Business Services

Equant IPVPN

Public security target for the Equant IPVPN service – international perimeter

Reference: AGUI-7F8GPQ
Version 1.0 ; 02/06/2008

Table of contents

Table of figures

Table of tables

1-Introduction

1.1-Identification

Identity of the ST	Public Security Target for the Equant IP VPN service - international perimeter.
Version of the ST	version 1.0 (public version) (02/06/2008) This document describes the public security target extracted from the evaluated version (security target v3P6)
Authors	Orange Business Services
Identity of the TOE	**Equant IPVPN Service - International Perimeter**
Version of the TOE	1.0 - version associated to the ALC-CMS and ALC-CMC delivery in version 1P5

1.2-Target of Evaluation Overview

The Target of Evaluation (TOE) is the Equant IPVPN service offered by Orange Business Services. The evaluation of the TOE consists of a "system evaluation" within the French security certification scheme (Certification Body: DCSSI).

The Equant IPVPN service was launched in 1999 and is available in 146 countries with five classes of differentiated and prioritized services: voice, video and three data classes for customers' business applications. This core solution can enable a simplified and efficient communication infrastructure, which operates 24x7 anywhere customers do business using mobile, wireless, DSL, Ethernet or optical transport.

To support this service, France Telecom uses the IP Global Network (IGN), a backbone based on the MPLS/VPN technology, which allows Orange Business Services to provide its customers with virtual private networks (VPN).

From a security perspective, the Equant IPVPN service is designed and operated to guarantee the following properties:

- Isolation of customer VPNs among each others, at layer 3;
- Backbone router integrity and access control;
- Proper interfaces with VPN partners, for VPNs that need to be extended to areas France Telecom does not cover;
- For the NBIG and SIA customers, controlled interconnection of their VPNs with the Internet (while maintaining the isolation between VPNs).

The security provided by the service is based on:

- The MPLS/VPN technology implemented in the routers;
- Controlled accesses to IGN network devices;
- Administration services ensuring:
  - the conformity of router configurations with regard to security templates and security policies
  - verification of the integrity of the VPNs

It relies both on the equipment in the IGN and on administration equipment deployed in premises that are under the control of France Telecom.

1.3-TOE Description

This sections aims at providing a precise description of the Target Of Evaluation (TOE).

It begins with a quick description of the MPLS/VPN technology on which the service is based (section 1.3.1-). It then describes the services the system offers, not only in terms of services offered to the customer, but also in terms of interactions with the administration and monitoring teams (see section 1.3.2-). A focus is then made on the ways the VPNs may interact with the Internet (see 1.3.3-).

Finally, a high-level description of the internal design of the TOE is provided (section 1.3.4-), as well as a description of the possible sources of interaction, i.e. a clarification of the environment of the TOE (section 1.3.5-).

1.3.1-Principles of MPLS/VPN Technology

At a basic level, remote sites of different customers are connected to the same backbone. The goal is to separate the customers' flows logically in order to maintain one or several virtual private networks for each customer.

Rather than directly routing the IP packets in the network on the basis of their IP address, the MPLS (Multi Protocol Label Switching) protocol is based on lower-level labels. The commutation is therefore carried out on data belonging to OSI level 2 and not on data belonging to OSI level 3 such as IP addresses.

Thus, to ensure VPN flow isolation, two levels of labels are used:

- The first level of labels is used to forward packets on the core network. Only "Provider" routers (P routers) that constitute the core network are handling these labels.
- The second level of labels is managed by Provider Edge routers (PE routers), that constitute the interface between the customers' routers (CE routers) and the core network.

To define the VPNs a unique Route Distinguishers (RD) is associated to each VPN.

Each PE router is configured to provide as many Virtual Routing and Forwarding tables (VRF) as there are VPNs defined on it. Each VRF table is kept separate from the others. The above-mentioned labels are used to switch frames within a VRF, defining a single VPN. This technique makes it impossible to transfer an IP packet from a given customer to the VPN of another customer.

A good illustration of this is that a customer can define his own IP addressing plan independently from the other ones; this addressing plan can neither come into conflict with the Internet's nor with the other customers'.

Figure 1 provides an overview of how an IP packet is routed in a VPN:

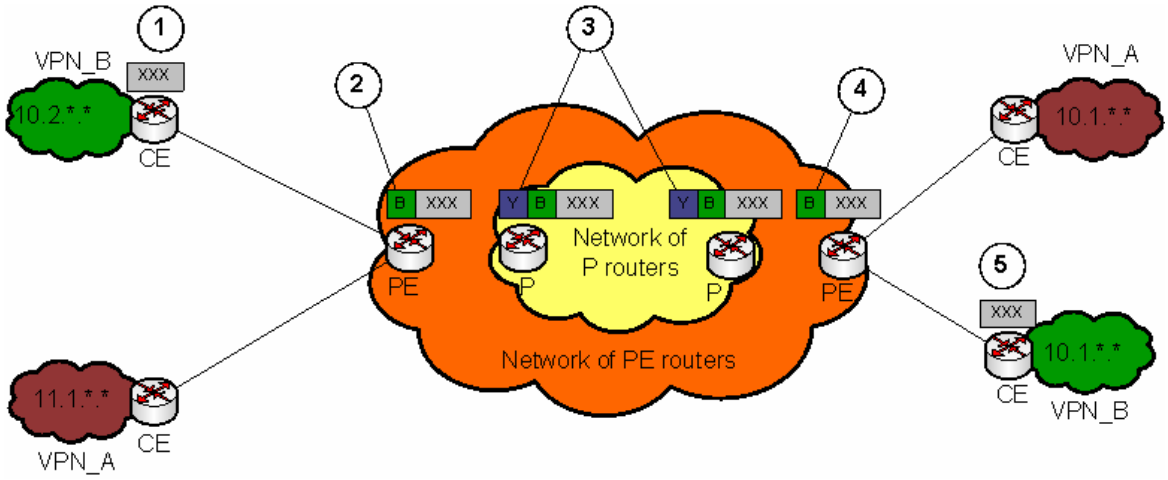

Figure 1: Principles of the MPLS/VPN technology

1) Data is routed from the enterprise's CE router to the PE router to which it is bound;

2) The ingress PE router assigns an external label to the IP packet (RD, in green in the figure); the same label is assigned to all the IP packets received on that interface of the PE.

3) Then, in the core network, level 1 labels are assigned by P router to ensure correct MPLS routing up to the egress PE. Prior to forwarding the IP datagram to the egress PE, the last P router removes the level 1 label;

4) The egress PE router removes the RD;

5) The egress PE routes the IP datagram to the customer CE corresponding to the received RD.

Thus, thanks to the presence of one routing table per VPN on the PE routers, the MPLS/VPN technology guarantees the separation of one VPN from all other VPNs.

In addition, the manipulation of MPLS labels is only performed on devices within Orange Business Services' network, which is fully under France Telecom's responsibility. In other words, the MPLS labels are not known from the CE routers, and therefore the CE routers are not able to manipulate these labels.

1.3.2-Security Services Offered

The TOE guarantees that some security properties are offered to the customer; it supports administration and integrity verification services.

1.3.2.1-Security Properties Offered to the Customers

From a security perspective, France Telecom guarantees the following to the subscribers of the Equant IP VPN service:

> The separation of data flows over the different produced VPN (no flow injection, no flow escape);

> The separation between VPN flows and the other flows (administration flows), with the exception of Internet flows in the specific case of subscribers to the NBIG and SIA offers (see sections 1.3.3- and 1.3.5.2- for further details)

- The network devices in Orange Business Services' infrastructure that are involved in data routing and transmission are not accessible from the Internet and from VPN partners (except ASBR PE interconnections).

1.3.2.2-Service and Infrastructure Administration

Two types of administration activities can be distinguished:

- Infrastructure administration, which consists in the maintenance of the backbone, the installation of new PEs, upgrade of existing PEs, the management of the router administrators' rights, etc.
- VPN and user equipment management, which consists in the management of the VPN configurations, the management of VPN interfaces on the PEs (production of new interfaces, modification or removal of interfaces), and the management of the CEs.

The management of the CEs associated to a VRF is performed through a dedicated management VPN which do no put in danger the integrity of the customer's VPNs.

Organizational and technical means are implemented to separate the two types of activities that are backbone management and customers' VPNs management. In particular:

- A strict hierarchy of access rights is defined to finely control the accesses to the routers. This hierarchy is based in one hand on a scope (types of routers that may be accessed) and, in the other hand, on the type of accesses granted for each scope.
- The teams of administrators authorized to operate on each field are differentiated. A authorization policy is implemented to actually enforce this separation.

To control the access to the devices in the backbone, ControlNet, a dedicated administration network, is implemented to host the various management applications; it constitutes a mandatory access point for the administration of PEs and VPNs. This point is developed in section 1.3.4.2-.

1.3.2.3-Security Monitoring

Data collection

Whatever the administration activity is, administration events are recorded to allow auditing the configuration changes and ensure accountability.

The configuration of the PEs and of the produced VPNs is monitored in order to check that:

- The PE configurations are conformant to defined standards
- Unauthorized ports are not opened

The monitoring tools also ensure that:

- The routers' operations are logged
- The failures of SNMP connections are logged
- The errors on TELNET connections are logged
- Conformity of the VRFs is maintained (SAFE and other tools)

Log concentration and correlation

System data gathering and analysis on the IGN (where the IPVPN P and PE equipments are located) and on administration network (where the IPVPN administration takes place) is done through a network of servers running netForensics software. Logs from P and PE equipments, TACACS authentication servers, administration servers and related equipment such as firewalls is collected and processed through a specialized service.

The netForensics service performs the following actions on the collected data:

- Live alerts: the data is analyzed and filtered through rulesets to isolate suspicious events; detection of such an event is immediately reported to the operational teams.
  This includes data correlation, where information collected from various devices is compared and analyzed together to reveal incidents that might not be visible from a single source.
- Weekly reporting: security reports are produced and analyzed.
- Forensics: should a security incident occur, netForensics can be used to track back the source of the incident and help assess the exact damage.
- Log archiving: collected data is stored for analysis and reporting for a duration of 3 months in a specialized database, after which it is archived on tape and stored for a minimum of 5 years.

1.3.3-Separation of the VPN Flows from the Internet Flows

IGN is a network dedicated to the VPN flows; it is not a multiservice network. This means that no Internet flows are transferred as such over the backbone. On the other hand, Internet traffic may flow within a customer VPN if wanted.

However, Orange Business Services offers three services that require implementing interactions between the subscribers' VPNs and the Internet. These services are the following:

- *Network Based Internet Gateway* (NBIG) is a service that allows customers to vehicle their Internet flows over their own VPN. This implies an interconnection point between the customer VPN and the Internet.
- *Secure ISP Access* (SIA) is a service that allows customers to extend their networks to sites that cannot be directly connected by the IGN. The SIA subscribers' VPNs are extended using IPSEC links, allowing a secure transport of intranet flows over the Internet up to the remote customers' sites.
- *Business Everywhere* (BEW) is a service allowing nomad staff of Equant IPVPN service customers to access their corporate intranet from anywhere they do business. In practice, this requires to define an interaction point where the secured flows from the nomad client are injected in the company's VPN. The principle is the same as the SIA service.

Except for these three well-defined services, the system does not implement interfaces to exchange data with the Internet, in particular at the interfaces with the VPN partners.

The VPNs of customers that are not subscribers of the NBIG, SIA or BEW services are not concerned by these interconnections.

These interactions of VPNs with the Internet, as well as the other interfaces of the TOE will be discussed in further detail in section 1.3.5-TOE Environment.

1.3.4-TOE General Overview

This section presents a general overview of the TOE and of its components.

