Can't read MIB file (keys not changed)
    (MIB cannot be read – signature problem)

23. MIB file incoherent (keys not changed)

(corrupted MIB file)

24. Change keys failed (keys may be partially changed)
(key change refused)

25. Fatal: Change keys done but can't write MIB file
(new keys cannot be used to encrypt and sign the MIB file)

vpn_inst:

26. Tripwire Init Error <Content of the Tripwire error file>

6.1.8 Strength level for the Security Functional Requirements

The minimum strength level for the FDP_IFC and FDP_IFF specific TOE Security Functional Requirements is SOF-high. This function strength is demonstrated in the document " Analyse des vulnérabilités des équipements TrustWay VPN v2.0".

There are no permutational or probabilistic mechanisms in the TOE.

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. The documents listed in the TOE configuration list will be used as to satisfy assurance evaluation requirements.

7 PP claims

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

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Threats and Security Objective Sufficiency

DEFAULT_SECURITY_POLICY

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

Threat prevention:
O.DEFAULT_SECURITY_POLICY ensures that the default security policy is drop.
Threat detection:
none
Protection after occurrence:
O.DEFAULT_SECURITY_POLICY will dropped all data on channel A and B.

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.

Threat prevention:
O.CONFIDENTIALITY_INTERNAL_USER_DATA ensures that there is no clear data resident in the TOE after power off.
Threat detection:
None
Protection after occurrence:
None

T_FALSE_FRAME_INJECTION

Injection of data by a hacker between the TOE and the TDM with a view to being delivered to the protected recipient.

Threat prevention:
O.SECURE_ADMINISTRATIVE_DIALOG ensures the authentication of the administrative data sent by the TDM whereas O.KEY_PROTECTION ensures keys protection relative to the administrative dialog.
Threat detection:
O.AUDIT will report authentication errors between the TOE and the TDM.
Protection after occurrence:
O.SECURE_ADMINISTRATIVE_DIALOG ensures that the corresponding data are dropped after authentication failure.

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.

Threat prevention:
O.KEY_PROTECTION ensures keys protection in the hardware token or in the TCRX cryptographic processor and O.SECURE_ADMINISTRATIVE_DIALOG protects against key disclosure during distribution.
Threat detection:
None
Protection after occurrence:
None

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.

Threat prevention:
O.KEY_PROTECTION ensures keys protection in the hardware token or in the TCRX cryptographic processor and O.SECURE_ADMINISTRATIVE_DIALOG protects against key forgery during distribution
Threat detection:
O.AUDIT will report integrity errors in the frames exchanged between between the TOE and the TDM.
Protection after occurrence:
O.SECURE_ADMINISTRATIVE_DIALOG ensures that the corresponding data are dropped after integrity failure

T_SENSITIVE_DATA_DISCLOSURE

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

Threat prevention:
O.CONFIGURATION_PROTECTION ensures that only remote administrators are authorized to view the security policy O.TRIPWIRE, OE.INTEGRITY_FUNCTIONS will ensure software protection relative to security policy treatment and O.SECURE_ADMINISTRATIVE_DIALOG protects against security policy disclosure during distribution by the TDM.
Threat detection:
none
Protection after occurrence:
None

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.

Threat prevention:
O.CONFIGURATION_PROTECTION ensures that only remote administrators are authorized to modify the security policy O.TRIPWIRE, OE.INTEGRITY_FUNCTIONS will ensure software protection relative to security policy treatment and O.SECURE_ADMINISTRATIVE_DIALOG protects against security policy forgery during distribution by the TDM.
Threat detection:
O.AUDIT will report integrity errors in the frames exchanged between between the TOE and the TDM.
Protection after occurrence:
O.SECURE_ADMINISTRATIVE_DIALOG ensures that the corresponding data are dropped after integrity failure

T_MISUSE

Buying a TVPN equipment or stealing it after personnalisation or buying a TDM station in order to enter the user network and exchange sensitive data with the user equipments.

