NATURE - TYPE Security Target (public version)

TITLE **VIRTUAL PRIVATE NETWORKS ISOLATION IN EQUANT IP VPN SERVICE**

SUMMARY
Public Security Target for MPLS / VPN on RAEI Network

AUTHOR EQUANT/CSN/PE&D			**VISA** EQUANT/CSN/PE&D		
Recipient(s)	**Department**	**A**	**Recipient(s)**	**Department**	**I**

HISTORY

Date	**Issue No.**	**Reason for Changes**
15/11/2001	1.0	Creation of a public version at the end of evaluation : - french to english translation - rationales and confidential items removed

TABLE OF CONTENTS

1 ST Introduction

1.1 ST Identification

ST Identity Virtual Private Networks isolation in Equant IP VPN service - Version 1.0

Author Christophe ANSELME-MOIZAN

TOE Identity Virtual Private Networks isolation in Equant IP VPN service – version 1.0

Common Criteria version used for ST redaction Version 2.1

1.2 TOE overview

To provide its MPLS/VPN product on the french market, Equant uses Transpac Internet backbone. This product provides customers with a virtual private network equivalent to a point-to-point leased lines set. This Internet backbone is built with :

- The RAEI network (which is the french edge Internet backbone of Transpac)
- The RBCI network (which is the french core Internet backbone of Transpac)

The MPLS/VPN product of Equant is called Equant IP VPN.

In order to guarantee customers that the service provided is equivalent to leased lines, Equant wants to assess that the technologies used to implement the MPLS/VPN always ensure the following security requirements :

- Traffic separation between customers VPN,
- Traffic separation between Internet and customers VPN,
- RAEI routers configuration integrity.

1.3 CC compliance

This security target has been designed according to these references :

- [CC-1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCIMB-99-031, version 2.1, August 1999
- [CC-2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, CCIMB-99-032, version 2.1 August 1999
- [CC-3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, CCIMB-99-033, version 2.1, August 1999

This ST is part 2 extended and part 3 augmented.

2 TOE Description

2.1 Type of system

TOE is a system offering network services similar to usual VPN with some specific characteristics due to IP environment :

- Traffic separation,
- Access control to RAEI routers,
- Routers configuration and routing tables integrity.

Nota : the provided service does not rely on cryptographic mechanisms. Nevertheless it offers a VPN since it ensures traffic separation (cf. glossary).

2.2 TOE description, area, boundaries

TOE is a representative subset of Equant VPN (MPLS) service in France. This subset consists in :

- 2 PE (Provider Edge routers) for network management access,
- 2 PE for customers access,
- a specific software tool for VPN production (VPN management tool),
- 2 TACACS servers for administrators authentication on PE and VPN management tool,
- a configuration integrity checking tool,
- a supervision application,
- an NTP server for trusted time base.

This subset is the minimum required to be able to provide 2 distinct customers VPN. Handling more customers is only done by adding interfaces on existing PE or adding more PE. Adding interfaces or PE modifies neither the way MPLS/VPN technology is used nor the way the managing tools work and are used.

The RBCI network (core IP backbone) does not take part in the TOE.

2.2.1 Hardware description

The hardware part of the TOE is made of :

- **Hosts**
    - VPN management tool Server
    - TACACS Servers
    - Configuration Checking server
    - PE admin firewall
    - NTP Server
    - Supervision Server
- **PE routers**
- **PE/P interconnections**

2.2.2 Software description

The software part of the TOE is made of :

- **Specific tool for VPN production (**VPN management tool)
- **PE routers configuration checking software**
- **Routers supervision**
- **Authentication server (TACACS)**
- **PE Operating System**

MPLS, MPLS/VPN, IS-IS, TDP and MPiBGP protocols are implemented by PE routers operating system. These protocols are those used to enforce MPLS/VPN

2.2.3 Assets requiring protection

Assets are security relevant elements of the TOE that include TSF data and user data :

a) **User data** are customer's data flow switched by MPLS.

b) **TSF data** are :

- PE routers configuration part that is used in the TOE context :
    - ✓ MD5 secret key used for MPiBGP authentication,
    - ✓ PE and VPN administrators profiles and privileges definition,
    - ✓ VRF import/export definition,
    - ✓ VRF attached RD definition,
    - ✓ Network interface attached VRF definition,
    - ✓ TACACS server definition,
    - ✓ PE local username definition.
- Routing tables exchanged between routers.
- VPN tags attached to customer's data flow (external tags).

Nota : assets list in PE configuration is informational and not exhaustive.

2.2.4 General description

The figure below shows the TOE implementation with two distinct customer's VPN. Each PE router (PE 1 and PE 2) offers VPN access to the 2 customers. 2 PE are dedicated to management networks interconnection to the backbone (One is for VPN management tool, the other is for all the others management tools). On these "management" PE are connected :

- TACACS authentication servers,
- PE configuration checking server,
- Supervision server,
- NTP server,
- VPN management tool.

The PE management network is protected by a dedicated firewall. The VPN management network is protected by a router embedded firewall.

There are 4 types of administrators working on the TOE :

- **PE administrators** are in charge of PE routers configuration (excepted VPN production).
- **VPN administrators** are in charge of customer's VPN production via VPN management tool.
- **PE management tools administrators** are in charge for supervision server, TACACS server (for authentication on PE), NTP server and PE configuration checking server.
- **VPN management tools administrators** are in charge of VPN management tool and the TACACS server that authenticates users on VPN management tool.