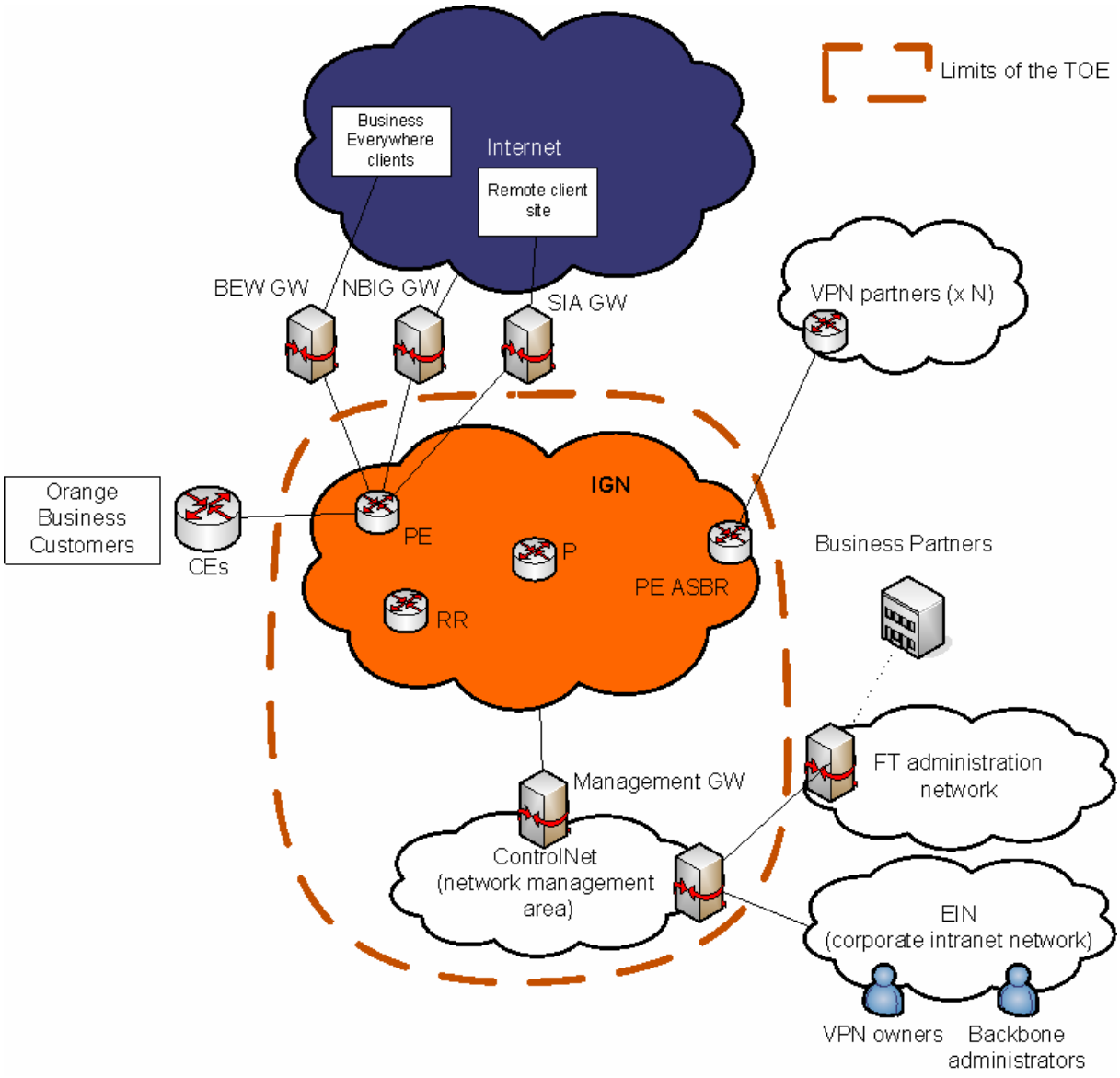

Figure 2 : TOE overview

1.3.4.1-The IGN network

The IGN network is Orange Business Services' international network dedicated to enterprises' VPN flows.

This network is composed of the following elements:

P routers

The IGN network contains P routers that ensure the processing of level 1 MPLS labels. The network of P routers does not process any VPN tags.

These routers are managed by administration teams different from the customers' VPN administration teams.

Route Reflectors (RR)

Route Reflectors act as focal points for MP-iBGP sessions; route reflectors allow advertising routes throughout the network without requiring a full-mesh logical connection of all the other routers.

In the following, the route exchange will be presented from a logical point of view, this means, from one PE to another one.

These specific routers are managed like P routers.

PE routers

The PE routers are the entry points of the network to which the customers' CE can be connected.

A virtual routing and forwarding (VRF) table is associated to each VPN interface of a PE. Each of these tables contains the parameters (Route Distinguisher, import and export route targets, etc.) that characterize the customer's VPN.

At the IP interfaces (backbone side), the routing process of the PE is using the global routing table of the router (GRT). The GRT only serves the purpose of PE administration; it is not used to define Internet routes as usually done in multiservice networks.

PE configurations may be changed either for the purpose of the management of backbone (e.g., creation of new interfaces between other P, PE or RR routers of the backbone) or for the purpose of the management of customers' VPNs (e.g. creation of new customer interfaces, VRFs, …).

ASBR PE

The PE ASBR (Autonomous System Border Router) routers ensure the interconnection with partner networks for countries not covered by IGN.

ASBR PEs are managed like the other backbone equipments (P, PE, RR routeurs).

1.3.4.2-ControlNet: the administration network

As explained previously, the isolation of MPLS VPNs essentially relies 1) on the correct configuration of the VRFs and of the PE at the moment the production is done and 2) on the fact that these configurations continuously strictly adhering to what they should be (i.e. the customers' needs and the operating needs).

Thus, it is important to adequately control access to the network equipment. For this purpose, an administration network, called ControlNet, is established as the sole source of all management actions performed on the IGN backbone. This network hosts and securely operates the management tools needed to manage the routers and the VPNs.

ControlNet constitutes a mandatory access network through which to reach the PEs in order to manage their configurations or the VPNs.

1.3.5-TOE Environment

This section presents the entities that are located outside the boundaries of the target of evaluation and that may interact with it.

1.3.5.1-The customers of the Equant IPVPN service

The customers of the Equant IPVPN service are connected to the IGN through CE routers located within their premises and connected to the PE routers.

1.3.5.2-Business Everywhere, SIA and NBIG customers

As explained in section 1.3.3-, the Business Everywhere, SIA and NBIG services require implementing points of interaction between the customer VPNs and the Internet.

For this purpose, Orange Business Services operates gateways that are located between a PE in its Autonomous System (AS), and the Internet (IAR or GIBN). As such, these gateways are outside the scope of the TOE. In fact, they are outside the AS and unable to handle VPN tags.

The Business Everywhere and SIA gateways play a similar role, identifying and authenticating the remote clients (nomad clients or remote customers' sites) before exchanging secured flows between them and the appropriate customer VPN.

The NBIG gateways are PAT/NAT points that allow servers or workstations within the customer's intranet to exchange data with the Internet via an official address assigned by Orange Business Services. This address is the only one announced to the outside world. In addition, a firewall is implemented at the entry point of each VPN in order to prevent unauthorized data from being exchanged with the Internet.

From the perspective of the Target Of Evaluation, each PE interface connected to one of these gateways with the intent of providing a VPN with these Internet-related services can be considered as a standard entry point of this VPN (i.e. as if it were connected to a CE interface).

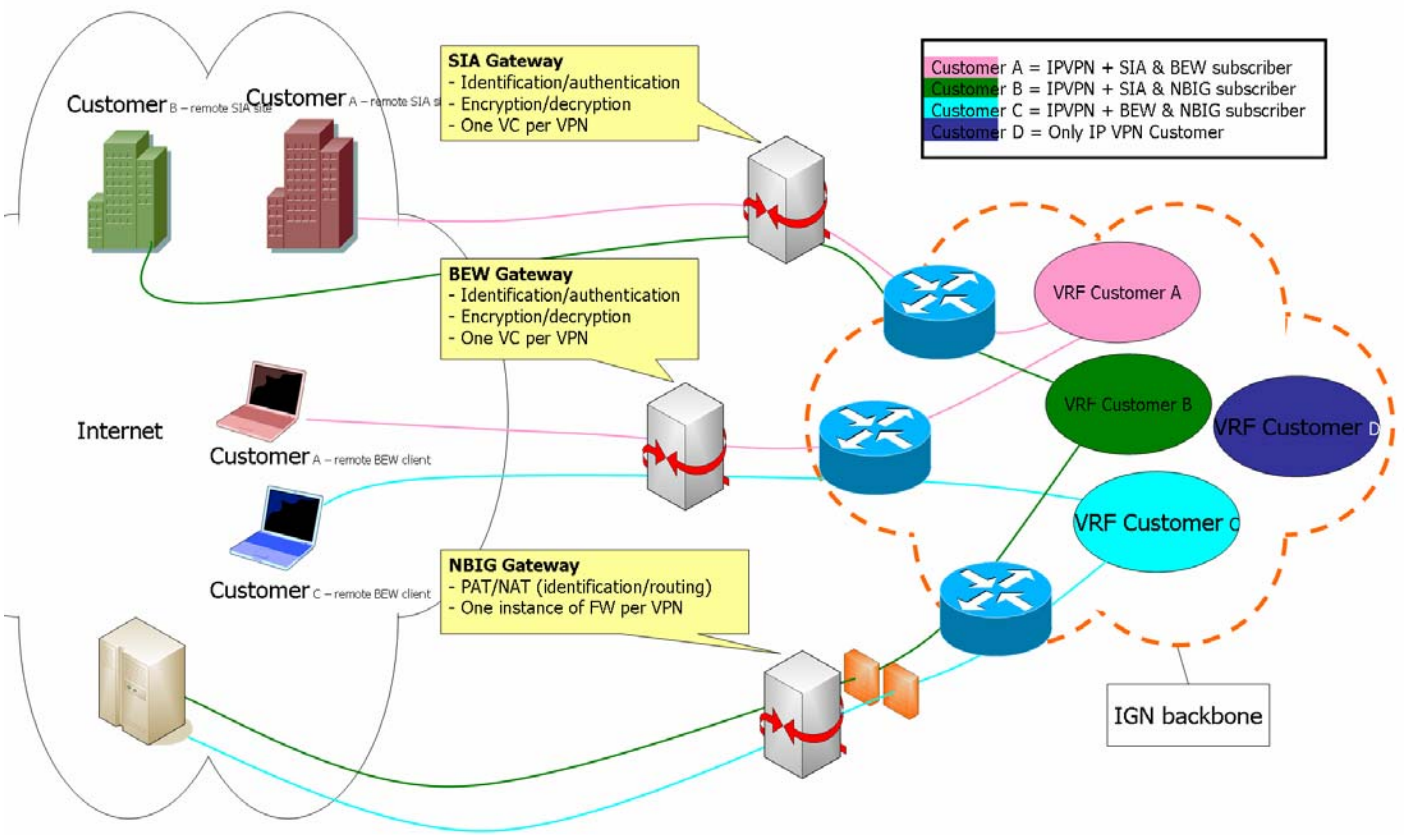

Figure 3 : Interface with the Internet

The way these services are produced and isolated from one another is beyond the scope of this Target of Evaluation. However, Orange Business Services guarantees that IPVPN customers which are not NBIG, SIA or BEW subscribers have no interaction between their VPN and these services.

1.3.5.3-VPN Partners

To extend the Equant IPVPN service to geographical areas not covered by Orange Business Services' network infrastructure (IGN), Orange Business Services establishes service agreements with VPN partners.

Depending on their technical capabilities, one can distinguish between two kinds of VPN partner networks:

> VPN partners operating multiservice MPLS networks (i.e., networks handling both VPN and Internet flows) These networks are called LIN. A good example is RAEI, the French MPLS network operated by Orange Business Services France.
> At the interfaces with the LINs, no Internet flows are imported "as such" into IGN.

> VPN partners operating strictly VPN-oriented networks (networks dedicated to VPN flows)

Whatever category the VPN partner belongs to, the standard interconnection with it is performed through ASBR PE routers is a back-to-back VRF model (no VPN tags are exchanged). The only exception is the gateway with RAEI: the interconnection is based on the MP-eBGP model, which implies the exchange of VPN Tags..

1.3.5.4-Equipment providers

In some cases, staffs of companies that provide network equipment to Orange Business Services need to access network devices in order to perform level 4 support operations. The access is allowed from a specific administration network of FT (out of the TOE scope) and a rebound in ControlNet. The equipment providers' staffs use dedicated administration accounts and IP addresses.

1.4-Evaluation scope

The evaluation is to be carried out on the operational service for conformity testing, and on a representative laboratory environment for intrusive tests that could damage the service.

IP equipments

The following configuration list provides information used for identifying which model and IOS software version of routers are used during the evaluation of the TOE.

Devices	Chassis Type	IOS software version	Supplier
PE routers	75xx	12.2(12j)	Cisco
		12.2(12k)	
		12.2(28b)	
	72xx	12.1(3a)T8 = 12.1(20010811:092825)	
		12.0(26)S2	
		12.1(14)E4	
	10xxx / PRE1	12.0(25)SX9	
		12.0(25)SX10	
	10xxx / PRE2	12.2(27)SBB4	
RR	72xx/NPE-G1	12.0(28)S1	
P routers	75xx	12.0(28)S5	
	12xxx	12.0(28)S1	
PE-ASBR	10xxx/PRE2	12.2(27)SBB1	
		12.2(27)SBB4	

Table 1: IP equipments' configuration list

ControlNet network management systems

The following configuration list provides the necessary information for identifying which software and OS software version are used in the network management systems during the evaluation of the TOE:

Network Management System	Software version	OS software version	Supplier
Purple TACACS	tac_plus v.1.0.1	Sun Solaris 8 and 9 / linux	Equant proprietary software
IPToolBox	v.2.6.0	Sun Solaris 8/linux	Equant proprietary software
GINI/XIPI – FTP/SFTTP server	Solaris FTP daemon	Sun Solaris 8 /linux	Sun Solaris
IPCFM - Configuration Repository	v. 2.8	Sun Solaris 8/linux	Equant proprietary software
SAFE	v.2.2	Linux Platon G7R0C2 (Red Hat Enterprise AS 4.0 Update 4)	IBM for server system. Equant proprietary software
NetForensics	nFX OSP v.3.4.1	Solaris 8 / linux	Netforensics
GPS-NTP	NTS-200 (Paris) 182-9004v8.2	182-9005v8.2	TrueTime
	S-200 - Release Version 1.10 Software Version 1.6.1.83	1.10.1.103	Symmetricom
NTP servers (gatesway routers between EIN and ControlNet)	Check Point NGX (R60)	Nokia IPSO 4.1 Solaris 9/linux	Checkpoint SUN
ControlNet firewalls between the EIN and the ControlNet	Check Point NGX (R60)	Nokia IPSO 4.1 Sun Solaris 9/linux	Checkpoint
ControlNet firewalls between the IGN and the ControlNet	ScreenOS 5.4.0r3.0	ScreenOS 5.4.0r3.0	Juniper

