PREMIER MINISTRE

Secrétariat général de la Défense nationale

Direction centrale de la sécurité des systèmes d'information

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

Rapport de certification 2001/24

Cloisonnement des réseaux privés virtuels dans le cadre du service Equant IP VPN

(version 1.0)

Janvier 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

CERTIFICAT 2001/24

Cloisonnement des réseaux privés virtuels dans le cadre du service Equant IP VPN

(version 1.0)

Développeur : Equant
Exploitant : France telecom transpac

Critères Communs
EAL1 Augmenté

Commanditaires : Equant, France telecom transpac

Le 7 janvier 2002,

Les Commanditaires :
Le Directeur général
de France telecom transpac
Philippe Bernard

L'Organisme de certification :
Le Directeur central de la sécurité
des systèmes d'information
Henri Serres

Le Directeur ingénierie produit et
développement d'Equant
Philippe Laplane

Cette solution a été évaluée par un centre d'évaluation de la sécurité des TI conformément aux Critères Communs pour l'évaluation de la sécurité des TI version 2.1 et à la méthodologie commune pour l'évaluation de la sécurité des TI version 1.0.

Ce certificat ne s'applique qu'à la version évaluée de la solution dans sa configuration d'évaluation et selon les modalités décrites dans le rapport de certification associé. L'évaluation a été conduite en conformité avec les dispositions du Schéma français d'évaluation et de certification de la sécurité des TI. Les conclusions du centre d'évaluation enregistrées dans le rapport technique d'évaluation sont cohérentes avec les éléments de preuve fournis.

Ce certificat ne constitue pas en soi une recommandation de la solution par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise. Ce certificat n'exprime directement ou indirectement aucune caution de la solution par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

Organisme de certification :
Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Chapitre 1

Résumé

1.1 Objet

1 Ce document est le rapport de certification de la solution «Cloisonnement des réseaux privés virtuels dans le cadre du service Equant IP VPN (version 1.0)».

2 La cible d'évaluation est un sous-ensemble représentatif du service Equant IP VPN sur le territoire français. Ce service est basé sur la solution réseau MPLS/VPN (Multi Protocol Label Switching / Virtual Private Network). La configuration évaluée est constituée des équipements minimaux pour permettre la création deux flux réseaux distincts et cloisonnés pour deux clients distincts.

3 La solution MPLS/VPN offre les caractéristiques de sécurité suivantes :

- cloisonnement des flux,
- contrôle d'accès aux routeurs du RAEI (Réseau d'Accès pour les Entreprises à Internet),
- intégrité de la configuration et des tables de routages des routeurs du RAEI.

4 La solution n'intègre pas la fonctionnalité de confidentialité des flux.

5 La gestion de nouveaux flux réseaux cloisonnés par rapport aux flux précédents pour des clients supplémentaires se fait uniquement par l'ajout de nouveaux PE (Provider Edge) ou d'interfaces supplémentaires sur les PE existants.

6 Le développeur de la cible d'évaluation est Equant :

- Equant,
  9, rue du Chêne Germain
  35512 Cesson Sévigné Cedex,
  France.

7 L'exploitant de la cible d'évaluation est France telecom transpac :

- Transpac SA,
  Tour du Maine Montparnasse,
  33, avenue du Maine - B13,
  75755 Paris Cedex 15,
  France.

8 L'évaluation a été menée conformément aux Critères Communs [CC] version 2.1 et à la méthodologie définie dans la Méthodologie d'Evaluation Commune [CEM] version 1.0.

9 L'évaluation de ce système atteint le niveau d'assurance EAL 1 augmenté des composants d'assurance ADV_HLD.1 (Conception de haut niveau) et AVA_VLA.2 (Analyse de vulnérabilité indépendante).

10 L'évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information d'AQL :

- Alliance Qualité Logiciel, Groupe Silicomp
  rue de la Châtaigneraie
  BP 127
  35513 Cesson Sévigné
  France.