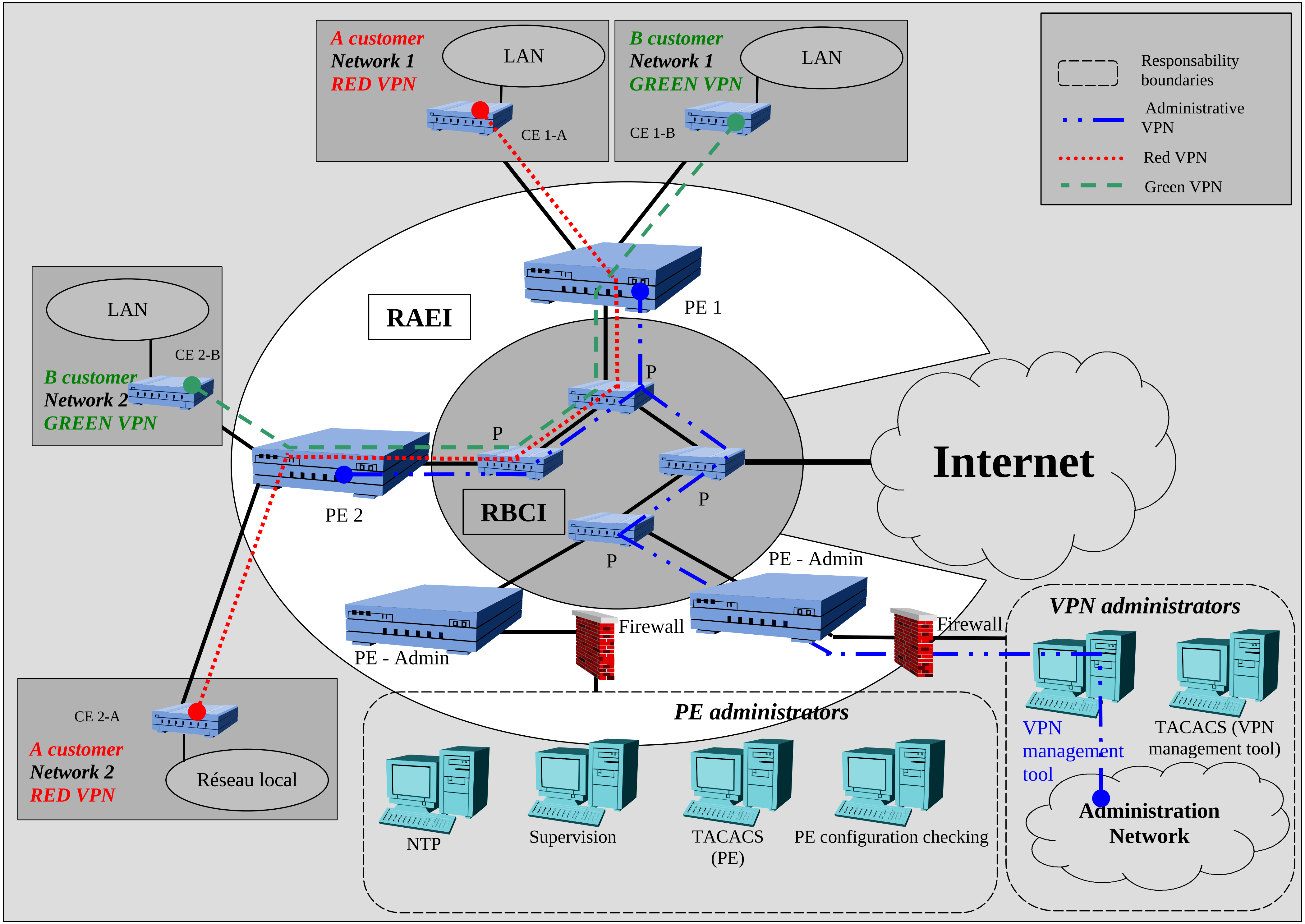
PE TACACS authentication server is used by PE routers to authenticate PE administrators and allow them to connect to the router. This server is under PE management tools administrators responsability. These administrators are also responsible for the supervision server, the NTP server and the PE configuration checking server.

PE administrators use these servers as simple users and have no administrative privileges on these hosts. They have full control on PE management.

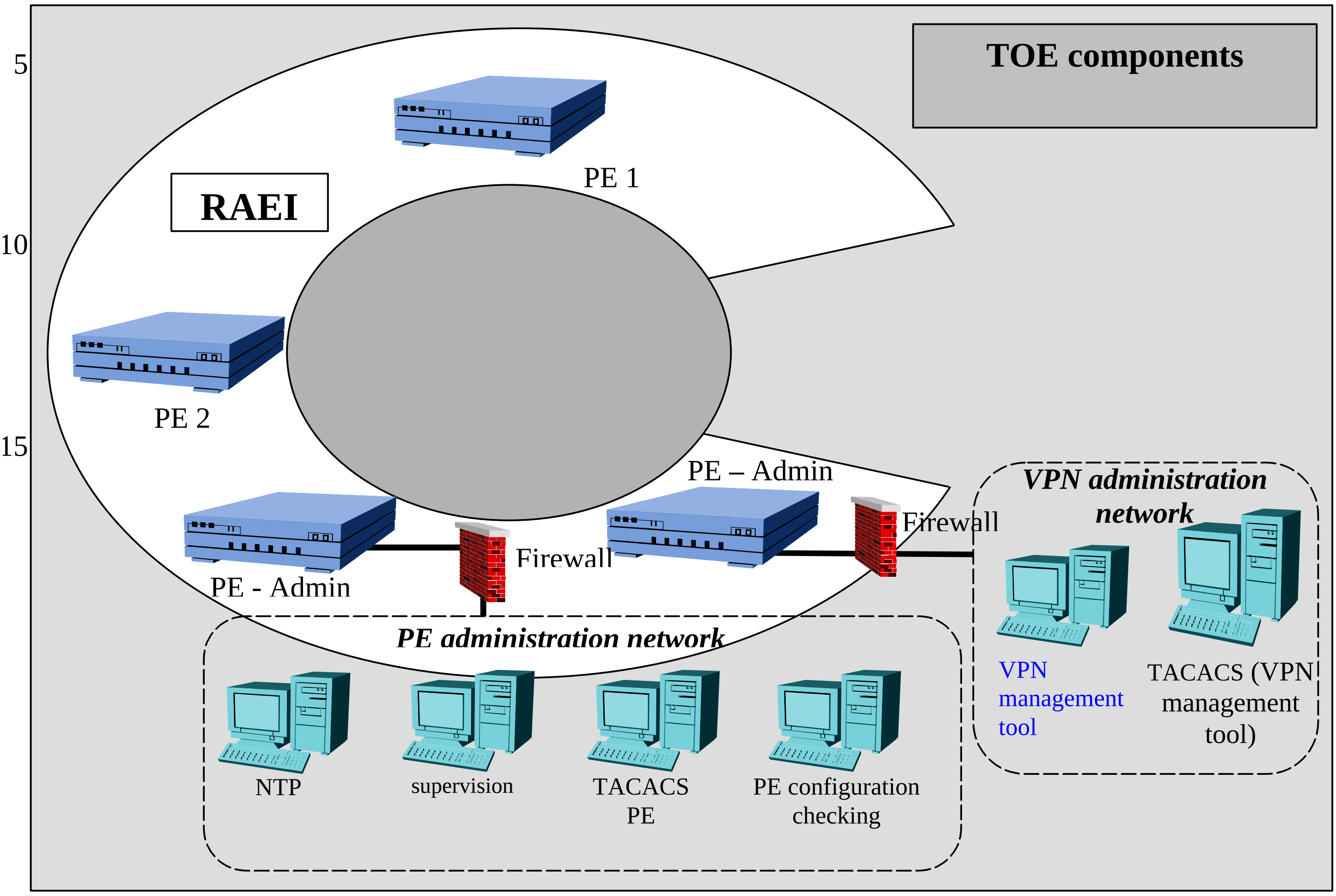
Supervision server can only be accessed from PE management network. Any access to this server is impossible from outside this network.
The time server (NTP) provides a shared time base betwween the TOE components (PE, TACACS server,…).