Table 2: Network management systems' configuration list

Preparative guidance documents

[ESR 10K Hardware Installation Guidance]	« Installation Network Agreement for ESR 10000 hardware as PE router » - Ref: NE-IGN-CISCO/INA 0002 – Version: 14
[ESR 10K Software Installation Guidance]	« Software agreement for CISCO ESR 10K 12.0.25SX9 IOS release on RAEI and IGN backbones » - Ref : NE-IGN-CISCO/RCN 010 – Version: 1.0, 05/21/2007
[TACACS – Installation Guide	«Equant TACACS – Installation Guide» - ref. MDAM-7BHMEA, version 1.0 – 02/04/2008
[IPTOOLBOX –SIF]	« System Integration Form IPTOOLBOX » - Ref : IS/SIF/000000 - Version :2.2 - 02/01/08

[IPCFM –SIF]	« System Integration Form IP – CFM » - Ref: IS/SIF/000000 - Version :2.4, 08/03/2007
[Firewalls CNT/IGN – RCN]	«CIMP Release Control Notice » - Ref : N/A – Version: 1.5, 09/25/2007
[Firewalls EIN/CNT – RCN]	«Release Control Notice - ControlNet FireWalls Project » - Ref: CNT FW Release Control Notice – Version : 1.4.1, 07/05/2007
[nFX OSP – SIF]	« System Integration Form SOC netForensics Security Information Management Application » - Ref: IS/SIF/000000 – Version: 1.0.1, Jan 2008
[SAFE – MI]	«EQT096 INSTALLATION MANUAL SAFE version 2.1» - Ref: EQT096-MI-2.1 – Version:1.0, 26 Feb 2007
[NTS – 200 –User Manual]	«NTS-200-GPS User's Manual» - Ref : NA – February 2005
[GINI/XIPI – FTP SIF]	« GINI/XIPI-FTP/SFTP server in the ControlNet - System Integration Form» - Ref: n.a

Operational guidance documents

[IPVPN Overview]	«MANUAL OPERATOR GUIDANCE Global IP VPN - Overview » - Ref: AUTO-001363 - Alias OPINFO/INF 001611) – Version 1.0, 08/03/2005
[IPVPN Configuration]	« MANUAL OPERATOR GUIDANCE Global IP VPN – Configuration » - Ref: AUTO-001363 Alias OPINFO/INF 001612 – Version 1.0, 09/28/2006
[IPVPN Troubleshooting]	« MANUAL OPERATOR GUIDANCE Global IP VPN – Troubleshooting » - Ref: AUTO-001613 - Alias OPINFO/INF 001613 – Version 1.0 , 08/03/2005
[Quick Guide – Troubleshooting IP Faults]	«Quick guide to trouble shoot IP Faults » - Ref: GCS/CVM/01/002 – Version .1.4 – 02 Feb 2002
[Generic PE – Overview]	« MANUAL OPERATOR GUIDANCE ESR10K GenericPE overview » - Ref: AUTO-001840 - Alias OPINFO/INF 001840 – Version 1.0, 06/08/2004
[Generic PE – Configuration]	« MANUAL OPERATOR GUIDANCE ESR10K GenericPE Configuration Guidelines » - Ref: AUTO-001841 - Alias OPINFO/INF 001841 – Version 1.0, 04/11/2005.
[Generic PE – Troubleshooting]	« MANUAL OPERATOR GUIDANCE ESR10K GenericPE Toubleshooting Guidelines » - Ref: AUTO-001843 – Alias OPINFO/INF 001843 - Version 1.0, 11/01/2004
[IPVPN for Partners – Overview]	«MANUAL OPERATOR GUIDANCE IP VPN for Partners – Overview » - Ref: AUTO-001796 Alias OPINFO/INF 001796 –Version 1.0, 11/28/2005
[IPVPN for Partners – Configuration]	«MANUAL OPERATOR GUIDANCE IP VPN for Partners - Configuration Guide » - Ref: AUTO-001797 – Alias OPINFO/INF 001797 – Version 1.0, 10/17/2005
[IPVPN for Partners – Troubleshooting]	« MANUAL OPERATOR GUIDANCE IP VPN For Partners - Troubleshooting Guide» - Ref: AUTO-001798 Alias OPINFO/INF 001798 – Version 1.0, 11/28/2005
[TACACS –SIF]	« System Integration Form - Tacacs Plus authentication & synchronization Unified access to the IP routers project » - Ref : IS/SIF/000000 – Version : Version : 2.0, 01/31/2008
[TACACS-Troubleshooting]	« Internal Purple Tacacs Troubleshooting & Operations Procedures » - Ref : TACACS_EQUANT/ OPI 0001 v2T1 – Version: v1.2, 03/27/2006
[IPTOOLBOX –SIF]	« System Integration Form IPTOOLBOX » - Ref : IS/SIF/000000 - Version :2.2 - 02/01/08

[IPCFM –SIF]	« System Integration Form IP – CFM » - Ref: IS/SIF/000000 - Version :2.4, 08/03/2007
[IPCFM – WebAdmin Manual]	«IPCFM – WebAdmin User Guide » - Ref: N/A – Version 1.0, 10/26/2007
[Firewalls CNT/IGN – RCN]	«CIMP Release Control Notice » - Ref : N/A – Version: 1.5, 09/25/2007
[Firewalls EIN/CNT – RCN]	«Release Control Notice - ControlNet FireWalls Project » - Ref: CNT FW Release Control Notice – Version : 1.4.1, 07/05/2007
[nFX – Alarm Management]	« netForensics CE Alarms Handbook » - Ref : N/A – Version: 1.6, 07/20/2007
[nFX –Handbook]	«nF Security Handbook All Perimeters» - Ref : N/A – Version : 1.4, Jan 2007 – Format : Microsoft Powerpoint
[nFX OSP – SIF]	« System Integration Form SOC netForensics Security Information Management Application » - Ref: IS/SIF/000000 – Version: 1.0.1, Jan 2008
[nFX OSP user training]	«nFX Open Security Platform User Training» - ref. n.a
[SAFE – MU]	« SAFE USER GUIDE V2.0 » - Ref: N/A – Version: 1.8, Jan 2007
[NTS – 200 –User Manual]	«NTS-200-GPS User's Manual» - Ref : NA – February 2005
[GINI/XIPI – FTP SIF]	« GINI/XIPI-FTP/SFTP server in the ControlNet - System Integration Form» - Ref: n.a

2-Conformance Claim

The present security target is conformant to the Common Criteria:

> Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model
June 2005 Version 3.0 Revision 2, CCMB-2005-07-01

> Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements
July 2005 Version 3.0 Revision 2, CCMB-2005-07-02

> Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements
July 2005 Version 3.0 Revision 2, CCMB-2005-07-03

No conformance with a protection profile is claimed.

This TOE is CC Part 2 conformant and CC Part 3 conformant.

The assurance level of the ST is EAL2, augmented by ALC_FLR.1.

3-Security problem definition

3.1-Assets

Two categories of assets can be identified: firstly the assets belonging to final users, and secondly the assets belonging to the TOE itself.

3.1.1-Customers' Assets

The customers' assets are the following:

Customers flows

The customers flows are the information flows exchanged from a customer's site to another through a dedicated virtual private network / intranet.

3.1.2-Sensitive assets of the TOE

The following assets are the assets the TOE manages and uses to provide its services securely.

VPN routes

As discussed earlier, a VRF is associated to each VPN interface of the PEs.

In order to allow the PEs to route the flows through the customer's VPN, the VPN routes are advertised to the PEs supporting this VPN (having at least one interface belonging to this VPN).

VPN tags

VPN tags are level 2 MPLS tags that are attached to information flows. They allow the identification of VPNs.

PE configuration data

PE configuration data include the following elements:

- Definition of the authentication and authorization and accounting servers parameters (definition of router administrator profiles);
- Definition of tracability rules for the commands;
- Route import / export rules;
- A route distinguisher by VRF;
- A binding between VRFs and network interfaces;
- SNMP configuration (including community names);
- Access control lists

Management data

Management data may include different types of administration-related information:

- servers' configurations
- administrators' accounts and related authentication data
- SNMP community names
- ...

Management data may need to be protected both when they are stored or used on the equipments or the management applications, and when they are imported into /exported from the TOE or exchanged within the TOE.

3.2-Users

In practice, the TOE has two types of users:

- Users of the service that are connected through a client interface. Users of this type have no privileges and cannot access any security function. They can only use the system to transfer information through a VPN.
- Users that are in charge of the administration of the VPN, of the equipments or of the production tools.

3.2.1-Customer users

3.2.1.1-Internet gateways

Three types of Internet gateways are connected to the TOE to ensure specific interconnection with the Internet. The behavior of each of these gateways is described with further details in section 1.3.5.2

Business Everywhere Gateway

Through the Business Everywhere Gateway, the nomad staff of companies having subscribed to the Business Everywhere service may be connected to their corporate network.

NBIG Gateway

The NBIG gateways provide Internet connectivity to each VPN for which the customers also subscribed to the NBIG service.

SIA Gateway

The SIA gateways allow SIA subscribers to establish a connection between their VPN and a remote site, through an IPSEC tunnel over the Internet.

3.2.1.2-Miscellaneous

CE

CEs are routers installed in the customer's premises. They make the interface between the customer's LAN and the backbone.

Each CE is connected to a PE through a specific interface, bound to the customer's VPN.

ASBR-PE - International partners

France Telecom has agreements with operators to be able to extend some VPNs to areas where France Telecom does not have its own infrastructure.

As discussed earlier in this document, there are two categories of VPN partners:

- LSSUs, this means multiservice networks operated by third parties
- MPLS/VPN only networks operated by third parties

The standard interconnection with these operators is ensured by using ASBR-PEs based on a back-to-back VRF model. The interconnection with RAEI, Orange Business Services? MPLS/VPN infrastructure in France, is based in the MP-eBGP model.

In this evaluation, the VPN partners' ASBR peer routers are not considered as users of the TOE. They should rather be seen as means/resources the TOE uses to extend the service.

3.2.2-Management and monitoring staff

Different roles of administrators are defined to ensure the management of the service, of the equipments and security monitoring:

Backbone devices administrators

Backbone devices administrators are responsible for installing, configuring, maintaining the backbone devices (P, PE, RR).

CE and VPN Owners

The VPN owners are responsible for the administration of the CEs (located in the customer sites) and of the VPNs (configured on the PEs).

Monitoring staff

Monitoring teams are in charge of the network supervision.

These persons are authorized to access traces generated by network equipments during administration operations.

SOC staff

SOC staff is people working in the Security Operating Center.

They are grouped into monitoring teams in charge of supervising the network security.

These persons are authorized to access the traces of security events generated by network equipments and to alert the operational teams in charge of the concerned perimeter that, in turn, take any useful responsive actions.

Providers' staffs

When heavy maintenance is needed on a given PE, provider's staff may be requested to perform maintenance operations on the equipments of IGN. To do this, they use accounts created specifically for this purpose. This access is governed by a dedicated security policy.

.Administrator of network management systems

Each network management system hosted in the Controlnet is under the responsibility of a specific application manager. He is in charge of the services served by the application. He performs all administrative tasks for the application such as managing user accounts, network services (i.e.: SSH, SSL, NTP synchronization, AAA servers…), log purge, applicative settings, security controls.

This role includes the management of:

- The configuration of the AAA servers, related to PE administration (management of the users, groups of users and the associated profiles, the routers and group of routers);
- The IP TOOLS servers in charge to offer a set of tools to operators;
- The IP TOOLS servers in charge to offer a set of tools to VPN owners;
- The tool monitoring the VRF conformity (SAFE);
- The server verifying the PE configuration (SAFE);

- netForensics, the tool in charge of collecting and filtering the SYSLOG flows.

Note:

- In the functional security requirements defined in chapter 5, these roles of “Backbone devices administrator”, “CE and VPN Owner”, “Monitoring staff”, “SOC staff” and “Providers’ staffs” are referred to under the generic term “router administrators”.
- The term “administrator”, used without any specific qualifier, is used to refer to any of the management roles defined in this section, or some of them, depending on the context.

3.3-Threats

This section presents the threats on the TOE.

NB: the attack paths presented here are provided as examples and should not be considered as exhaustive.

T.Saturation

A user succeeds in saturating the routers resources.

Threatening agent

- Ill-intentioned customer

Attack path

- Saturation of a PE connection by importing a too important number of routes in a VRF.

Threatened assets

- Customers flows going through the attacked PE.

T.CustomersVPNFlows.Escape

A user succeeds in establishing a flow between its own VPN and the VPN of another customer.

Threatening agent

- Ill-intentioned customer
- External attacker

Attack path

- Faking IP packets
- Modifying the VPN configuration.

Threatened assets

- Customer flows

T.CustomersVPNFLows.InterferenceFromTheInternet

An attacker on the Internet succeeds in interfering with customer VPN flow either by injecting or by escaping data.

Threatening agent

- External attacker

Attack path

- Faking IP packets

Threatened assets

- Customers flows

T.NetworkFlows.Eavesdropping

An attacker succeeds in eavesdropping the network traffic, using a logical access to IGN or from the administration network.

Threatening agent

- Ill-intentioned customer
- External attacker

Attack path

- Eavesdropping of the backbone communications (Equant IGN AS) from an authorized access point (VPN customer access), or from a machine on the Internet.

Threatened assets

- Customers flows
- PE configurations
- VPN routes being exchanged between routers
- Management data (such as administrators authentication data and SNMP comunity names)

T.NetworkFlows.Modification

An attacker succeeds in modifying data exchanged in the Orange Business Services network, using a logical access to IGN or through the administration network.

Threatening agent

- Ill-intentioned customer
- External attacker

Attack path

- Modification (insertion, deletion, change) of data exchanged on the backbone (Equant IGN AS) using an authorized access point (VPN customer access), or from a machine on the Internet.