Threat prevention:
OE.KEY_MANAGEMENT will guaranty that the VPN equipments received a cryptographic personalization (via the user SPC) that ensure authentication in the user network.
Threat detection:
O.AUDIT will report integrity errors in the frames exchanged between between the TOE and unknown TDM and/or the TOE and unknown VPN equipment.
Protection after occurrence:
First OE.REVOCATION ensures that stolen equipments are not activated by the TDM (the CIK cannot be sent). O.SECURE_ADMINISTRATIVE_DIALOG ensures that the data coming from unknown TDM are dropped after authentication failure and O.AUTHENTICATION_USER_DATA ensures that the data coming from unknown VPN equipment are dropped after authentication failure.

T_FUNCTIONS_FORGERY

Alteration of the software (internal error) that implements the TOE security functions causing alteration of the secure data exchanged or false data received by the user.

Threat prevention:
O.TRIPWIRE and OE.INTEGRITY_FUNCTIONS perform software integrity verifications.
Threat detection:
O.AUDIT will report tripwire alerts.
Protection after occurrence:
O. TRIPWIRE will force a reboot of the TOE after failure detection.

T_AUDIT
Attacks on secure elements not reported by the TOE. An attacker can access the audit alarms in order to read sensitive information reported by the syslog message, modify the message content or delete it.

Threat prevention:
O.AUDIT ensures that security events are sent towards remote audit servers.
Threat detection:
None
Protection after occurrence:
None

T.COHERENCE_POL

The security policy applied at the level of a subnet IP is different from the one expected since defined by the administrator.

Threat prevention:
O. COHERENCE_POL guaranties the coherency and OE.INTEGRITY_FUNCTIONS ensures protection of software elements impacted by security policy management.
Threat detection:
None
Protection after occurrence:
None

T.ADMIN_REPLAY

Capture of administration IP packets sequence in order to play them again

Threat prevention:
O. ADMIN_REPLAY ensures protection against administration replay attacks.
Threat detection:
none
Protection after occurrence:
O. ADMIN_REPLAY will ensure that corresponding reply frames are dropped.

8.1.2 Policies and Security Objective Sufficiency

P.SERVICES

The TOE must apply the VPN security policies defined by the security administrator.

The TOE must provide all the security services necessary to implement the protections that are specified in these security policies.

- Confidentiality protection of applicative user data
- Authenticity protection of applicative user data
- Confidentiality protection of topological data (addressing plan)
- Authenticity protection of topological data

This component is met by the following objectives :
O.CONFIDENTIALITY_EXCHANGED_USER_DATA and O.INTEGRITY_USER_DATA (user data protection), O.HANDLE (security policy application), O.CONFIGURATION_PROTECTION (security policy protection) and O.KEY_PROTECTION

(keys protection), O.TRIPWIRE and OE.INTEGRITY_FUNCTIONS (software applications aprotection).

P.CRYPTO

The DCSSI cryptographic referential [3] must be applied for key management (generation, destruction, usage and distribution) and cryptographic functions used by the TOE and relative to the standard strength level.

This component is met by the following objective :
O_CONFIDENTIALITY_EXCHANGED_USER_DATA ,
O_INTEGRITY_EXCHANGED_USER_DATA, O_AUTHENTICATION_USER_DATA,
O.CONFIGURATION_PROTECTION, O.SECURE_ADMINISTRATIVE DIALOG, O. KEY_PROTECTION.

8.1.3 Assumptions and Security Objective Sufficiency

A. CRYPTO

This component ensures that all cryptographic keys must have been generated according to recommendations specified in the DCSSI cryptographic referential [3] for the standard strength level. This component is met by the following objective: OE.CRYPTO.

A.LOCAL

This component states that all the administrative equipments and all the associated data media must be placed in secure environments. This component is met by the following objective: OE.ADMINISTRATION.

A.TDM_PROTECTION

This component ensures that TDM operating system will be strengthened before its first use. This component is met by the following objective: OE.TDM_PROTECTION.