VPN management tool TACACS server is used by VPN management tool to authenticate VPN administrators and to allow them to connect to the server.
VPN administrators and PE administrators are different persons :
VPN administrators are in charge of producing and managing customer's network. But they are not allowed to manage PE routers : their personal accounts are handled by a TACACS server which is different from the PE administrators one. This TACACS server is under the VPN management tools administrators.
VPN administrators use the VPN management tool and its TACACS server as simple users and have no administrative privileges on these hosts.
They have the full control on VPN management and can only create, modify or delete customer's VPN on PE routers via VPN management tool. They have no way to connect directly to the PE routers as the PE TACACS server does not know their accounts. On the other hand, they have full control on CE router's (located at customer's edge) but those routers are out of the TOE scope. VPN management tool software access PE routers via a dedicated administrative VPN.

All administrators are assumed to be trusted users of the TOE, so that they cannot be considered as a threat agent.


A customer
Network 1
RED VPN
LAN
CE 1-A
B customer
Network 1
GREEN VPN
LAN
CE 1-B
Responsability boundaries
Administrative VPN
Red VPN
Green VPN
LAN
CE 2-B
B customer
Network 2
GREEN VPN
RAEI
PE 1
P
P
PE 2
Internet
RBCI
P
P
PE - Admin
Firewall
PE - Admin
Firewall
VPN administrators
VPN management tool
TACACS (VPN management tool)
Administration Network
CE 2-A
A customer
Network 2
RED VPN
Réseau local
PE administrators
NTP
Supervision
TACACS (PE)
PE configuration checking

In order to preserve readability , TOE boundaries have not been drawn on the last page's figure. TOE is defined as the set of components included in the next figure :



VPN / MPLS technical overview

MPLS technology and more precisely MPLS/VPN lies on tags distribution and their use in traffic switching. Tags are identifiers inserted between data link and network layers which allow to associate each datagram with a defined flow. Packets handled by MPLS are no longer layer 3 routed datagrams but MPLS packets that are switched by specific mechanisms.
There are two levels of tags :

- tags used to switch packets in the core of the backbone,
- tags used to create VPN.

(a) The first ones (or **internal tags**) are used to make the MPLS network work. They are handled by P routers. These routers don't know about external tags. They only switch first level tags.

(b) The second ones (or **external tags**) are only used by PE routers to switch to the right VPN. They are not modified during packets transport. Only PE routers know about those tags.

PE routers at VPN termination have a dedicated routing table associated with each VPN : the VRF (VPN Rounting and Forwarding table) and a global routing table. VRFs and the global routing table are totally independent from each others. For each PE/CE interface on a router, the associated VRF is built dynamically by routing information exchanges between CE and PE. The VRF is used to find which addresses are accessible in this VPN from this PE.

In a MPLS/VPN on a PE router, addresses used ares 96 bits VPN-IPV4 adresses. These adresses are built from a 64 bits "Route Distinguisher" (RD) and the 32 bits IP address.