Threatened assets

- Customers flows
- PE configurations
- VPN routes being exchanged between routers

T.PE.Takeover

An attacker succeeds in taking over a PE (access to the full configuration commands).

Threatening agent

- Ill-intentioned customer
- External attacker

Attack path

- Usurpation of a PE administrator's identity, or use of an IOS weakness/vulnerability, or take benefit of a misconfiguration

> Access to an appliance form an interconnected network

Threatened assets

> PE configuration

In case of success of this attack, this may lead to break the isolation of the VPNs produced on the targeted PE and could allow exchanging flows between the VPNs and/or on the Internet.

T.AdminTools.Takeover

An attacker succeeds in taking over an administration tool.

Threatening agent

> Ill-intentioned customer

> External attacker

Attack path

> Usurpation of a VPN administrator's identity

Threatened assets

> PE configuration

T.CustomersFlows.IsolationBreakDown

The actions of an external attacker or a router administrator's mistake/mis-configuration may lead to break down the isolation of customers' VPNs.

Threatening agent

> Router administrator

> External attacker

Attack path

> Mis-configuration caused by a router administrator

> Spoofing of one of the routers at the interconnection to Internet and reception of wrong routing information from an external attacker.

Threatened assets

> Customers flows

3.4-Organisational security policies

3.4.1-Operational Constraints on the TOE

This section presents constraints applying to the TOE in its operational environment.

P.Accounting

In order to make them auditable and imputable, the TOE shall record the traces of administration operation performed on the configurations of PEs and VPNs. In particular, the identity of the person responsible for the operations shall be recorded along with the other audit information.

P.ProvidersAccesses

In order to allow maintenance operations, the TOE shall authorise providers' accesses.

Like any other router administrators, providers' staffs shall be authenticated. Access to the equipments shall only be granted to providers' staffs in read only mode. The accesses shall be restricted in terms of scope (i.e. accessed appliances).

Consistently with *P.Accounting*, the TOE shall ensure traceability and accountability of the performed actions.

P.ControlAtProductionTime

At production time, the operators producing VPN accesses shall perform controls to make sure that the accesses produced are conformant to the customer request.

3.4.2-Constraints on the TOE's Life Cycle

This section presents the constraints on the TOE life cycle that are associated to security evaluation.

P.LifeCycleConstraints

The development environment of the TOE shall be conformant to the assurance packet EAL2 augmented by component ALC_FLR.1.

Application note:

For more information about the meaning of this constraint, see the application note associated to the organisational security objective *OD.LifeCycleConstraints*.

3.5-Assumptions

Regarding the environment of the TOE, the following assumptions are made:

A.PhysicalAccess

France Telecom is directly or indirectly responsible for the access control to all the appliances of the TOE. France Telecom implements measures adequate to prevent intrusions in the premises hosting the equipments.

A.Administrators

The administrators of the system components are trained and capable to use the appliances and tools they use.

The administrators are assumed to be trusted people. Voluntary disruptive actions from administrators are not envisioned.

A.AutonomousSystem

Data flowing into a customer VPN, from a PE to another one, can only be exchanged within the Equant autonomous system (AS).

International VPNs can only be extended through the interconnections with local partners.

A.OperationsAndMaintenance

Any materials composing the TOE are under the control of France Telecom that is responsible for their good operation and their maintenance.

A.RemoteManagementAccess

Remote administration operations, out of working hours, are performed through remote access to EIN, then access to ControlNet.

The means used to secure this type of access include an authentication of the operator, and guarantee confidentiality and integrity of exchanged data.

A.PasswordsManagement

The passwords of the administrators are generated, stored and distributed in a way ensuring that they are only known from their owners.

The administrators are also committed not to share their passwords with each others.

NOTE: this is governed by a specific "Authentication Policy".

A.VPNExtensionServices

The entities of France Telecom that manage the services extending the VPNs (namely, BEW, SIA and NBIG) are responsible of the correct parameterization of the customers' accounts.

In particular, they should guarantee that:

- The Business Everywhere and SIA gateways are capable of identifying and authenticating the sender of the incoming customer flows and capable of injecting the flows in the right VPN.
- The NBIG gateways are capable of identifying and routing the customer flows in the right VPN and from the VPN to the Internet. The NBIG gateways implement one instance of firewall per interconnected VPN.

Application note:

As a consequence of this assumption, the customers that did not subscribe to Business Everywhere or SIA or NBIG services have no interface with it. Therefore, they cannot be threatened by any accidental mis-configuration on one of the gateways performed outside the scope of control of the TOE.

A.ServersManagement

Some equipments of ControlNet that support PE and/or VPN management applications do not directly ensure security functions.

The administration of those equipments is assumed to be performed in a manner ensuring the security of the provided services.

A.ProvidersAccess

Providers' remote accesses to the backbone routers are made possible using an administration network operated by France Telecom and a rebound in ControlNet.

This administration network shall be managed by France Telecom in a manner such that its security level is comparable to the one of ControlNet. In particular, this means that accesses shall only be granted to remote machines with known IP addresses and on network links guaranteeing confidentiality and integrity of exchanged data.

4-Security objectives

4.1-Security objectives for the TOE

4.1.1-Protection of the Customers' Flows

O.CustomerFlows.Isolation

The TOE shall ensure that no flow can be exchanged:

- Between two networks bound to PE interfaces belonging to separate VPNs;
- Between a network bound to a PE belonging to a given VPN and a network bound to a PE interface that does not belong to a VPN (e.g., an administration interface, a backbone internal interface)).

In particular, the use of a specific global VPN to manage the terminal equipments (CE) shall not compromise the isolation of a customer's VPN from each others.

O.NoInterferenceFromOutsideIGN

The TOE shall ensure that:

- Administration flows are authorized only for services authorized on the PE and are originated from machines belonging to the administration network;
- The internal addresses of the backbone are not advertised outside IGN, except for a limited number of cases where advertising routers address is required: administration addresses of PEs that are known from bouncing servers and accessible only from ControlNet, interconnection address of an ASBR-PE known from the partner’s peer ASBR PE routeur;
- For subscribers of the NBIG service: Internet flows are exchanged through the customer's VPN and via the NBIG gateways; otherwise no flows are exchanged between NBIG and the customer's VPN.

O.InterconnectionWithPartners

In addition to the isolation of the customer's flows inside the backbone, up to the interconnection with the partner network (see previous objective), the TOE shall ensure that:

- the VPN topologies are connected as point-to-point IPV4 connections with the partner (standard case)
- the VPN topologies are shared with the partner for the specific case of the French MPLS VPN backbone (RAEI). In that case, the TOE shall ba able to identify the VPN topologies that can be shared with this partner from the others.

Application note:

Connecting VPN topologies as point-to-point IPV4 connections with the partner means ensuring the isolation of the VPNs at the interconnection itself: the VPN partner's interconnection ASBR PE is shown as if it were as many customers CE as there are interconnected VPNs. This implies In particular that no VPN tags are exchanged with the VPN partners at such a type of interconnections.

Sharing the VPN topologies with the VPN partner practically implies the sharing of VPN tags between the VPN partners at the interconnection.

4.1.2-Safe Management and Protection of VRFs

O.PreSaturation

The TOE shall trigger a pre-saturation alarm message when the number of routes of a same VRF reaches a given threshold.

O.VPNRoutesExchange.PEinaVPN

The TOE shall guarantee that the VPN routes are only exchanged between PEs and VRFs supporting a same VPN.

4.1.3-Administration

O.Administrators.Authentication

The TOE shall authenticate the administrators on the management tools and on the P, the RR or the PE before being allowed to perform any action.

For any administrator, a user profile shall be defined identifying the scope (set of equipments) on which access may be granted as well as the type of allowed accesses (read only, limited read/write, full read/write).

Accounting shall be performed on the PE.

Application note:

This means that the administrators shall be authenticated either on the management tools or on the PE before being allowed to perform any action, depending on the device to be reached.

O.AccessControlToPEs

The TOE shall define architectural means to control the access to the PEs.

These means shall at least consist in configuring the PEs to refuse any administration flow originated from outside ControlNet.

Application note:

As a consequence, the management tools shall be hosted exclusively in ControlNet.

O.TrustedPath

The TOE shall ensure that VPN administration and PE administration is performed through a trusted path between the administrators' workstation and the management tools located in ControlNet.

This trusted path shall guarantee confidentiality and ensure integrity of the exchanged administration flows.

O.ConformityCheck

The TOE shall periodically check the conformity of the PE configurations.

The two types of conformity checks performed on the PE configurations are the following:

1) Conformity monitoring of the global configuration of each PE: this means, checking whether some security rules are actually met (e.g.: checking whether such or such port is opened/closed for such or such service, authentication server configuration, access control lists,...)

2) Integrity verification of the customers' VPN configurations on each PE. Informations about the VPN perimeters are provided to the VPN owners.

4.1.4-Audit

O.Accounting

The TOE shall keep traces of all the most important (all "write" commands and a set of "read" commands) events relating to VPN administration and PE administration and implement means to identify the responsibilities in case of problem.

4.2-Security objectives for the development environment

OD.LifeCycleConstraints

The development environment of the TOE shall conform to the assurance packet EAL2 augmented by component ALC_FLR.1.

Application note:

This objective requires that the TOE shall be evaluated by an independent security evaluation facility and reach the assurance level EAL2+.

The required assurance level implies provisioning the evaluator with the following:

- A security target (the present document), which shall completely and consistently present the security problem, security objectives, functional and assurance security requirements as well as a TOE summary specification. (ASE_xx)
- Development documentation that shall include:
  - Functional specifications of the TOE, presenting the external interfaces of the security functions (ADV_FSP.2);
  - A document presenting the TOE architecture in terms of components (ADV_TDS.1);
  - A document presenting and arguing the security architecture of the TOE (ADV_ARC.1).
- Project management and life cycle -related documentation shall include:
  - A list of the configuration management items constituting the TOE as well as the procedures in effect for configuration management (ALC_CMC.2 and ALC_CMS.2);
  - Documented procedures allowing to securely deliver the service to the final customer (ALC_DEL.1);
  - Documented procedures to manage security flaw and vulnerability remediation (ALC_FLR.1).
- User documentation that shall include:
  - Organisational procedures relating to security support requirements that allow the provider to meet meet the security objectives on the environment define in section 4.3-.
  - Documented administration procedures relating to installation and start-up of new components of the TOE (AGD_PRE.1);
  - Documented administration procedures relating to the use of the security functions, when the TOE is in its operational environment (AGD_OPE.1).
- Test documentation that shall include:
  - A specification and the results of the functional tests performed on the security function interfaces (ATE_FUN.1),
  - A demonstration of the test coverage (ATE_COV.1).

In addition, an access to the TOE shall be provided to the evaluator so that he will be able to perform additional independent tests (ATE_IND.2).

Finally, always as part of the evaluation, a independent vulnerability analysis shall be conducted by the evaluator. This analysis, based on the development and user documentation, shall demonstrate that no residual vulnerabilities are accessible to an attacker having a low attack potential (AVA_VAN.2).

4.3-Security objectives for the operational environment

4.3.1-Objectives on the Environment Due to Assumptions

OE.ControlledPhysicalAccess

France Telecom/Equant shall directly or indirectly control the access to the premises hosting the appliances composing the TOE.

The Customers shall directly or indirectly control the access to the premises hosting the CE routers provided by France Telecom/Equant.

OE.ProvidersAccesses

In order to allow maintenance operations, the TOE shall authorise providers' accesses.

Like any other administrators, providers' staffs shall be authenticated and their accesses shall be restricted in terms of scope (i.e. accessed appliances). Access shall only be granted in read only mode.

Consistently with O.Accounting, the TOE shall ensure traceability and accountability of the performed actions.

In addition, providers' remote accesses to the backbone routers are made possible using an administration network operated by France Telecom that is interfaced to ControlNet.

This administration network shall be managed by France Telecom in a manner such that its security level is comparable to the one of ControlNet. In particular, this means that accesses shall be granted to remote machines with known IP addresses and using network links guaranteeing confidentiality and integrity of exchanged data.

OE.CapableAdministrators

The administrators of the system components shall be trained and capable to use the appliances and tools they use.

The administrators are trusted people. They are not considered as threatening agents, in the sense that no voluntary disruptive actions from them are envisioned.

OE.AutonomousSystem

Data flowing into a customer VPN, from a PE to another one, can only be exchanged within the Equant autonomous system (AS).

International VPNs can only be extended through the interconnections with local partners.

Application note:

In practice, this objective means that the interior routing protocol (MP-iBGP) used to route information from an ingress PE to a egress PE is assumed to be correctly implemented on the equipments. This protocol does not allow to define interconnection points by other means than dedicated gateways implementing an exterior routing protocol (MP-eBGP in the case of the TOE).

The evaluation does not cover the implementation of these protocoles, but rather the fact that they are correctly configured.

OE.RemoteAdministrationAccess

Remote administration operations, out of working hours, are performed through the internal administration network

The means used to secure this type of access shall include an authentication of the operator, and guarantee confidentiality and integrity of exchanged data.

OE.VPNExtensionServices

The entities of France Telecom that manage the services extending the VPNs (namely, BEW, SIA and NBIG) shall be responsible of the correct parameterization of the customers' accounts.

In particular, they shall guaranty that:

- The Business Everywhere and SIA gateways are capable of identifying and authenticating the sender of the incoming customer flows and injecting the flows in the right VPN.
- The NBIG gateways are capable of identifying and routing the customer flows in the right VPN and from the VPN to the Internet. The NBIG gateways implement one instance of firewall per interconnected VPN.