A.SECURE_OPERATION

This component ensures that the TOE will be configured to operate in a secure mode. This component is met by the following objectives: OE.SECURE_OPERATION.

A.CONFIGURATION

This component ensures that the 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, OE.AUDIT_REVIEW (ensuring that he auditors shall analyse regularly the remote log files) and OE.MAINTENANCE (ensuring that administrator respects secure maintenance process).

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_EXCHANGED_USER_DATA	O_AUTHENTICATION_USER_DATA	O_HANDLE	O_CONFIGURATION_PROTECTION	O_KEY_PROTECTION	O_TRIPWIRE	O.SECURE_ADMINISTRATIVE_DIALOG	O_COHERENCE_POL	O_ADMIN_REPLAY	O_AUDIT	OE.CONFIGURATION	OE.NO_EVIL	OE.ADMINISTRATION	OE.KEY_MANAGEMENT	OE.INTEGRITY_FUNCTIONS	OE.CRYPTO	OE.AUDIT_REVIEW	OE.REVOCATION	OE.MAINTENANCE	OE.TDM_PROTECTION	OE.SECURE_OPERATION
T.DEFAULT_SECURITY_POLICY	x																							
T_ INTERNAL_USER_DATA _DISCLOSURE			x																					
T_FALSE_FRAME_INJECTION								x		x			x											
T_ KEYS_DISCLOSURE								x		x														
T_KEYS_FORGERY								x		x			x											
T_SENSITIVE_DATA_DISCLOSURE							x		x	x								x						
T_SENSITIVE_DATA_FORGERY							x		x	x			x					x						
T_FUNCTIONS_FORGERY									x				x					x						
T_MISUSE					x					x			x				x				x			
T_AUDIT													x											
T_COHERENCE_POL											x							x						
T_ADMIN_REPLAY												x												
P.SERVICES		x		x		x	x	x	x									x						
P.CRYPTO		x		x	x		x	x		x														
A.CRYPTO																			x					
A.LOCAL																x								
A.CONFIGURATION														x			x							
A.NO_EVIL															x					x		x		
A.TDM_PROTECTION																							x	
A.SECURE_OPERATION																								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/ VPN_ACCESS POLICY ensures that defaut security policy is "drop".

O.CONFIDENTIALITY_EXCHANGED_USER_DATA

This objective addresses confidentiality of user exchanged data. 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). Finally FDP_IFC.1/ VPN_ACCESS/POLICY and FDP_IFF.1/ VPN_ACCESS POLICY ensure application of rules permiting confidential information flow between peer TOEs.

O.CONFIDENTIALITY_INTERNAL_USER_DATA

This objective guaranties that no sensitive data are written on remanent memories. FDP_RIP.1 ensures that clear data flows are unavailable in case of TOE theft. Conception analysis through ADV_HLD.2 will validate this objective.

O.INTEGRITY_EXCHANGED_USER_DATA

This objective addresses integrity of user exchanged data. This is also guarantied by FCS_CKM.1 and FCS_CKM.4 ensuring secure key handling associated with secure HMAC operations (FCS_COP.1). Finally FDP_IFC.1/ VPN_ACCESS POLICY and FDP_IFF.1/ VPN_ACCESS POLICY ensure application of rules permiting integrity of information flow between peer TOEs.

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/Security Policy and FDP_ACF.1/Security Policy.

O.HANDLE

This objective guaranties that exchanged information between peer TOEs are handled in accordance with the security policy. FDP_IFC.1/ VPN_ACCESS/POLICY and FDP_IFF.1/ VPN_ACCESS_POLICY 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.
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/ **Authentication data** and FMT_MTD.2 ensures user attributes management and self test tunning performed by the authorized administrator (maintained by
FMT_SMR.1). Finally, FDP_IFC.1/CONFIG_AUDIT and FDP_IFF.1/CONFIG_AUDIT protects the integrity and confidentiality of configuration parameters when remotely audited or modified.