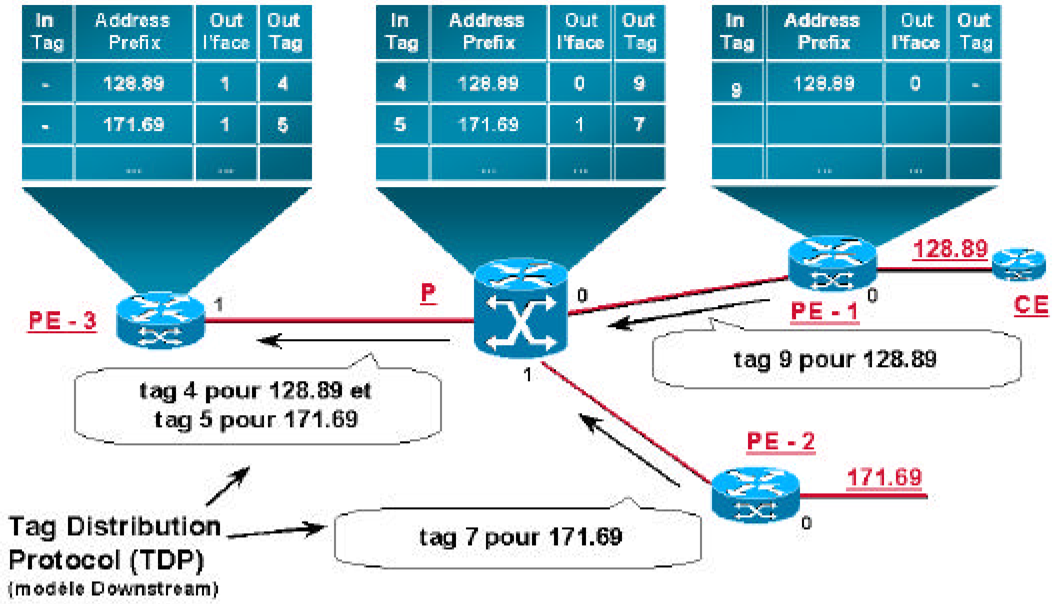
$$@VPN / IPv4 = RD + @IPv4$$

The "Route Distinguisher" is unique and characterizes the VPN. So it makes the IP address / VPN couple unique among all the VPN used on the backbone (i.e. IP address spaces of different VPN customers can overlap, their VPN/IPv4 adresses won't overlap).
The RD itself is built from the unique AS number of the provider (given by the NIC – 3215 for Transpac) and a number that identifies the VPN.

$$RD = 3215{:}xxxxNNNNN$$

MPLS/VPN needs a tag switched network in which the tags are used to switch packets of data. Internal tags (or level 1 tags) are distributed using TDP (Tag Distribution Protocol).

How TDP works is explained below.



In Tag	Address Prefix	Out I'face	Out Tag
-	128.89	1	4
-	171.69	1	5
	...	...	

In Tag	Address Prefix	Out I'face	Out Tag
4	128.89	0	9
5	171.69	1	7
	...	...	

In Tag	Address Prefix	Out I'face	Out Tag
9	128.89	0	-
	...	...	

There are 6 steps :

1. PE 1 sets a tag (here 9) for the flow incoming its interface n° 0 (IP : 128.89).
2. It distributes this tag to its neighbor (here a P router) using TDP.
3. PE 2 does the same and distributes the transport tag (here 7) for its interface n° 0 (IP : 171.69).
4. P receives tags associated with each of its interfaces (9 for interface 0 and 7 for interface 1) and the IP adresses associated with each interface/tag couple.
5. It sets its own tags for each received tags (4 for 128.89 et 5 for 171.69) and ditribute it to its neighbors (here PE 3).
6. PE 3 receives tags on its interface n° 1 and stores them in its tags table in order to be able to set a tag for each switched packet.

When an IP packet incomes a network interface associated to a VPN on a PE router, the router tags this packet with an external tag. This external tag identifies the VPN. Then, it looks in the VRF associated with the interface to find where to forward the packet. Then it sets the internal tag in order to switch the packet to the right destination. This tag is used to forward the packet to the next router.

Data Link (Level 2)	**Internal Tag** (modified in the backbone)	**External Tag** (VPN / IPv4 address)	IP (original level 3 packet)

Next routers on the packet way are P routers. They can not modify the external tag. They only switch packets according to the first level tag. This tag is modified in each router in order to switch the packet to the next router.
The last router in the backbone is a PE router (one at each end). When it receives the packet, it removes the internal tag and then, according to the external tag and the VRF, it knows to which VPN the packet belongs and on which interface it has to be forwarded. It removes the external tag and sends the packet (original IP packet) to the CE.

Routing and switching tables are ditributed in two ways regarding the type of tag :

- TDP protocol is used for PE-P and P-P internal tags switching tables exchanges.
- IS-IS is used for routing tables exchanges between PE routers.
- MPiBGP is used between PE at VPN ends to exchange VRF used for external tags switching.

MPiBGP is only used between PE routers that end the same VPN.

3 Security of TOE environment

3.1 Assumptions

Following assumptions are made on TOE environment :

H1 . Transpac enforces directly or indirectly physical access control to all TOE routing devices.
H2 . Routing devices outside RAEI (i.e. : RBCI) are subject to the same rules for configuration and physical protection as those on RAEI.
H3 . Administrators of all TOE components are trained on the equipments they are responsible for.
H4 . Traffic established in a VPN (PE to PE) can only be routed in Transpac AS.
H5 . PE administrators are not allowed to modify VPN configurations. Only VPN management tool is supposed to make these configurations.

3.2 Threats

Attack methods listed for each threat are given as examples and are not exclusive.

M1. A user establishes a data flow between his VPN and another customer's VPN.

Agent	Malicious customer
Attack	Packets forging
Asset	Customer data flow

M2. A hacker establishes from Internet a data flow to a customer's VPN.

Agent	External hacker
Attack	Packets forging
Asset	Customer data flow

M3. A hacker listens data flows on the network using a logical access to the network.

Agent	Malicious user, external hacker, Transpac employee
Attack	Backbone traffic sniffing (AS Transpac) from a customer access (VPN or Internet)
Assets	Customer data flow PE configuration VRF routing information

M4. A hacker modifies data flows content in the network using a logical access to the network.

Agent	Malicious user, external hacker, Transpac employee
Attack	Backbone traffic modification (AS Transpac) from a customer access (VPN or Internet)
Assets	Customer data flow PE configuration VRF routing information

M5. A hacker gets full control of a PE router

Agent	External hacker or malicious customer
Attack	PE administrator identity spoofing
Assets	PE Configuration

M6. A hacker gets full control of a management tool.

Agent	Attaquant extérieur ou client mal intentionné
Attack	Usurpation de l'identité d'un administrateur de VPN
Asset	PE configuration

M7. An administrator error leads to a disclosure in traffic separation.

Agent	PE or VPN administrator
Attack	Configuration error
Asset	Customer data flow

3.3 Organisational Security Policies

OG1. Cryptographic secrets management security policy
Policy defining how MD5 keys used for MPiBGP signing are generated and distributed

OG2. Passwords management security policy
Policy defining the way the passwords used for VPN administrators authentication on VPN management tool are generated and distributed.

OG3. Audit logs management and checking
Policy defining the way audit logs are generated and checked.

OG4. TOE routing devices operation and maintenance security policy
All TOE routing devices are under Transpac responsibility. Transpac operates and maintains these devices.