OE.ServersManagement

Some equipments of ControlNet that support PE and/or VPN management applications do not directly ensure security functions.

The administration of those equipments shall be performed in a manner ensuring the security of the provided services.

4.3.2-Objectives on the Environment Due to OSPs

OE.PasswordsManagement

The passwords of the administrators shall be generated, stored and distributed in a way ensuring that they are only known from their owner.

The administrators shall be committed not to share their passwords with each others.

OE.OperationsAndMaintenance

France Telecom/Equant shall operate and maintain the appliances constituting the TOE in a secure manner.

OE.ControlAtProductionTime

At production time, the operators producing a VPN shall perform controls to make sure that the access produced is conformant to the customer request.

5-Security requirements

5.1-Introduction

This chapter defines the security requirements applying to the TOE:

Sections 5.2 and 5.3 respectively define the security functional and assurance requirements covering the security problem presented previously.

Section 5.4 provides a justification for the satisfaction or the non-satisfaction of the necessary dependencies between requirements

Section 5.5 provides a justification for the coverage of the security problem by the security functional and assurance requirements

Note about refinements

Some security requirements are refined to precise their meaning in a normative manner.

The following mentions are used to specify the type of the refinement used:

Editorially refined:

Editorially refined is mentioned into brackets just after the title of the security requirement to mean that some editorial changes have been made regarding the standard requirement to enhance readability.

Non editorial refinement:

Non editorial refinements are additional clauses that are inserted after an element of a security requirement. They are used either to precise some points in the element (e.g. define the subject on which the requirement applies) or to complement the requirement by additional information.

Global refinement:

The global refinements are non editorial requirement applying to all the elements of a security requirement.

Systematic editorial refinement of component FCO_ITC.2.1

To fix a misprint in the catalogue of security functional requirements of the Common Criteria V3.0, the text of any component FCO_ITC.2.1 inserted in this document is systematically editorially refined without any “editorially refined” mention being inserted.

The standard text is changed a follows:

Standard text:

FCO_ITC.2.1 The TSF shall enforce [assignment: rules on whether import is allowed] when [assignment: subject][assignment: list of data] from a user bound to that subject.

Editorially refined text:

FCO_ITC.2.1 The TSF shall enforce [assignment: rules on whether import is allowed] when [assignment: subject] **imports** [assignment: list of data] from a user bound to that subject.

5.2-Security support requirements

This section is inserted in application of the DCSSI's note on system evaluations [NA_EVSYS]; it presents the requirements that relate to the non-IT security objectives on the environment.

In this section, the term "service provider" is used to relate to the term "developer" currently used in the CC context. This term simply relates to Orange Business Services.

5.2.1-Security support requirements for the service provider

This section presents the non-IT security requirements the service provider shall implement.

The following set of requirements allows the customer to gain the assurance that organisational measures are taken on the service provider's side in order to meet the security objectives on the environment define in section 4.3-.

5.2.1.1-Security support requirements for the service provider on its own side

SSR.AccessControl.Physical
The Service Provider shall control the physical accesses to the equipments located in it premises.

SSR.AccessControl.Providers
Providers' accesses to the equipments of the TOE shall be controlled so that:

- Any provider's accesses shall pass through ControlNet
- Any providers' staff shall be authenticated
- Any providers' access shall be restricted in terms of scope (accessed equipments)
- Only read accesses may be granded.

SSR.Administrators.Training
The administrators shall be trained in order to be able to correctly use the appliances and tools.

SSR.Administrators.RemoteAccesses
The service provider shall control the accesses of the administrators for interventions out of the working hours.

SSR.ServersManagement
The service provider shall operate and maintain the equipments supporting the PE and VPN management applications in a secure manner.

SSR.Passwords.Management
The service provider shall apply the procedures to manage the passwords securely.

SSR.OperationAndMaintenance
The service provider shall operate and maintain the appliances constituting the TOE in a secure manner.

SSR.ControlAtProductionTime
At production time, the operators producing a VPN shall perform controls to make sure that the access produced is conformant to the customer request.

5.2.1.2-Security support requirements for the service provider on the customers' sites

Except the service initialization procedure to be defined as part of assurance security requirement ALC_DEL.1, there is no specific security support requirement for the service provider on the customers' sides.

5.2.2-Security support requirements for the customer

According to the DCSSI's note [NA_EVSYS], this section should present the non-IT security requirements that shall be implemented on the customer's side to use the TOE in the context of the evaluation.

SSR.CE.AccessControl.Physical

The Customer shall control the physical accesses to the equipments (CE router provided by the Service Provider) located in it premises.

5.3- Security functional requirements

5.3.1-Introduction

This section aims at defining the objects, their attributes and the operations needed to specify the security functional requirements covering the security objectives for the TOE.

This section does not include any further definition of users and subjects. The definitions of users interacting with the TOE and subjects acting within the TOE are provided in sections 1.3.4 and 3.2.

5.3.1.1-VPN packets

Definition

VPN packets are information flows transferred from an ingress PE to an egress PE within a customer's VPN. VPN packets are also referred to as customer flows in the rest of the document.

Security attributes

IPVPN address

The IPVPN address is the destination address of the VPN packet in the backbone.

It is the concatenation of the destination IPv4 address of the packet in the customer's network and of the route distinguisher associated to the customer's VPN. The uniqueness of the route distinguisher makes this address unique in the whole MPLS network.

IPV4 address

The IPV4 address of a packet is the destination address of the packet in the customer's network.

Possible operations

Import of IP packets
IP packets are imported into the TOE on an ingress PE from a customer's CE. The TOE adds a VPN tag to the packet to build an VPN packet and the injects this latest into the adequate customer's VPN.

Export of IP packets
The egress PE exports IP packets to a customer's CE. The interface of the PE to which the packet should be delivered is identified using the customer's VPN tag.

5.3.1.2-VPN configurations

Definition

The configuration of a customer's VPN is distributed over several PEs; namely: the PEs ensuring the interconnection with the customer's CE.

On each of those PEs, a VRF holds the attributes of the VPN that are dedicated to the PE.

Security attributes

Import Route Target
The import Route Target is used to identify/filter the routes that the router can import into the present VRF.

Export Route Target
The export Route Target is exported along with the routes managed in the present VRF. It serves to identify the VPN to which the exported route belongs.

Route Distinguisher
The route distinguisher identifies the VPN on the routing plane. In this document, it is also referred to as "VPN Tag".

Possible operations

Production of a VPN / modification of a VPN configuration
Creation of a VPN interface on a PE and parameterization of the configuration of this VPN; modification of this configuration.

5.3.1.3-Routing information

Definition

Routing information refers to:

> The VPN routes managed by the PE routers (see previous section)

> The routes exchanged with partner networks (Internet and VPN partners)

Security attributes

Import Route Target
See section 5.3.1.2-.

Export Route Target
See section 5.3.1.2-.

Possible operations

Import and export of VPN routes between PE routers

> Export of routes belonging to a VRF to the other VRFs on other PEs.

> Import of routes in a VRF using the import route target attribute as a filter.

Import and export of routes from peer routers in the partner networks

> Import and export of VPN routes with the VPN partners.

5.3.2-Customers Flows

This section presents the requirements relating to the protection of the customers flows.

FCO_ITC.2/CEAdminFlows Import with security attributes

FCO_ITC.2.1/CEAdminFlows The TSF shall enforce **the following rule:**

> **Import is allowed if the destination Management/IPv4 address belongs to the VRF table that is associated to the customer's VPN on the ingress PE.**

when **the ingress PE** imports **management packets** from a user bound to that subject.

FCO_ITC.2.2/CEAdminFlows The imported data shall be imported with the security attributes**:**

> **IPV4 addresses**

.

FCO_ITC.2.3/CEAdminFlows The TSF shall associate the security attributes with the imported data.

FCO_ETC.1/CEAdminFlows Export of data and/or security attributes

FCO_ETC.1.1/CEAdminFlows The TSF shall enforce **the following rules:**

> **The CE interconnection interface to which route the data is found by**

>> **Selecting the VRF according to the VPN tag of the VPN packet,**

>> **Identifying the output interface using the IPV4 destination address included in the VPN packet**

> **The VPN tag of the VPN packet is removed before export**

when **a PE** exports **a CE administration flow (with its IPV4 address, but without the VPN tag)** to a user bound to that subject.

Non editorial refinement:

Otherwise, the packet is discarded (no VRF found) or the forwarded to another PE (no interface found).

FCO_ITC.2/VPNFlows Import with security attributes

FCO_ITC.2.1/VPNFlows The TSF shall enforce **the following rule:**

- **Import is allowed if the destination VPN/IPv4 address belongs to the VRF table that is associated to the customer's VPN on the ingress PE.**

when **the ingress PE** imports **IP packets** from a user bound to that subject.

FCO_ITC.2.2/VPNFlows The imported data shall be imported with the security attributes**:**

- **IPV4 addresses**

.

FCO_ITC.2.3/VPNFlows The TSF shall associate the security attributes with the imported data.
Non editorial refinement:

Security attributes = the VPN/IPV4 destination address of the packet. This address is composed of:

- the VPN tag of the customer VPN
- the imported IPV4 destination address

The security functional requirement *FCO_ITC.2/VPNFlows* defines import rules applicable to the customers' flows on the ingress PE before their injection in a VPN.

FCO_ETC.1/VPNFlows Export of data and/or security attributes

FCO_ETC.1.1/VPNFlows The TSF shall enforce **the following rules:**

- **The customer's interface to which route the data is found by**
  - **Selecting the VRF according to the VPN tag of the VPN packet,**
  - **Identifying the output interface using the IPV4 destination address included in the VPN packet**
- **The VPN tag of the VPN packet is removed before export**

when **an egress PE** exports **a customer flow (with its IPV4 address, but without the VPN tag)** to a user bound to that subject.

Non editorial refinement:

Otherwise, the packet is discarded (no VRF found) or the forwarded to another PE (no interface found).

5.3.3-Interconnection with VPN Partners

This section presents the security requirements regarding the interconnections with the VPN partners.

5.3.3.1-Peering with Group France Telecom

FCO_ITC.2/PeeringWithFTGroup Import with security attributes

FCO_ITC.2.1/PeeringWithFTGroup The TSF shall enforce **the following rule:**

- **Import is allowed if the destination VPN/IPv4 address belongs to the VRF table that is associated to the customer's VPN on the Partner ASBR-PE.**
- **Import is allowed if the RT associated to the VPN/IPv4 address is authorized to be transmitted between the ASBR gateway.**

when **an ASBR-PE** imports **VPN packets** from a user bound to that subject.

Non editorial refinement:

The user bound to the ASBR-PE (the subject) is another ASBR-PE in RAEI, the French MPLS/VPN network.

FCO_ITC.2.2/PeeringWithFTGroup The imported data shall be imported with the security attributes**:**

- **IPV4 addresses**

.

FCO_ITC.2.3/PeeringWithFTGroup The TSF shall associate the security attributes with the imported data.

Non editorial refinement:

Security attributes = the VPN/IPV4 destination address of the packet. This address is composed of:

- the VPN tag of the customer VPN
- the imported IPV4 destination address

FCO_ETC.1/PeeringWithFTGroup Export of data and/or security attributes

FCO_ETC.1.1/PeeringWithFTGroup The TSF shall enforce **the following rules:**

- **The customer's interface to which the flow shall be routed is found by**
  - **Selecting the VRF according to the VPN tag of the VPN packet,**
  - **Identifying the output interface using the IPV4 destination address included in the VPN packet**
- **the RT associated to the VPN/IPv4 address is authorized to be transmitted between the ASBR gateway.**

when **an ASBR-PE** exports **a customer flow (with its IPV4 address and with the VPN tag)** to a user bound to that subject.

Non editorial refinement:

Otherwise, the packet is discarded (no VRF found) or forwarded to another PE (no interface found).

5.3.3.2-Peering with other VPN Partners

FCO_ITC.2/PeeringBackToBackVRF Import with security attributes

FCO_ITC.2.1/PeeringBackToBackVRF The TSF shall enforce **the following rule:**

> **Import is allowed if the destination VPN/IPv4 address belongs to the VRF table that is associated to the customer's VPN on the Partner ASBR-PE**

when **an ASBR-PE** imports **IP packets** from a user bound to that subject.

FCO_ITC.2.2/PeeringBackToBackVRF The imported data shall be imported with the security attributes**:**

> **IPV4 addresses**

FCO_ITC.2.3/PeeringBackToBackVRF The TSF shall associate the security attributes with the imported data.

FCO_ETC.1/PeeringBackToBackVRF Export of data and/or security attributes

FCO_ETC.1.1/PeeringBackToBackVRF The TSF shall enforce **the following rules:**

> **The customer's interface to which route the data is found by**
>
> > **Selecting the VRF according to the VPN tag of the VPN packet,**
> >
> > **Identifying the output interface using the IPV4 destination address included in the VPN packet**
>
> **The VPN tag of the VPN packet is removed before export**

when **an ASBR-PE** exports **a customer flow (with its IPV4 address, but without the VPN tag)** to a user bound to that subject.

Non editorial refinement:

Otherwise, the packet is discarded (no VRF found) or the forwarded to another PE (no interface found).

5.3.3.3-Route advertising to VPN partners

FCO_ETC.1/RoutingInformation Export of data and/or security attributes

FCO_ETC.1.1/RoutingInformation The TSF shall enforce **the following rules:**

> **internal routes are not advertised to external entities**

when **a border equipment (ASBR-PE)** exports **routes** to a user bound to that subject.