O.KEY_PROTECTION

This objective addresses secure key distribution. FCS_CKM.2 ensures a secure key distribution method based on a secure proprietary SNMP dialog (FPT_ITT.1/Administration and FPT_ITT.3/Administration, FDP_IFC.1/KEY_POLICY and FDP_IFF.1/KEY_POLICY).

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. FAU_ARP.1 ensures that an alarm is generated upon detection of integrity violation.

O.SECURE_ADMINISTRATIVE_DIALOG

This objective addresses protection of the administrative dialog. This is guarantied by FPT_ITT.1/Administration and FPT_ITT.3/Administration ensuring confidentiality and integrity protection of the dialog between the TDM and the VPN equipments. This is also guarantied by FCS_CKM.4, FCS_CKM.2 and FDP_IFC.1/KEY POLICY and FDP_IFF.1/KEY POLICY ensuring secure key destruction (key generation is performed on the TDM).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. Audit data 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). FPT_STM.1 ensures correct time stamping of syslog messages with time synchronization controlled by FMT_MTD.1.

O. COHERENCE_POL

This objective addresses the coherency between the security policies defined and configured by the administrator and those applied in the VPN equipments. This is gauranted by

FPT_TRC.1/VPN_policy ensuring correct interpretation and thus correct application of defined security policies.

O.ADMIN_REPLAY

This objective deals with protection against replay of administration operations. FPT_RPL.1 ensures detection of administration data replay and subsequent alarm actions.

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_EXCHANGED_USER_DATA	O.AUTHENTICATION_USER_DATA	O.HANDLE	O.CONFIGURATION_PROTECTION	O.KEY_PROTECTION	O.TRIPWIRE	O.SECURE_ADMINISTRATIVE_DIALOG	O.AUDIT	O.COHERENCE_POL	O.ADMIIN_REPLAY
FAU_ARP.1									x		x		
FAU_GEN.1											x		
FAU_SAA.1											x		
FAU_SAR.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/Security Policy					x								
FDP_ACF.1/Security Policy					x								
FDP_IFC.1/CONFIG_AUDIT							x						
FDP_IFC.1/VPN_ACCESS_POLICY		x		x		x							
FDP_IFC.1/KEY_POLICY								x		x			
FDP_IFC.1/CONFIG_AUDIT							x						
FDP_IFF.1/VPN_ACCESS/POLICY	x	x		x		x							
FDP_IFF.1/KEY_POLICY								x		x			
FDP_RIP.1			x										
FMT_MOF.1							x						
FMT_MSA.1							x						
FMT_MSA.3							x						
FMT_MTD.1/Authentication data							x						
FMT_MTD.1/Time stamping											x		
FMT_MTD.2							x						
FMT_SMR.1							x						
FPT_ITT.1/ADMINISTRATION								x		x			
FPT_ITT.3/ADMINISTRATION								x		x			
FPT_RPL.1													x
FPT_STM.1											x		
FPT_TST.1									x				
FPT_TRCI1/VPN_POLICY												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.

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 internal sensitive data. This component is met by the following security functions : SF.KEYMANAGEMENT

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. This component is met by the following security function : SF.KEYMANAGEMENT.

FCS_COP.1 Cryptographic Operation

This component ensures that all data sent between peer TOEs are encrypted using Advanced Encryption Standard (AES), and authenticated using HMAC SHA. This

component is met by the following security functions :
SF.CONFIDENTIALITY.DATA.PROTOCOL, , SF.CONFIDENTIALITY.ADMIN, SF.CONFIDENTIALITY.CONFIGURATION, SF.INTEGRITY.DATA.PROTOCOL. and SF.INTEGRITY.DATA.CHECKSUM

FDP_ACC.2 / Security Policy 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 Policy 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/CONFIG_AUDIT Subset Information Flow Control

This component identifies the entities involved in protection of configuration and audit policies sent by the TDM towards the VPN equipments. This component is met by the following security function : SF.AUTHENTICATION.ADMIN

FDP_IFC.1/VPN_ACCESS_POLICY 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.CONTROL.CORRESPONDANTS.