4 Security objectives

4.1 TOE security objectives

O1. TOE enforces that no traffic can pass between :

- two networks connected to PE interfaces belonging to different VPN.
- a network connected to a PE interface belonging to a VPN and a network connected to a PE interface belonging to no VPN.

O2. TOE enforces that no traffic can pass between Internet and a network connected to a PE interface belonging to a VPN.

O3. TOE enforces that VRF information are exchanged only between PE supporting the same VPN.

O4. TOE enforces VRF integrity during their transit between PE routers.

O5. TOE enforces that PE and VPN can only be managed by authorized Transpac employees or tools.

O6. TOE enforces PE configurations integrity

O7. TOE enforces that every management action is logged.

O8. TOE enforces that remote VPN management is done through a trusted path.

Note : traffic is assumed to be full-duplex.

4.2 Environment security objectives

4.2.1 From assumptions (not derived in requirements)

EH1 . Transpac enforces a physical access control on PE routers.

EH2 . Routing devices outside RAEI (i.e. : RBCI) are subject to the same configuration rules as those on RAEI.

EH3 . Routing devices outside RAEI (i.e. : RBCI) are subject to the same physical protection rules as those on RAEI.

EH4 . VPN administrators are trained to use VPN management tool .

EH5 . Traffic in a VPN or management traffic can only be routed in Transpac AS.

EH6 . Only VPN administrators are allowed to modify VPN configurations on PE routers.

4.2.2 From security policies (derived in requirements)

EP1 . MD5 keys used for MPiBGP packets signing must be generated and ditributed according to cryptographic secrets management security policy.

EP2 . Passwords used for identification / authentication on VPN management tool must be generated and distributed according to passwords management security policy.

EP3 . Audit trails must be analyzed according to audit logs management security policy.

EP4 . Transpac must operate and maintain TOE equipments according to TOE routing devices operation and maintenance security policy.

5 TI security requirements

5.1 TOE security requirements

5.1.1 TOE functional security requirements

For readability, functional requirements are named according to the sensible asset they apply on. They are called Requirement_xxx where xxx is :

- FLU when they apply to customer data flow
- CPE when they apply to PE
- VRF when they apply to VRF
- VPN when they apply to VPN tags

	Assets			
	User data	**TSF data**		
	Customers data flow	PE Configuration	VRF	VPN tags
FDP_ACC.2	●			
FDP_ACF.1	●			
FDP_ETC.1	●			
FDP_ITC.1	●			
FDP_ITT.2	●			
FAU_TRA.1		●		
FAU_GEN.2		●		
FAU_SAR.1		●		
FAU_SAR.2		●		
FAU_STG.1		●		
FDP_SDI.2		●		
FIA_UAU.2		●		
FIA_UAU.6		●		
FIA_UID.2		●		
FMT_MTD.1		●		
FMT_SMR.1		●		
FPT_ITT.2		●		
FPT_STM.1		●		
FTA_TSE.1		●		
FTP_TRP.1		●		
FCS_COP.1			●	
FDP_ACC.2			●	
FDP_ACF.1			●	
FPT_ITT.3			●	
FMT_MSA.1				●
FMT_MSA.3				●

5.1.1.1 CUSTOMERS DATA FLOW

FDP_ACC.2_FLU - Total access control

FDP_ACC.2.1_FLU The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] and all operations among subjects and objects covered by the SFP.

assignment: *access control SFP* = VPN access policy.
assignment: *list of subjects and objects* = customers data flow : subjects = customers ; objects = customers data flow

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

FDP_ACF.1_FLU - Security attribute based access control

FDP_ACF.1.1_FLU The TSF shall enforce the [assignment: *access control SF*P] to objects based on [assignment: *security attribute*s, *named groups of security attributes*].

assignment: *access control SFP* = VPN access policy
assignment: *security attributes*, *named groups of security attributes* = VPN/IPv4 addresses

FDP_ACF.1.2_FLU The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled object*s].

assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled object*s = a customer's data flow entering a VPN interface on a PE router is tagged with the VPN tag associated with this interface. This flow is forwarded through the PE to another PE only if the VPN/ipv4 destination address belongs to the VRF associated with the customer's VPN interface on the originating PE. On the destination PE, the flow is forwarded to the interface associated with this VPN.

FDP_ACF.1.3_FLU The TSF shall explicitly authorise access of subjects to objects based on the following additional rules [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

assignment: *rules, based on security attributes, that explicitly authorise access of subjects to object*s = not applicable

FDP_ACF.1.4_FLU The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to object*s].

assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects* = all data flows between VPN interfaces that are not allowed by the corrsponding VRF on the PE are forbidden. A flow can never be forwarded between a VPN and a non VPN interface.

FDP_ETC.1_FLU - Export of user data without security attributes

FDP_ETC.1.1_FLU The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s*)] when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.1.2_FLU The TSF shall export the user data without the user data’s associated security attributes.

refinement: *user data* = customer's data flow
refinement: *user data’s associated security attributes* = VPN/IPv4 addresses
assignment: *access control SFP and/or information flow control SFP* = VPN access policy

<u>FDP_ITC.1_FLU - Import of user data without security attributes</u>

FDP_ITC.1.1_FLU The TSF shall enforce the [assignment: *access control SFP and/or information flow control SF*P] when importing user data, controlled under the SFP, from outside of the TSC.

assignment: ***access control SFP and/or information flow control SFP*** **= VPN access policy**

FDP_ITC.1.2_FLU The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

refinement: ***security attribute*** **= VPN/IPv4 addresses**

FDP_ITC.1.3_FLU The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rule*s].

assignment: ***additional importation control rule*****s = not applicable**

<u>FDP_ITT.2_FLU - Transmission separation by attribute</u>

FDP_ITT.2.1_FLU The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s*)] to prevent the [selection: *disclosure, modification, loss of use*] of user data when it is transmitted between physically-separated parts of the TOE.

assignment: ***access control SFP(s) and/or information flow control SFP(s*****) = VPN access policy**
selection: ***disclosure, modification, loss of use*** **= disclosure**

FDP_ITT.2.2_FLU The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following: [assignment: *security attributes that require separation*].