Non editorial refinement:

> in the context of the TOE, the expression "routes export" is meant for "routes advertising"
>
> more explicitly "user bound to that subject" is used to designate, respectively:
>
> > an ASBR-PE of the VPN partner network, bound to a ASBR-PE of IGN

5.3.4-Management of VRFs and Routes

This section presents the requirements relating to the management of the VRF tables and to the exchange of routes between VRFs belonging to a same VPN.

FPT_RSA.1/Saturation Maximum quotas for subjects and objects

FPT_RSA.1.1/Saturation The TSF shall enforce maximum quotas for **the number of routes** that **a same VRF and a same PE** can use **simultaneously**.

FPT_RSA.1.2/Saturation The TSF shall **generate an alert signal** when a maximum quotum is **surpassed**.

FDP_ACC.1/RoutesAdvertising Access control

FDP_ACC.1.1/RoutesAdvertising The TSF shall **allow** an operation of a subject on an object **if and only if the following rules are met for the following operations:**
Export of VPN routes from a PE to its BGP neighbor:

- **Operation: Export of VPN routes from a PE to PEs in its BGP neighbor**
- **Subject: the exporting PE**
- **Object: routes of a VRF**
- **Condition: always possible. The value of the "export RT" attribute of the VRF is exported along with the routes.**

Import of a VRF from a PE

- **Operation: Import of routes of a VRF from a PE in the BGP neighbor of the receiving PE**
- **Subject: the receiving PE**
- **Object: routes of the VRF, and associated 'export RT' attribute**
- **Condition: the value of the "export RT" attribute of the received route equals one of the "import RT" attributes of the receiving VRF.**

.

Application note:

In the network, the route reflectors (RR) are specific routers that play a role of relay station. Their role is twofold:

1) they fristly receive any route advertisement messages send by PE;

2) they then transfer these messages to the others routers in the backbone.

This avoids the network to be fully-meshed.

5.3.5-PE Administration and VPN Administration

This section presents the functional requirements relating to the management of the PE configurations and of the VPNs configurations.

5.3.5.1-Identification and Authentication of Users and Subjects

This section specifies the functional requirements relating to user and subjects identification and authentication.

FIA_UAU.1/Administrators User authentication by TSF

FIA_UAU.1.1/Administrators The TSF shall authenticate a user before the user can bind to **a PE**.

Application note:

This requirement only applies to the PEs themselves, not to the PE and VPN management tools.

FIA_UAU.5/Administrators Re-authentication

FIA_UAU.5.1/Administrators The TSF shall re-authenticate the user if **after 30 minutes inactivity**
.

FIA_UAU.5.2/Administrators When this re-authentication fails, the TSF shall **unbind the user from the administrated PE**.

Global refinement:

This only applies to the PEs themselves, not to the PE and VPN management tools.

FIA_UID.2/Administrators User identification

FIA_UID.2.1/Administrators The TSF shall identify a user before the user can bind to **a management tool (i.e. a VPN configuration or PE configuration tool) or a PE**.

FIA_USB.1/Administrators User-subject binding

FIA_USB.1.1/Administrators Upon binding a user to **a PE or a management tool the security attributes of the subject shall remain unchanged**.
Non editorial refinement:
user = *administrator*

5.3.5.2-Protection of PE Configurations

FPT_TST.2/PEConfig Integrity testing

FPT_TST.2.1/PEConfig The TSF shall run a suite of tests **periodically during normal operation** to verify the integrity of **the configuration of each PE**.
Non editorial refinement:

This test shall be performed weekly.

The conformity check shall consist in verifying that each PE configuration meets some security requirements (presence or absence of directives related to security, routing of packet to the right interface of the PE,...) and, in checking using a probe whether the internal equipments of the network are reachable.

The conformity of the PE configuration is checked against a collection of security templates for the PE configuration.

FDP_ACC.1/AdministrationFlows Access control

FDP_ACC.1.1/AdministrationFlows The TSF shall **allow** an operation of a subject on an object **if and only if the following rules are met:**
the subject shall operate from ControlNet

- **operation: exchange administration flows with the object**
- **subject's attributes:**
  - **origin address of the flow: within the range of addresses of the ControlNet**

.
Non editorial refinement:

- *object* = a PE router
- *subject* = a management tool sending administration flows to the PE router

Application note:

No authentication of the subject itself is required on the PE. However, as previously required, the user shall be identified (*FIA_UID.1/Administrators*), authenticated (*FIA_UAU.1/Administrators*) and logged to the PE (*FIA_USB.1/Administrators*) before being able to access the PE through a management tool.

5.3.6-Management of the Administrators' Accounts

This section presents the functional security requirements covering the management of the administrators' accounts and profiles.

FDP_ACC.1/AdminProfiles Access control

FDP_ACC.1.1/AdminProfiles The TSF shall **allow** an operation of a subject on an object **if and only if one of the following rules is met:**

- **operation: ip command and arguments sent on a router**
- **subject: the router management tool**
- **object: a equipment on the backbone (P, PE, RR, ControlNet router)**
- **conditions:**
  - **the equipment belongs to the *scope* the router administrators may access**
  - **the command sent and the arguments passed are included in the router administrators access *profile*.**

FDP_ISA.1/AdminProfiles Security attribute initialization

FDP_ISA.1.1/AdminProfiles The TSF shall **use the following rules**

- **the router administrator's profile shall indicate the set of accessible routers: the router administrator's scope. The scope shall be one or a list of the predefined scopes, or a sub-scope of a predefined scope**
- **the router administrator's profile shall indicate the access level granted to the router administrator for each scope. The access profile shall be one of the predefined access profiles**

to assign an initial value to the security attribute **user profile** whenever a **new router administrator account** is created.

Global refinement:

This requirement only concerns the creation of router administrators' profiles on the authentication servers.

Application note:

Scopes may be defined to permit a router administrator to access only to some types of routers. For instance, accesses may be granted to allows a router administrator reaching ControlNet, ASBR-PEs, backbone routers (P or RR routers) or PE routers.

The type accesses allowed for a router administrator may be only to read routers configurations and/or to perform some write commands. Access profiles are defined as lists of authorized commands and parameters.

FIA_URE.2/Administrators User registration with storage of authentication data

FIA_URE.2.1/Administrators The TSF shall be able to register new users.

Non editorial refinement:

users = administrators

FIA_URE.2.2/Administrators [Editorially Refined] The TSF shall **obtain values for user's login and authorizations (profile) from *privileged users (i.e. having an tool or administration user profile)***.

FIA_URE.2.3/Administrators The TSF shall store these user security properties in **dedicated authentication servers (managing groups dedicated to router administrators' authentication)**.

FIA_URE.2.4/Administrators [Editorially Refined] The TSF shall **receive authentication data from the *super-user registering the user***.

FIA_URE.2.5/Administrators The TSF shall store this authentication data in **each authentication servers' storage space**.

5.3.7-Protection of Administration Flows

FCO_IID.1/AdministrationFlows Integrity of imported data without recovery

FCO_IID.1.1/AdministrationFlows The TSF shall monitor the integrity of **imported administration requests** provided to **a management tool** by a user bound to that subject for **deletion, insertion, modification and replay** anomalies.

FCO_IID.1.2/AdministrationFlows On detection of an anomaly the TSF shall discard the data and/or security attributes.

FCO_IED.1/AdministrationFlows Integrity of exported data without recovery

FCO_IED.1.1/AdministrationFlows When **an administration tool** transmits **responses to administration requests** to a user bound to that subject, the TSF shall provide that user the means to detect **modification, deletion, insertion and replay** anomalies.

FCO_CID.1/AdministrationFlows Confidentiality of imported data

FCO_CID.1.1/AdministrationFlows The TSF shall assist in protecting the confidentiality of **administration requests** provided to **a management tool** by a user bound to that subject.

FCO_CED.1/AdministrationFlows Confidentiality of exported data

FCO_CED.1.1/AdministrationFlows The TSF shall protect the confidentiality of **responses to administration requests** provided by **a management tool** to a user bound to that subject.

5.3.8-Audit and Protection of the Audit Tracks

This section describes the functional security requirements regarding audit trails management.

It covers both the aspects of log generation, with respect to functional security requirements defined above, the aspects of audit trails protection, and also the time stamping service that is supporting the audit activities.

FAU_GEN.2/AuditTracks Audit data generation with time

FAU_GEN.2.1/AuditTracks The TSF shall store an audit record in **the equipment/tool [1]** of the following events:

- **Authentication / identification on the router (successful or erroneous) [PE router];**
- **Authentication request on an authentication server [TACACS server, depending on the authentication request];**
- **Modification in the configuration of a PE router [PE router, TACACS server].**
- **Exceedance of a maximum number of routes in a VRF or in a PE [PE router] and shut-down of the audit functions**.

Non editorial refinement:

[1]: the audit records shall be stored on the equipment on which the auditable operation is performed. For each of the above-listed events, the equipment or the tool where the audit record is stored is specified between brackets.

FAU_GEN.2.2/AuditTracks The TSF shall record within each audit record the following information:

a) Date and time of the event, type of event, values of **the subject's identity and the user's identity**, the **success and failure** of the event; and

b) **None**.

Application note:

In point a) of FAU_GEN.2.2:

- the subject's identity is the name of the application used to change the router configuration
- the user's identity is the login of the administrator who changed the router configuration

FMI_TIM.1/TimeReference Time stamps

FMI_TIM.1/TimeReference The TSF shall maintain the current time in **the Time Server** to an accuracy of **1 second**.

FDP_ACC.1/TimeReference Access control

FDP_ACC.1.1/TimeReference The TSF shall **allow** an operation of a subject on an object **if the following rules are met:**

- **Operation: change of the *time reference* or of the *time source configuration***
- **Subject: the time server**
- **Object: the time reference**

- **Condition: the user bound to the time server is identified and authenticated**

FAU_SAA.1/LogCorrelation Potential violation analysis

FAU_SAA.1.1/LogCorrelation The TSF shall 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/LogCorrelation The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of **a subset of the events collected by netForensics** known to indicate a potential TSP violation;
b) **no other rules**.

5.3.8.2-Access to Audit Trails

FDP_ACC.1/AuditTracks Access control

FDP_ACC.1.1/AuditTracks The TSF shall **allow** an operation of a subject on an object **if and only if:**

- **Operation: *read PE management logs (including VPN production logs)***
  - **Object: audit tracks of a PE**
  - **Subject: management tool**
  - **Condition: the router administrator is successfully authenticated, is authorized to access the router (router administrators' access scope) and is authorized to read the router logs (router administrator access profile)**
- **Operation: *modify* and *delete***
  - **Object: audit tracks of a PE**
  - **Subject: an administrator**
  - **Condition: never allowed.**

.

Global refinement:

these rules apply on the centralized syslog management tools (netForensics)

FPT_RSA.1/AuditTracks Maximum quotas for subjects and objects

FPT_RSA.1.1/AuditTracks The TSF shall enforce maximum quotas for **storage resources** that **the log centralization server** can use **simultaneously**.

FPT_RSA.1.2/AuditTracks The TSF shall **replace the oldest tracks** when a maximum quotum is **surpassed**.
Non editorial refinement:

The log concentration server shall be managed so that:

> logs are available online on the server during 3 months

> then logs are archived on a permanent storage medium

5.4-Security assurance requirements

The security assurance requirement level is EAL2. The EAL is augmented with ALC_FLR.1.

5.5-Dependencies

5.5.1-Security functional requirements dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCO_ETC.1/VPNFlows	No dependencies	
FCO_ITC.2/CEAdminFlows	(FCO_IID.1 or FCO_IID.2)	
FCO_ETC.1/CEAdminFlows	No dependencies	
FCO_ITC.2/VPNFlows	(FCO_IID.1 or FCO_IID.2)	
FCO_ETC.1/VPNFlows	No dependencies	
FPT_RSA.1/Saturation	No dependencies	
FDP_ACC.1/RoutesAdvertising	(FDP_ISA.1)	
FDP_ACC.1/AdminProfiles	(FDP_ISA.1)	FDP_ISA.1/AdminProfiles
FDP_ISA.1/AdminProfiles	(FDP_ACC.1)	FDP_ACC.1/AuditTracks
FIA_URE.2/Administrators	(FDP_ACC.1)	FDP_ACC.1/AdminProfiles
FCO_IID.1/AdministrationFlows	No dependencies	
FCO_IED.1/AdministrationFlows	No dependencies	
FCO_CID.1/AdministrationFlows	No dependencies	
FCO_CED.1/AdministrationFlows	No dependencies	
FCO_ITC.2/PeeringWithFTGroup	(FCO_IID.1 or FCO_IID.2)	
FCO_ETC.1/PeeringWithFTGroup	No dependencies	
FCO_ITC.2/PeeringBackToBackVRF	(FCO_IID.1 or FCO_IID.2)	
FCO_ETC.1/PeeringBackToBackVRF	No dependencies	
FCO_ETC.1/RoutingInformation	No dependencies	
FIA_UAU.1/Administrators	(FIA_UID.2) and (FIA_URE.2)	FIA_URE.2/Administrators, FIA_UID.2/Administrators
FIA_UAU.5/Administrators	(FIA_UAU.1 or FIA_UAU.2)	FIA_UAU.1/Administrators
FIA_UID.2/Administrators	(FIA_USB.1)	FIA_USB.1/Administrators
FIA_USB.1/Administrators	No dependencies	
FPT_TST.2/PEConfig	No dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FDP_ACC.1/AdministrationFlows	(FDP_ISA.1)	
FAU_GEN.2/AuditTracks	(FMI_TIM.1 or (FCO_IID.1 and FCO_ITC.1)) and (FDP_ACC.1) and (FPT_RSA.1)	FMI_TIM.1/TimeReference, FDP_ACC.1/AuditTracks, FPT_RSA.1/AuditTracks
FMI_TIM.1/TimeReference	(FDP_ACC.1)	FDP_ACC.1/TimeReference
FDP_ACC.1/TimeReference	(FDP_ISA.1)	FDP_ISA.1/AdminProfiles
FAU_SAA.1/LogCorrelation	(FAU_GEN.1)	FAU_GEN.2/AuditTracks
FDP_ACC.1/AuditTracks	(FDP_ISA.1)	FDP_ISA.1/AdminProfiles
FPT_RSA.1/AuditTracks	No dependencies	

Table 3: Functional requirements dependencies

5.5.1.1-Rationale for the exclusion of dependencies

The dependency FCO_IID.1 or FCO_IID.2 of FCO_ITC.2/CEAdminFlows is unsupported.