FDP_IFC.1/KEY_POLICY Subset Information Flow Control

This component identifies the entities involved in the distribution of cryptographic keys by the TDM. This component is met by the following security functions : SF.AUTHENTICATION.ADMIN

FDP_IFF.1/CONFIG_AUDIT Subset Information Flow Control

This component ensures protection of configuration and audit policies sent by the TDM towards the VPN equipments. This component is met by the following security function : SF.AUTHENTICATION.ADMIN

FDP_IFF.1/VPN_ACCESS_POLICY 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.CONTROL.CORRESPONDANTS.

FDP_IFF.1/KEY_POLICY Simple Security Attributes

This component ensures protection of cryptographic keys distributed by the TDM. This omponent is met by the following security functions : SF.AUTHENTICATION.ADMIN

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.

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.TDM.

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.TDM.

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.TDM.

FMT_MTD.1 / authentication data Management of TSF Data

This component ensures that the TSF restricts the ability to modify, delete, and assign user attributes to only the Authorized Administrator. This component is met by the following security function : SF.TDM.

FMT_MTD.1 /Time stamping 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 :SF.TDM

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.TDM.

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.TDM.

FPT_ITT.1/Administration Basic internal TSF data transfert protection

This component ensures confidentiality and integrity protection of the administration dialog between the TDM and the VPN equipments. This component is met by the following security functions : SF.CONFIDENTIALITY.ADMIN and SF.INTEGRITY.ADMIN

FPT_ITT.3/Administration TSF data integrity monitoring

This component ensures integrity protection of the administration dialog and take actions upon detection of integrity error. This component is met by the following security functions : SF.INTEGRITY.ADMIN and SF.EVENT.

FPT_RPL.1 Replay detection

This component ensures that administration data sequences cannot be replayed. This component is met by the following security function : SF.CONTROL.REPLAY.

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.TDM.

FPT_TRC.1/VPN_POLICY Internal TSF consistency

This component ensures the coherency between the security policies defined and configured by the administrator and those applied in the VPN equipments : This component is met by the following security functions : SF.CONFIDENTIALITY.ADMIN and SF.INTEGRITY.ADMIN (protection of security policies between the TDM and the TOE), SF.INTEGRITY.TOE (integrity of software implementing the policies).

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.

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.ADMIN	SF.CONFIDENTIALITY.CONFIGURATION	SF.INTEGRITY.DATA.PROTOCOL	SF.INTEGRITY.DATA.CHECKSUM	SF.INTEGRITY.DATA.FAILURE	SF.INTEGRITY.TOE	SF.INEGRITY_ADMIN	SF.INTEGRITY.NETWORK	SF.AUTHENTICATION.ADMIN	SF.CONTROL.MESSAGE	SF.CONTROL.CORRESPONDANTS	SF.CONTROL.PORTS	SF.CONTROL.LOCALFIREWALL	SF.CONTROL_REPLAY	SF.KEYMANAGEMENT	SF.TDM	SF.EVENT
FAU_ARP.1																			x
FAU_GEN.1						x	x							x					x
FAU_SAA.1						x	x							x					x
FAU_SAR.1																			x
FCS_CKM.1																	x		
FCS_CKM.2																	x		
FCS_CKM.4																	x		
FCS_COP.1	x		x	x	x	x													
FDP_ACC.2/ Security Policy													x						
FDP_ACF.1/ Security Policy													x						
FDP_IFC.1/CONFIG_AUDIT											x								
FDP_IFC.1/VPN_ACCESS_POLICY													x						
FDP_IFC.1/KEY_POLICY											x								
FDP_IFF.1/CONFIG_AUDIT											x								
FDP_IFF.1/VPN_ACCESS_POLICY													x						
FDP_IFF.1/KEY_POLICY											x								
FDP_RIP.1		x																	
FMT_MOF.1										x		x			x			x	x
FMT_MSA.1																		x	
FMT_MSA.3																		x	
FMT_MTD.1/Authentication data																		x	
FMT_MTD.1/Time stamping																		x	
FMT_MTD.2																		x	
FMT_SMR.1																		x	
FPT_ITT.1/ADMINISTRATION			x						x										
FPT_ITT.3/ADMINISTRATION			x						x										x
FPT_RPL.1																x			
FPT_STM.1																			x
FPT_TST.1								x											
FPT_TRCI.1/VPN_POLICY			x					x	x										