assignment: ***security attributes that require separation*** **= VPN / IPv4 addresses**

5.1.1.2 PE CONFIGURATIONS

<u>FAU_TRA.1_CPE - Audit data generation</u>

FAU_TRA.1.1_CPE The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
Refinement: not applicable on TACACS server because audit function is always on. On VPN management tool, audit can be desactivated.

b) All auditable events for the [selection: *minimum, basic, detailed, not specifie*d] level of audit; and
c) [assignment: *other specifically defined auditable event*s].

selection: *minimum, basic, detailed, not specifie*d = not specified
assignment: *other specifically defined auditable events* = events listed below :

- **Authentication on the router (successful or not).**
- **Router configuration modification.**
- **Corrupted VRF data reception.**

FAU_TRA.1.2_CPE 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
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant informatio*n]

assignment: *other audit relevant information* = a text describing the event so that audit can be done by simply reading logfiles.

FAU_GEN.2_CPE - User identity association

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

refinement: *user* = PE or VPN administrators

FAU_SAR.1_CPE - Audit review

FAU_SAR.1.1_CPE The TSF shall provide [assignment: *authorised user*s] with the capability to read [assignment: *list of audit informatio*n] from the audit records.
FAU_SAR.1.2_CPE The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1.1_CPE.2
assignment: *authorised user*s = PE administrators
assignment: *list of audit information* = logfiles content
FAU_SAR.1.2_CPE.2
refinement: *user*s = PE administrators

FAU_SAR.2_CPE - Restricted audit review

FAU_SAR.2.1_CPE The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.1_CPE - Protected audit trail storage

FAU_STG.1.1_CPE The TSF shall protect the stored audit records from unauthorised deletion.
FAU_STG.1.2_CPE The TSF shall be able to [selection: *prevent*, *detec*t] modifications to the audit records.

selection: ***prevent, detec*****t = prevent**

FDP_SDI.2_CPE Stored data integrity monitoring and action

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity error*s] on all objects, based on the following attributes: [assignment: *user data attribute*s].

refinement: ***user data*** **= PE configuration**
assignment: ***integrity errors*** **= all integrity errors and modifications**
assignment: ***user data attributes*** **= diff between PE configuration of the day and the day before.**

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *action to be take*n].

assignment: ***action to be taken*** **= send an e-mail with differences between the configuration of the day and the day before.**

FIA_UAU.2_CPE - User authentication before any action

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

refinement: ***user*** **= PE administrators, VPN administrators**

FIA_UAU.6_CPE - Re-authenticating

FIA_UAU.6.1_CPE The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is require*d].

refinement: ***user*** **= PE administrators**
assignment: ***list of conditions under which re-authentication is require*****d = the last authentication on the PE was more than 30 minutes ago**

FIA_UID.2_CPE - User identification before any action

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

refinement: *user* = PE or VPN administrators / management tools

FMT_MTD.1_CPE - Management of TSF data

FMT_MTD.1.1_CPE The TSF shall restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, *clea*r, [assignment: *other operations*]] the [assignment: *list of TSF dat*a] to [assignment: *the authorised identified role*s].

FMT_MTD.1_CPE is iterated twice.

FMT_MTD.1.1_CPE.1
selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*] = set, modify, delete
assignment: *list of TSF data* = PE configuration
assignment: *the authorised identified roles* = PE administrators

FMT_MTD.1.1_CPE.2
selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*] = set, modify, delete
assignment: *list of TSF data* = VPN configuration on PE
assignment: *the authorised identified roles* = VPN administrators

FMT_SMR.1_CPE - Security roles

FMT_SMR.1.1_CPE The TSF shall maintain the roles [assignment: *the authorised identified role*s].

assignment: *the authorised identified roles* = PE administrators, VPN administrators

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

refinement: *users* = administrators

FPT_ITT.2_CPE - TSF data transfer separation

FPT_ITT.2.1_CPE The TSF shall protect TSF data from [selection: *disclosure*, *modificatio*n] when it is transmitted between separate parts of the TOE.

refinement: *TSF data* = management commands issued by VPN management tool

selection: *disclosure, modification* = disclosure and modification

FPT_ITT.2.2_CPE The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

refinement: *user data* = customers data flows
refinement: *TSF data* = management commands issued by VPN management tool

<u>FPT_STM.1_CPE - Reliable time stamps</u>

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

<u>FTA_TSE.1_CPE - TOE session establishment</u>

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: *attribute*s].

assignment: *attributes* = addresses and ports of the management network forbidden from the outside (network filtering)

<u>FTP_TRP.1_CPE - Trusted path</u>

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

selection: *remote, loca*l = remote
refinement: *users* = VPN administrators

FTP_TRP.1.2_CPE The TSF shall permit [selection: *the TSF, local users, remote user*s] to initiate communication via the trusted path.

selection: *the TSF, local users, remote user*s = remote users
refinement: *users* = VPN administrators via VPN management tool

FTP_TRP.1.3_CPE The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is require*d]].

selection: *initial user authentication*, [assignment: *other services for which trusted path is require*d] = VPN administrators using VPN management tool

5.1.1.3 VRF TABLES

<u>FCS_COP.1_VRF - Cryptographic operation</u>

FCS_COP.1.1_VRF The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

assignment: *list of cryptographic operations* = BGP routing tables hash
assignment: *cryptographic algorithm* = MD5
assignment: *cryptographic key sizes* = MD5 diversification key is composed of 10 characters including 2 non alphanumerics and a diversifiant that is different for each packet
assignment: *list of standards* = MD5

<u>FDP_ACC.2_VRF - Total access control</u>

FDP_ACC.2.1_VRF The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] and all operations among subjects and objects covered by the SFP.

assignment: *access control SFP* = VRF exchange between PE policy : VRF exchange only allowed between PE involved in a same VPN.
assignment: *list of subjects and objects* = subject : PE ; object : VRF

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

<u>FDP_ACF.1_VRF - Security attribute based access control</u>

FDP_ACF.1.1_VRF The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes, named groups of security attributes*].

assignment: *access control SFP* = VRF exchange between PE policy (see description above)
assignment: *security attributes, named groups of security attributes* = RD

FDP_ACF.1.2_VRF The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects* = VRF exchange is only allowed between PE

mutually declared as BGP neighbors. RD of routes exchanged must have been allowed for import and export on each of the two PE.