The IPv4 protocols do not include any integrity check on the destination address sent to a router.

The dependency FCO_IID.1 or FCO_IID.2 of FCO_ITC.2/VPNFlows is unsupported.

The IPv4 protocols do not include any integrity check on the destination address sent to a router.

The dependency FDP_ISA.1 of FDP_ACC.1/RoutesAdvertising is unsupported.

This access control policy is based on the notion of BGP neighbour.

When a new PE is added in the network, the installation procedures include the instructions declaring this new router to its neighbour routers.

This procedure is an organisational procedure that cannot be the subject of a functional requirement.

The dependency FCO_IID.1 or FCO_IID.2 of FCO_ITC.2/PeeringWithFTGroup is unsupported.

The IPv4 protocols do not include any integrity check on the destination address sent to a router.

The dependency FCO_IID.1 or FCO_IID.2 of FCO_ITC.2/PeeringBackToBackVRF is unsupported.

The IPv4 protocols do not include any integrity check on the destination address sent to a router.

The dependency FDP_ISA.1 of FDP_ACC.1/AdministrationFlows is unsupported.

The dependency with component *FDP_ISA.1* is not satisfied because, on each PE, the range of authorized addresses is parameterized when the PE is configured for the first time. This is addressed by the policy *OD.LifeCycleConstraints* which is covered by the assurance requirement *AGD_OPE.1*.

Note that the management of this range of authorized addresses is then done as part of a PE configuration procedure. All the requirements applying to PE configuration remain thereby applicable.

5.5.2-Security assurance requirements dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.2, ADV_TDS.1
ADV_FSP.2	(ADV_TDS.1)	ADV_TDS.1
ADV_TDS.1	No dependencies	
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.2
AGD_PRE.1	No dependencies	
ALC_CMC.2	(ALC_CMS.1)	ALC_CMS.2
ALC_CMS.2	No dependencies	
ALC_DEL.1	No dependencies	
ALC_FLR.1	No dependencies	
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies	
ASE_INT.1	No dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.1)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies	
ASE_TSS.1	(ASE_INT.1) and (ASE_REQ.1)	ASE_INT.1, ASE_REQ.2
ATE_COV.1	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.2, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.1
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_FUN.1)	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_FUN.1
AVA_VAN.2	(ADV_ARC.1) and (ADV_FSP.1) and (ADV_TDS.1) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

Table 4: Assurance requirements dependencies

6-TOE summary specification

6.1-Organizational security measures

SM.AccessControl.Physical

This security measure is specified in the following document:

> [Physical Security Controls]

SM.CE.AccessControl.Physical

This security measure is specified in the following document:

> [Physical Security Controls in Customer premises], §5.5.

SM.AccessControl.Providers

This security measure is specified in the following documents:

> [Provider Access Management]

> [Third party access Management]

.

SM.Administrators.Training

This security measure is specified in the following document:

> [Equant Security Policy]

SM.Administrators.RemoteAccesses

This security measure is specified in the following document:

> [NUAR Registration Procedure]

SM.ServersManagement

This security measure is specified in the following documents:

> [ESSC – Security Standard]

> [ESSC – Implementation Solaris]

> [Unix - Security Policy]

SM.Passwords.Management

This security measure is defined in the following documents:

> [NUAR Registration Procedure]

SM.OperationAndMaintenance

This security measure is defined in the following documents:

> [Material Maintenance Service]

SM.ControlAtProductionTime

This security measure is defined as part of the service initialization process. The related test procedure is defined in

> [ALC_DEL.1, §3]

6.2-TOE security functions

6.2.1-Management of Customer Flows

SF.AccessControlOnVPNFlows

This security function ensures the access control on the VPN flows imported in and exported from the customers VPNs.

This function is implemented:

> in the PEs, at the interconnection with the customers' CEs. It covers the isolation of the VPN flows from one customer VPN to another and the isolation of the CE management VPN from the other flows.

> in the ASBR-PEs, at the interconnection with the VPN partners. This covers two types of interconnections: the interconnection with RAEI, in MP-eBGP mode, where VPN tags are exchanged with the partner, and the other interconnections, made on a back-to-back VRF model.

SF.ExchangesOfVPNRoutes

This security function ensures controlled exchanges of VPN routes between VRFs within the TOE.

The VPN routes are exported from a PE with the value of the attribute "export Route Target", which is indicated in the VRF.

The routes can be imported in a VRF of another PE only if the exported RT appears in the importing VRF as value of attribute "import Route Target".

The couple of attributes "import Route Target" and "export Route Target" therefore allow to confine the advertising of the RT in a same VPN. This mechanism ensures that the routes defining a VPN can be advertised only in routing tables associated to it.

6.2.2-Interconnection with other Networks

SF.UnreachabilityOfEquipements

This security function ensures that the addresses of the routing equipments located inside the TOE are not advertised to the interconnected networks.

Its implementation encompasses two technical measures: 1) Correct parameterization of the PE to prevent internal route (and addresses) advertising; 2) A check performed using a probe on the Internet, to ensure that the internal addresses of the network cannot be reached from the Internet.

6.2.3-PEs and VPNs secure administration

This section presents the security function related to the secure administration of the PEs and VPNs, which encompasses:

> Administrators authentication (*SF.Authentication*);

> Requiring the administration flows to rebound in one of the administration areas (*SF.AdministrationFlowsRebound*);

> Protecting the administration flows against disclosure and modification (*SF.ProtectionOfAdministrationFlows*).

SF.Authentication

The control of the remote access to the PEs is based on an authentication based on a login/password. This authentication is ensured via an authentication, authorization and accounting server.

Each PE administrator has a dedicated user account and specific access rights (a profile).

When an identification and authentication session succeeds, the authentication server applies the user profile (PE administrator / VPN administrator) to the authenticated user.

For heavy maintenance operations, staffs of the providers use specific PE administrators accounts with restricted rights (read only).

SF.ReboundOfAdministrationFlows

This security function ensures access control to the administration functions.

The PEs only accept administration flows originated from tools hosted in ControlNet.

The PE administrators and the VPN administrators therefore must use management tools hosted in ControlNet to operate on the PEs.

SF.ProtectionOfAdministrationFlows

Protection of the administration flows.

The administration data exchanged between the administrators workstations in OBS's intranet and the tools in ControlNet are transmitted through SSL or SSH sessions (depending on the tools).

These protocols ensure:

> authentication of the server to the client;

> monitoring the integrity of exchanges data;

> confidentiality of exchanged data.

6.2.4-Administration of the Tools

SF.ToolsAdministration

Management of the management tools and servers

The tools and the servers in ControlNet define specific functionality allowing to configure them, to manage users accounts, etc. They define specific management profiles for the users in charge of their management.

Application note:

Others aspects of tools' management are already covered by other security functions:

> *SF.Authentication* covers authentication of the tools administrators;

> *SF.ProtectionOfAdministrationFlows* covers the protection of tools administration flows.

6.2.5-Monitoring of PE Configurations

This section presents the security function addressing the monitoring of the PE configurations. This encompasses:

> Monitoring the global configuration of the PEs (*SF.PEGlobalConfigurationsMonitoring*), and

> Monitoring the VPN configurations on the PEs (*SF.VPNMonitoring*).

SF.PEGlobalConfigurationsMonitoring

Verification of the global configuration of the PEs.

The PE configurations are collected daily on the configuration server.

This function checks that elements related to security are actually in place in the global configuration of each PE.

SF.VPNMonitoring

Verification of the VPNs

The PE configurations are collected daily on configuration server.

This function ensures that no inconsistency is detected in the route import/export rules and that the flows of each VPN are actually exported to the corresponding client interface.

6.2.6-Audit and Management of the Audit Trails

SF.Audit

Audit of the administration operations and alert triggering.

PE Administration The traces of the events related to the administration of the PEs are recorded on the TACACS server and then collected on a log concentration server.

The logs of PE administration are accessible to users that can access the PE, according to their profile. They are accessible in read, and only in read, through the netForensic tool by the monitoring staff.

VPN Administration

The traces of the events related to the administration of the VPNs are recorded on:

- The authentication servers, and accessible to the VPN administrators and VPN supervision staff through a tools dedicated to collect and filter the generated logs;
- The VPN production tool, under the users' accounts;
- The authentication servers that log any connection request.

The logs of VPN administration are accessible in read through the netForensics tool to the monitoring staff.

Alarm Triggering

The PEs are recording the most important administration events (any write operation). In particular, an alert is triggered when the number of routes on a same VRF or a same PE reaches a given threshold.

These alarms are triggered via netForensics.

SF.TimeReference

Time reference.

The TOE has a unique time reference provided by an NTP server at its disposal.

The management of the time reference is restricted to the administrators of the NTP server.

6.3-Associations between TOE summary specification and security requirements

6.3.1-Associations between the security measures and support requirements

Support requirements	Security measures
SSR.AccessControl.Physical	SM.AccessControl.Physical

Support requirements	Security measures
SSR.CE.AccessControl.Physical	SM.CE.AccessControl.Physical
SSR.AccessControl.Providers	SM.AccessControl.Providers
SSR.Administrators.Training	SM.Administrators.Training
SSR.Administrators.RemoteAccesses	SM.Administrators.RemoteAccesses
SSR.SystemSecureManagement	SM.SystemSecureManagement
SSR.Passwords.Management	SM.Passwords.Management
SSR.ControlAtProductionTime	SM.ControlAtProductionTime

6.3.2-Associations between the security functions and functional requirements

Functional requirements	TOE security functions
FCO_ETC.1/VPNFlows	SF.AccessControlOnVPNFlows
FCO_ITC.2/CEAdminFlows	SF.AccessControlOnVPNFlows
FCO_ETC.1/CEAdminFlows	SF.AccessControlOnVPNFlows
FCO_ITC.2/VPNFlows	SF.AccessControlOnVPNFlows
FCO_ETC.1/VPNFlows	SF.AccessControlOnVPNFlows
FCO_ITC.2/PeeringWithFTGroup	SF.AccessControlOnVPNFlows
FCO_ETC.1/PeeringWithFTGroup	SF.AccessControlOnVPNFlows
FCO_ITC.2/PeeringBackToBackVRF	SF.AccessControlOnVPNFlows
FCO_ETC.1/PeeringBackToBackVRF	SF.AccessControlOnVPNFlows
FCO_ETC.1/RoutingInformation	SF.UnreachabilityOfEquipements
FPT_RSA.1/Saturation	SF.Audit
FDP_ACC.1/RoutesAdvertising	SF.ExchangesOfVPNRoutes
FIA_UAU.1/Administrators	SF.Authentication
FIA_UID.2/Administrators	SF.Authentication
FIA_USB.1/Administrators	SF.Authentication
FIA_UAU.5/Administrators	SF.Authentication
FPT_TST.2/PEConfig	SF.PEGlobalConfigurationsMonitoring, SF.VPNMonitoring, SF.UnreachabilityOfEquipements
FDP_ACC.1/AdministrationFlows	SF.ReboundOfAdministrationFlows
FDP_ACC.1/AdminProfiles	SF.ToolsAdministration
FDP_ISA.1/AdminProfiles	SF.Authentication, SF.ToolsAdministration
FIA_URE.2/Administrators	SF.Authentication
FCO_IID.1/AdministrationFlows	SF.ProtectionOfAdministrationFlows
FCO_IED.1/AdministrationFlows	SF.ProtectionOfAdministrationFlows
FCO_CID.1/AdministrationFlows	SF.ProtectionOfAdministrationFlows
FCO_CED.1/AdministrationFlows	SF.ProtectionOfAdministrationFlows
FAU_GEN.2/AuditTracks	SF.Audit

Functional requirements	TOE security functions
FMI_TIM.1/TimeReference	SF.TimeReference
FDP_ACC.1/TimeReference	SF.TimeReference
FAU_SAA.1/LogCorrelation	SF.Audit
FDP_ACC.1/AuditTracks	SF.Audit
FPT_RSA.1/AuditTracks	SF.Audit