8.3.1 SFR dependencies

SFR	CC dependencies	Dependencies satisfied
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAA.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.2, FCS_CKM.4
FCS_CKM.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	FCS_CKM.1
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4
FDP_ACC.2/ Security Policy	FDP_ACF.1	FDP_ACF.1/ Security Policy
FDP_ACF.1/ Security Policy	FDP_ACC.1, FMT_MSA.3	FMT_MSA.3
FDP_IFC.1/CONFIG_AUDIT	FDP_IFF.1	FDP_IFF.1/CONFIG_AUDIT
FDP_IFC.1/VPN_ACCESS_POLICY	FDP_IFF.1	FDP_IFF.1/VPN_ACCESS_POLICY
FDP_IFC.1/KEY_POLICY	FDP_IFF.1	FDP_IFF.1/KEY_POLICY
FDP_IFF.1/CONFIG_AUDIT	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1/CONFIG_AUDIT, FMT_MSA.3
FDP_IFF.1/VPN_ACCESS_POLICY	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1/VPN_ACCESS_POLICY, FMT_MSA.3
FDP_IFF.1/KEY_POLICY	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1/KEY_POLICY, FMT_MSA.3
FDP_RIP.1	No dependencies	
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMR.1
FMT_MSA.1	FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_IFC.1/VPN_ACCESS_POLICY, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1/Authentication data	FMT_SMF.1, FMT_SMR.1	FMT_SMR.1
FMT_MTD.1/Time stamping	FMT_SMF.1, FMT_SMR.1	FMT_SMR.1
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	FMT_MTD.1/Authentication data, FMT_SMR.1
FMT_SMR.1	FIA_UID.1	
FPT_ITT.1/ADMINISTRATION	No dependencies	No dependencies
FPT_ITT.3/ADMINISTRATION	FPT_ITT.1	FPT_ITT.1/ADMINISTRATION
FPT_RPL.1	No dependencies	No dependencies
FPT_STM.1	No dependencies	No dependencies
FPT_TRC.1/VPN_POLICY	FPT_ITT.1	FPT_ITT.1/ADMINISTRATION
FPT_TST.1	FPT_AMT.1	

The dependency FMT_MSA.2 of FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1 is not supported. This dependency does not need to be satisfied because keys are generated, deleted, managed and distributed according to the DCSSI cryptographic referential. The cryptographic operations are performed in accordance with cryptographic algorithms and key sizes that meet the DCSSI cryptographic referential.

The dependency FMT_SMF.1 of FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 is not supported.This dependency does not need to be satisfied because the management functions are performed on the TDM, out of the scope of the TOE.

The dependency FDP_ACC.1.1 of FDP_ACF.1 is not supported. A TrustWay VPN 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 (drop, forward, IPSEC-Transport, IPSEC-Tunnel).

The dependency FPT_AMT.1 of FPT_TST.1 is not supported. Software applications that implement the TOE's functions and that handle sensitive data are checked on a regular basis during operation by Tripwire, which is configured, launched and driven by the TOE.

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).

References

[1] International Organization for Standardization, *ISO/IEC 15408-2:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, August 2005.

[2] International Organization for Standardization, *ISO/IEC 15408-3:2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, August 2005.

[3] Mécanismes de cryptographie : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard. Version 1.0. DCSSI.

[4] Processus de qualification d'un produit de sécurité – niveau standard v1.0, July 2003 DCSSI, 001591/SGDN/DCSSI/SDR

[5] Gestion des clés cryptographiques règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard Version 1.0, March 13st 2006 DCSSI