FDP_ACF.1.3_VRF The TSF shall explicitly authorise access of subjects to objects based on the following additional rules [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects* = not applicable

FDP_ACF.1.4_VRF The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects* = all VRF exchanges between PE that are not declared as BGP neighbors or using RD not authorised by import/export rules are denied.

FPT_ITT.3_VRF TSF data integrity monitoring

FPT_ITT.3.1_VRF The TSF shall be able to detect [selection: *modification of data, substitution of data, re-ordering of data, deletion of data*, [assignment: *other integrity errors*]] for TSF data transmitted between separate parts of the TOE.

selection: : *modification of data, substitution of data, re-ordering of data, deletion of data,* [assignment: *other integrity errors*] = VRF modification

FPT_ITT.3.2_VRF Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: *specify the action to be taken*].

assignment: *specify the action to be taken* = ignore VRF data received ang log the event.

5.1.1.4 VPN TAGS

FMT_MSA.1_VPN - Management of security attributes

FMT_MSA.1.1_VPN The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

assignment: *access control SFP, information flow control SFP* = VPN management function access policy
selection: *change_default, query, modify, delete,* [assignment: *other operations*] = set, modify or delete
assignment: *list of security attributes* = VPN tag associated to each interface

assignment: *the authorised identified role*s = VPN administrators

FMT_MSA.3_VPN - Static attribute initialisation

FMT_MSA.3.1_VPN The TSF shall enforce the [assignment: *access control SFP, information flow control SF*P] to provide [selection: *restrictive, permissive, other propert*y] default values for security attributes that are used to enforce the *SF*P.

assignment: *access control SFP, information flow control SF*P = VPN access policy
selection: *restrictive, permissive, other propert*y = restrictive

FMT_MSA.3.2_VPN The TSF shall allow the [assignment: *the authorised identified role*s] to specify alternative initial values to override the default values when an object or information is created.

assignment: *the authorised identified role*s = nobody

5.1.2 TOE security assurance requirements

EAL1	*ACM_CAP.1*	Version numbers
	ADO_IGS.1	Installation, génération and start-up procedures
	ADV_FSP.1	Informal functional specification
	ADV_RCR.1	Informal correspondance demonstration
	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
	ATE_IND.1	Independent testing – conformance
Augmentation	*AVA_VLA.2*	Independent vulnerability analysis
	ADV_HLD.1	Descriptive high-level design

5.2 Environement security requirements

ESE1 . MD5 keys used for MPiBGP packets signing are generated and delivered according to « cryptographic secrets management security policy ».

ESE2 . Passwords used for authentication on VPN management tool are generated and delivered according to « passwords management security policy ».

ESE3 . Audit trails are analyzed according to "audit logs management security policy".

ESE4 . Transpac operates and maintains TOE equipments according to "TOE routing devices operation and maintenance security policy".

6 TOE specifications

6.1 TOE security functions

SF1. VPN flows access control

A flow between customers networks passes through PE routers. A PE allows a flow from a customer network connected to one of its VPN interfaces only if this flow destination is known in the VRF of the VPN associated with this interface.

SF2. Non-VPN flows access control

A PE never allows a flow from a customer network connected to one of its non-VPN interfaces to be forwarded to a customer network reachable through a VRF.

SF3. VRF exchange

A VPN is identified by its RD which is known by all PE involved in this VPN. Only PE knowing this RD can exchange VRF data relative to this VPN.

SF4. VRF exchange integrity

During VRF data exchanges between PE, the originating PE computes a hash of the data and sends it with the data to the receiving PE (belonging to the same VPN). This PE also computes the hash of the received data and compares it with the received hash. If the two hashes are equal, it accepts the data otherwise it refuses and drops the data.

The hash is computed using MD5 diversified by a secret key generated by Transpac and shared only by the RAEI PE. This key caracteristics are defined in cryptographic secrets management policy document.

SF5. Identification / Authentication on VPN management tool

Remote access to VPN management tool is submitted to previous authentication. This identification / authentication is done by VPN management tool in a HTTP form. Each VPN administrator has his own login. This authentication is based on login/password and relies on the TACACS server used by VPN management tool.

SF6. Identification / authentication on PE

Remote access to PE is based on login/password. This authentication relies on PE TACACS server. Each PE administrator has his own login. VPN management tool proceeds as a PE administrator to authenticate on PE. VPN management tool also has its own login.

When authentication succeeds, PE TACACS server sends user profile to the PE.

SF7. management functions access control

VPN administrators can not connect directly to PE. They must use VPN management tool. Management data flow, produced by VPN management tool, are transmitted in a dedicated VPN.

SF8. Management Network access control

The access to the network hosting management tools is controled by network filtering.

SF9. Management actions audit

All events relatives to PE or VPN management are logged on the corresponding TACACS server. PE log all the events relatives to them. VPN management tool only logs VPN management relative events. PE administrators have access to all the logs and VPN administrators have access to VPN management tool logs.

SF10. PE configuration checking

PE configurations are backed up daily on the configuration checking server. They are compared with the configuration backed up the day before. If a change is detected, an alert is sent by e-mail to the PE management tools administrator.

SF11. VPN management

VPN management tool can only create or delete VPN. By default a customer access belongs to none of the VPN. PE administrators can create, modify or delete the entire PE configuration.

SF12. Reliable time base

TOE has a reliable time base delivered by a NTP server.

6.2 Assurance measures

AM1. TOE identification

TOE is identified by the version numbers of all its components (PE IOS version number, VPN management tool version number, ...).

These version numbers are not easy to know for a customer, so he will not be able to check by himself the version numbers of the components used. TOE configuration is given in 2.2.1 an 2.2.2 of this document. These paragraphs are the delivery for ACM_CAP.1 requirement.