Table 5: Functional requirements towards security functions association

TOE security functions	Functional requirements
SF.AccessControlOnVPNFlows	FCO_ETC.1/VPNFlows, FCO_ITC.2/CEAdminFlows, FCO_ETC.1/CEAdminFlows, FCO_ITC.2/VPNFlows, FCO_ETC.1/VPNFlows, FCO_ITC.2/PeeringWithFTGroup, FCO_ETC.1/PeeringWithFTGroup, FCO_ITC.2/PeeringBackToBackVRF, FCO_ETC.1/PeeringBackToBackVRF
SF.ExchangesOfVPNRoutes	FDP_ACC.1/RoutesAdvertising
SF.UnreachabilityOfEquipements	FCO_ETC.1/RoutingInformation, FPT_TST.2/PEConfig
SF.Authentication	FDP_ISA.1/AdminProfiles, FIA_URE.2/Administrators, FIA_UAU.1/Administrators, FIA_UAU.5/Administrators, FIA_UID.2/Administrators, FIA_USB.1/Administrators
SF.ReboundOfAdministrationFlows	FDP_ACC.1/AdministrationFlows
SF.ProtectionOfAdministrationFlows	FCO_IID.1/AdministrationFlows, FCO_IED.1/AdministrationFlows, FCO_CID.1/AdministrationFlows, FCO_CED.1/AdministrationFlows
SF.ToolsAdministration	FDP_ACC.1/AdminProfiles, FDP_ISA.1/AdminProfiles
SF.PEGlobalConfigurationsMonitoring	FPT_TST.2/PEConfig
SF.VPNMonitoring	FPT_TST.2/PEConfig
SF.Audit	FPT_RSA.1/Saturation, FAU_GEN.2/AuditTracks, FAU_SAA.1/LogCorrelation, FDP_ACC.1/AuditTracks, FPT_RSA.1/AuditTracks
SF.TimeReference	FMI_TIM.1/TimeReference, FDP_ACC.1/TimeReference

Table 6: Security functions towards functional requirements association

7-Annexes

7.1-Referenced Documents

ESR 10K Hardware Installation Guidance
« Installation Network Agreement for ESR 10000 hardware as PE router » - Ref: NE-IGN-CISCO/INA 0002 – Version: 14

ESR 10K Software Installation Guidance
« Software agreement for CISCO ESR 10K 12.0.25SX9 IOS release on RAEI and IGN backbones » - Ref : NE-IGN-CISCO/RCN 010 – Version: 1.0, 05/21/2007

IPVPN Overview
«MANUAL OPERATOR GUIDANCE Global IP VPN - Overview » - Ref: AUTO-001363 - Alias OPINFO/INF 001611) – Version 1.0, 08/03/2005

IPVPN Configuration
« MANUAL OPERATOR GUIDANCE Global IP VPN – Configuration » - Ref: AUTO-001363 Alias OPINFO/INF 001612 – Version 1.0, 09/28/2006

IPVPN Troubleshooting
« MANUAL OPERATOR GUIDANCE Global IP VPN – Troubleshooting » - Ref: AUTO-001613 - Alias OPINFO/INF 001613 – Version 1.0 , 08/03/2005

Quick Guide – Troubleshooting IP Faults
«Quick guide to trouble shoot IP Faults » - Ref: GCS/CVM/01/002 – Version .1.4 – 02 Feb 2002

Generic PE – Overview
« MANUAL OPERATOR GUIDANCE ESR10K GenericPE overview » - Ref: AUTO-001840 - Alias OPINFO/INF 001840 – Version 1.0, 06/08/2004

Generic PE – Configuration
« MANUAL OPERATOR GUIDANCE ESR10K GenericPE Configuration Guidelines » - Ref: AUTO-001841 - Alias OPINFO/INF 001841 – Version 1.0, 04/11/2005.

Generic PE – Troubleshooting
« MANUAL OPERATOR GUIDANCE ESR10K GenericPE Toubleshooting Guidelines » - Ref: AUTO-001843 – Alias OPINFO/INF 001843 - Version 1.0, 11/01/2004

IPVPN for Partners – Overview
«MANUAL OPERATOR GUIDANCE IP VPN for Partners – Overview » - Ref: AUTO-001796 Alias OPINFO/INF 001796 –Version 1.0, 11/28/2005

IPVPN for Partners – Configuration
«MANUAL OPERATOR GUIDANCE IP VPN for Partners - Configuration Guide » - Ref: AUTO-001797 – Alias OPINFO/INF 001797 – Version 1.0, 10/17/2005

IPVPN for Partners – Troubleshooting
« MANUAL OPERATOR GUIDANCE IP VPN For Partners - Troubleshooting Guide» - Ref: AUTO-001798 Alias OPINFO/INF 001798 – Version 1.0, 11/28/2005

NA_EVSYS
Note d'application – Interprétation des CC pour les évaluations de systèmes, NOTE/07.1draft5, SGDN/DCSSI/SDR, 04 juillet 2007.

Physical Security Controls

«Photo ID and Facility Access Control Policy» - Ref: EM-SM-0008 - Version 1.3, October 30, 2007

Physical Security Controls in Customer premises

«IP VPN Service Security Policy » – Ref: POL-SEC-NS-07 – version 2.8 July, 2006

Provider Access Management

«Equipment Supplier Access Security Policy» - Ref: POL-SEC-NS-09 – version 2.4 - October 26, 2007

Third party access Management

«Third Party Access Security Policy» - Ref: POL-SEC-NS-11 – Version 1.6 October 30, 2007

Equant Security Policy

«Equant Security Policy» - Ref : POL-SEC-CS-003 – Version: 3, March 2002

NUAR Registration Procedure

«NUAR Registration Procedure» -Ref: NA - v.1.2 – 11/18/02

ESSC – Implementation Solaris

«ESSC Security standard implementation for Solaris 8, 9 & 10 » - Ref : ESSC-SESM-SOL-01 - Version: 0.4, 08/08/2007

ESSC – Security Standard

«Equant Server Security Certification - Security Standard » - Ref : N.A Version: 1.1, 21/08/2007

Unix - Security Policy

«Unix systems security policy » -Ref : POL-SEC-NS-04 – Version: 1.4, 06/26/2006

Material Maintenance Service

«Equant_SSM-schedule-A-Service-Description» -Word Format – ref: N.A

ALC_DEL.1

«Service delivery procedure Unix systems security policy » -Ref : MEXT-77CGDG – Version: 1.2, 12/14/2007

TACACS – Installation Guide

«Equant TACACS – Installation Guide» - ref. MDAM-7BHMEA, version 1.0 – 02/04/2008

TACACS –SIF

« System Integration Form - Tacacs Plus authentication & synchronization Unified access to the IP routers project » - Ref : IS/SIF/000000 – Version : Version : 2.0, 01/31/2008

TACACS-Troubleshooting

« Internal Purple Tacacs Troubleshooting & Operations Procedures » - Ref : TACACS_EQUANT/ OPI 0001 v2T1 – Version: v1.2, 03/27/2006

IPTOOLBOX –SIF

« System Integration Form IPTOOLBOX » - Ref : IS/SIF/000000 - Version :2.2 - 02/01/08

IPCFM – WebAdmin Manual

«IPCFM – WebAdmin User Guide » - Ref: N/A – Version 1.0, 10/26/2007

IPCFM –SIF

« System Integration Form IP – CFM » - Ref: IS/SIF/000000 - Version :2.4, 08/03/2007

Firewalls CNT/IGN – RCN

«CIMP Release Control Notice » - Ref : N/A – Version: 1.5, 09/25/2007

Firewalls EIN/CNT – RCN

«Release Control Notice - ControlNet FireWalls Project » - Ref: CNT FW Release Control Notice – Version : 1.4.1, 07/05/2007

nFX – Alarm Management

« netForensics CE Alarms Handbook » - Ref : N/A – Version: 1.6, 07/20/2007

nFX –Handbook

«nF Security Handbook All Perimeters» - Ref : N/A – Version : 1.4, Jan 2007 – Format : Microsoft Powerpoint

nFX OSP – SIF

« System Integration Form SOC netForensics Security Information Management Application » - Ref: IS/SIF/000000 – Version: 1.0.1, Jan 2008

nFX OSP user training

«nFX Open Security Platform User Training» - ref. n.a

NTS – 200 –User Manual

«NTS-200-GPS User's Manual» - Ref : NA – February 2005

SAFE – MI

«EQT096 INSTALLATION MANUAL SAFE version 2.1» - Ref: EQT096-MI-2.1 – Version:1.0, 26 Feb 2007

SAFE – MU

« SAFE USER GUIDE V2.0 » - Ref: N/A – Version: 1.8, Jan 2007

GINI/XIPI – FTP SIF

« GINI/XIPI-FTP/SFTP server in the ControlNet - System Integration Form» - Ref: n.a

7.2-Index

T

V

7.3-Abbreviations

Abbreviation	Meaning
AAA	Authentication, Autorisation and Accounting
AS	Autonomous System
ASBR	Autonomous System Border Router
BEW	Business Everywhere
BGP	Border Gateway Protocol
eBGP	Exterior Border Gateway Protocol
iBGP	Interior Border Gateway Protocol
CC	Common Criteria (CC term)
CE	Customer Edge
DMZ	De-Militarised Zone
DSL	Digital Subscriber Line
EAL	Evaluation Assurance Level (CC term)
EIN	Equant IntraNet
GIBN	Global Internet Backbone Network
GRT	Global Routing Table
GW	Gateway
HPOV	HP OpenView
IAR	Internet Access Router
IGN	IP Global Network
IOS	Internetwork Operating System
IP	Internet Protocol
IPSEC	IPSECurity
IPV4	Internet Protocol Version 4
IPVPN	Equant IPVPN : name of the managed MPLS VPN service of Orange Business Services
IS-IS	Intermediate system to intermediate system
ISP	Internet Service Provider
LAN	Local Area Network
LIN	Local Internet Network
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
NBIG	Network Based Internet Gateway
NTP	Network Time Protocol

Abbreviation	Meaning
OSI	Open systems interconnection
OSP	Organisational security policy
PC	Personal computer
PDA	Personal digital assistance
PE	Provider Edge
PAT	Port Address Translation
RAEI	Réseau d'Accès des Entreprises à Internet
RBCI	Réseau Backbone et de Collecte Internet
RD	Route Distinguisher
RR	Route Reflector
RT	Route Target
SAFE	Security Assessment and Followup Engine
SIA	Secure ISP Access
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
SYSLOG	SYStem LOG
TACACS	Terminal.Access Controller.Access.Control System
RADEQUA	Réseau d'Accès aux EQUipements Administrés
TELNET	TErminal NETwork
TOE	Target Of Evaluation
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding

7.4-Glossary

Term	Definition
Autonomous system	An autonomous system is a network or a set of networks being under the control of an entity that applies a consistent routing policy. Each autonomous system is identified using an Autonomous System Number (ASN) allocated for BGP routing.
ASBR	A router ensuring the interconnection between two autonomous systems.
Business Everywhere	Business Everywhere is a service of Orange Business Services allowing customers of the Equant IPVPN service to extend their intranet to nomad terminals (laptops, workstations, mobile phones).
BGP	BGP BGP is a routing protocol allowing to route information at the border of an autonomous system and between autonomous systems. This protocol is the routing protocol Internet uses. See also iBPG et eBGP.
CE	A router located in a customer's premises and ensuring the interconnection between customers LAND and the shared network.
HPOV	Software suite provided by Hewlett Packard allowing wide scale network and system management.
IGN	The IGN network is the MPLS/VPN network managed by Orange business Services on a worldwide and translational perimeter. This network allows multinational companies to connect their sites located around the world. Thanks to partnerships with local operators, the connectivity can also be extended to countries Orange Business Services does not covers. The extention to France is a specific example of such a partnership.
IPVPN	Equant IPVPN : name of the managed MPLS VPN service of Orange Business Services
IS-IS	IS-IS is an Interior Gateway Protocol (IGP) used inside an autonomous system.
eBGP	Routing protocol in the BGP family used to route information between two autonomous systems.
iBGP	Routing protocol in the BGP family used to route information inside an autonomous systems.
MPLS/VPN	MPLS VPN is a family of methods allowing to take advantage of the MPLS protocol to create virtual private networks. The created VPNs are based on the separation and the differentiation of the virtual networks flows without any substantial overhead. This technology allows very important rates as well as a fine management of the service quality.
NTP	NTP is a protocol allowing clients to manage their synchronisation with a dedicated time reference

Term	Definition
OSI	OSI is a network standardization initiative that, in particular, defined a reference model for network protocols enabling their interoperability. By extension, the OSI levels are the commonly used levels at which network protocols may be defined.
PE	PE routers are routers located at the border of an autonomous system to ensure the interconnection with customers' sites (the use CE routers) and the shared network.
ASBR-PE	See ASBR.
RAEI	The RAEI network is a multiservice managed by Orange Business Services, il est dédié aux flux des enterprises in France. The term multiservice means that the network provides the customers with various services, such as the transportation of corporate VPN flows and customer's Internet flows.
Peer routers	Peer routers are routers located on both sides of the interconnection between two networks. At the interconnections between IGN and the VPN partners, the peer routers are ASBR-PE routers..
SAFE	SAFE is a security monitoring tool involved in the supervision of the PEs' global configuration.
SNMP	SNMP is a protocol allowing the remote administration of network components
Syslog	Accounting message generated by a network component.
TACACS	TACACS is a authentication, autorization and accounting protocol.
TELNET	TELNET is a protocol allowing direct remote connection to network components in a shell console.
VPN	In this document, and in the documents provided as part of this evaluation, the term VPN is used to identify a virtual entity fully managed by Orange Business Services and allowing the connection of distant customers' sites with each others. As a consequence, the term VPN flows, also referred to as IPVPN flows, only applies to data transfers inside the IGN network. The flows between a PE and a customers's site simply are IPV4 flows. As a consequence, from a physical perspective, the CE routers located in the customers' premises cannot be considered a supporting the VPNs. The logical entity encompassing customer's flows from one site (ie. a CE router) to another (ie. another CE router) is referred to as the term "intranet".
VRF	A VRF is a virtual routing table containing the different commands defining a customer's VPN on a router. One can say that a VPN is globally defined using all the VRFs defined on the PEs at the interconnection with the customers' sites.

Business
Services

orange™