AM2. Installation, generation and start-up

PE receipt is out of the scope of this security target. Production (personalization and configuration) is documented in [Installation et configuration des PE]. This measure is compliant with ADO_IGS.1.

AM3. Functional specifications

[Spécifications fonctionnelles de la TOE] document includes TSF and its external interfaces description. This measure is compliant with ADV_FSP.1.

AM4. Informal correspondence demonstration

[Démonstration informelle de correspondance] document includes :

- correspondence between global TOE specifications and functional specifications,
- correspondence between functional specifications and high level design.

This measure is compliant with ADV_RCR.1.

AM5. Administrator guidance

[Manuels d'administration de Global Intranet] documents describe all the possible states of configuration elements of the system :

- PE routers

- VPN management tool
- TACACS (PE and VPN management tool)
- PE configuration checking tool

They also describe the way to safely manage the TOE
This measure is compliant with AGD_ADM.1 and contributes to AVA_VLA.2 (by defining safe management procedures that counter exploitation vulnerabilities).

AM6. User guidance

[Manuels utilisateur de Global Intranet] document describes TOE security functions available for the user.
This measure is compliant with AGD_USR.1 and contributes to AVA_VLA.2 (by defining safe TOE using procedures that counter exploitation vulnerabilities).

Note : due to complete transparency of this service, no user manual is given to the MPLS/VPN customer. Only a memo containing support phone number is given to the customer.

AM7. TOE availability for tests purposes

TOE is available for security and functional tests. A platform corresponding to the figure in introduction section is built for TOE evaluation. This platform includes two VPN for two different fake customers and the management tools used in production environment..
This measure is compliant with ATE_IND.1 (independant testing - compliance) and contributes to AVA_VLA.2 (for penetration testing).

AM8. [Analyse des vulnérabilités du MPLS/VPN sur réseau RAEI] document contains independent TOE vulnerability analysis and a rationale that sthows these vulnerabilities are not exploitable. This measure contributes to AVA_VLA.2.

AM9. TOE high level design availability

[Conception de haut niveau de la TOE] document describes general structure of the TSF, the different subsystems part of it and their external interfaces. This measure is compliant with ADV_HLD.1

6.3 Assurance requirements / assurance measures correspondance

	AM1	AM2	AM3	AM4	AM5	AM6	AM7	AM8	AM9
EAL1									
ACM_CAP.1	●								
ADO_IGS.1		●							
ADV_FSP.1			●						
ADV_RCR.1				●					
AGD_ADM.1					●				
AGD_USR.1						●			
ATE_IND.1							●		
Augmentation									
AVA_VLA.2					●	●		●	
ADV_HLD.1									●

6.4 Security measures for environnement

EM1. MD5 keys used for MPiBGP packets signing are generated and delivered according to « cryptographic secrets management security policy ».
Ref : PE-SECURITE/ENG.COG.001-F.

EM2. Passwords used for authentication on VPN management tool are generated and delivered according to « passwords management security policy ».
Ref : CSI/EXM IT 023

EM3. Audit trails are analyzed according to "audit logs management security policy".
Ref : RADEQUA/EXM /MU001

EM4. Transpac operates and maintains TOE equipments according to "TOE routing devices operation and maintenance security policy".
Ref : CSI/EXM IT 023

7 Glossary

AS Autonomous System defined as the part of Internet managed autonomously by a unique administrative entity (operator). AS is characterised by the unicity of routing policy.
AS number is unique.

BGP Border Gateway Protocol is a routing table distribution protocol.

CE Customer Edge router used to connect customers networks to the RAEI.

Customer User of MPLS / VPN.

MPiBGP Routing protocol similar to BGP .

MPLS Multi Protocol Label Switching is a packet switching protocol. See section 2.2.6

P Provider routers (in the core of the backbone – RBCI).

PE Provider Edge routers (at the edge of the backbone – RAEI).

RAEI "Réseau d'Accès pour les Entreprises à Internet". This network is located in France.

RBCI "Réseau Backbone Connecté à Internet". This network is located in France.

RD Route Distinguisher (see introduction section)

TACACS Terminal Access Controller Access Control System

TDP Tag Distribution Protocol see section 2.2.6.

VPN A VPN (Virtual Private Network) is a private network built on a public network. It relies on traffic separation that is not necessarely cryptographic.

VRF VPN Routing and Forwarding tables are exchanged between PE to enforce routing in a VPN.

8 References

Access to all these references except *[Manuels utilisateur de Global Intranet]* is restricted.

[Installation et configuration des PE]	***Fourniture ADO_IGS - Projet VIOLETTE*** *Global One*, PE-SECURITE/ENG COG 002, 6/02/2001.
[Spécifications fonctionnelles de la TOE]	***Fourniture ADV_FSP - Projet VIOLETTE, version 1.4*** Global one, PE-SECURITE-ENG SPE 001, 22/05/01.
[Démonstration informelle de correspondance]	***Fourniture ADV_RCR 1/2 - Projet VIOLETTE, version 1.0*** Global One, PE-SECURITE/ENG SPE 002, 30/05/01 ***Fourniture ADV_RCR 1/2 - Projet VIOLETTE, version 1.0*** Global One, PE-SECURITE/ENG SPE 003, 30/05/01
[Manuels d'administration de Global Intranet]	***Fourniture AGD_ADM - Projet VIOLETTE, version 1.2*** Global One, PE-SECURITE/ENG COG 003, 31/05/01
[Manuels utilisateur de Global Intranet]	***Fourniture AGD_USR - Projet VIOLETTE, version 1.0*** Global One, PE-SECURITE/ENG COG 004, 30/05/01
[Conception de haut niveau de la TOE]	***Fourniture ADV_HLD - Projet VIOLETTE, version 1.3*** Global One, PE-SECURITE-ENG ARC 002, 28/05/01
[Analyse des vulnérabilités du MPLS/VPN sur réseau RAEI]	***Fourniture AVA_VLA - Projet VIOLETTE, version 1.5*** Global One, PE-SECURITE/ENG TST 001, 11/06/01