1.2 Contexte de l'évaluation

11 L'évaluation de ce système s'est déroulée de mars 2001 à octobre 2001.

12 Les commanditaires de l'évaluation sont Equant et France telecom transpac.

Chapitre 2

Description de la cible d'évaluation

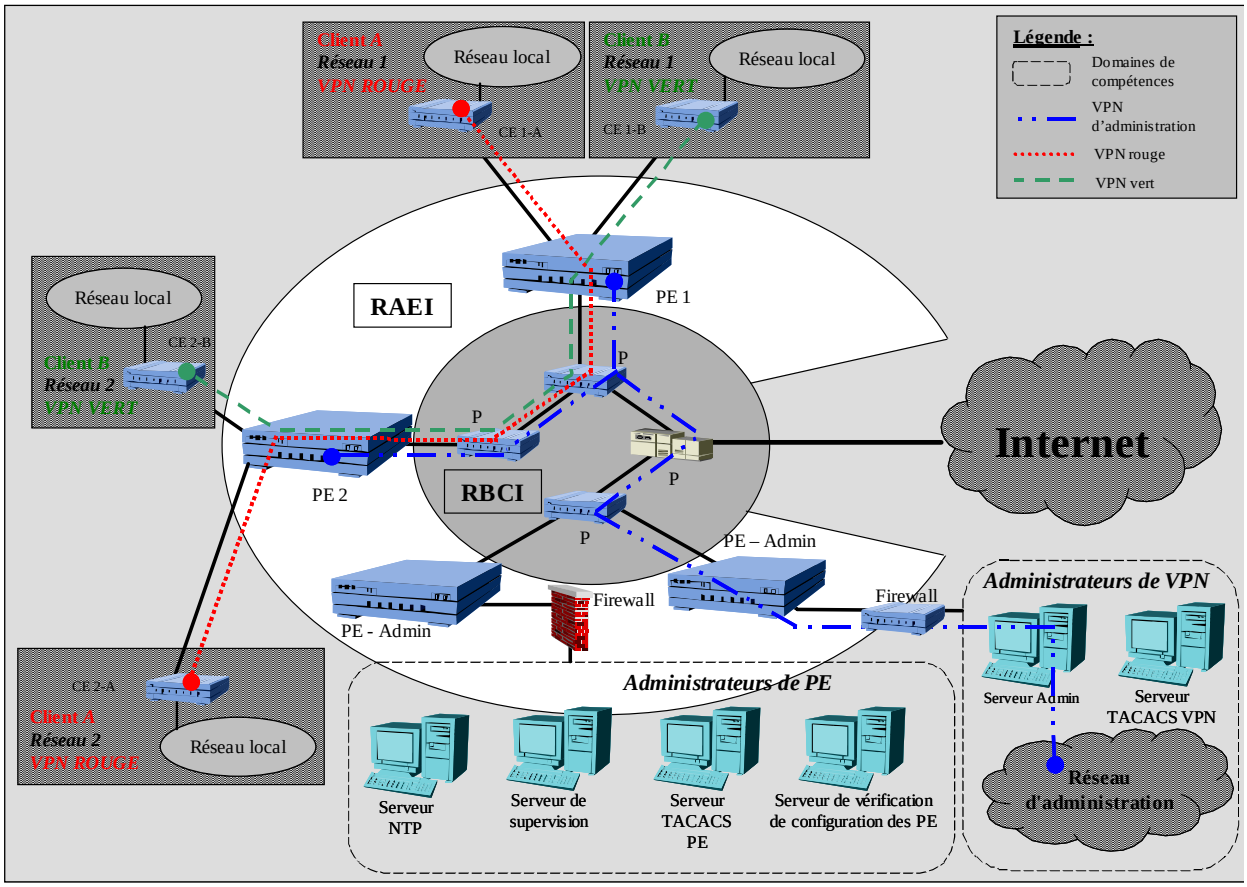
2.1 Identification

13 La cible d'évaluation est le «Cloisonnement des réseaux privés virtuels dans le cadre du service Equant IP VPN (version 1.0)».

2.2 Périmètre de la cible d'évaluation

14 La configuration évaluée est constituée de quatre routeurs PE appartenant au réseau RAEI ainsi que d'un outil propriétaire pour la création de VPN clients.

15 L'architecture du réseau VPN/MPLS est représentée dans le schéma ci-dessous :



- Les routeurs CE (Customer Edge), hors de la cible d'évaluation, permettent aux clients de se connecter au réseau via les PE qui sont hébergés par l'exploitant.

- Deux PE, au minimum, sont donc utilisés par les clients pour l'établissement d'un flux VPN/MPLS.

- Deux PE permettent d'accéder chacun via un Firewall aux réseaux d'administration.

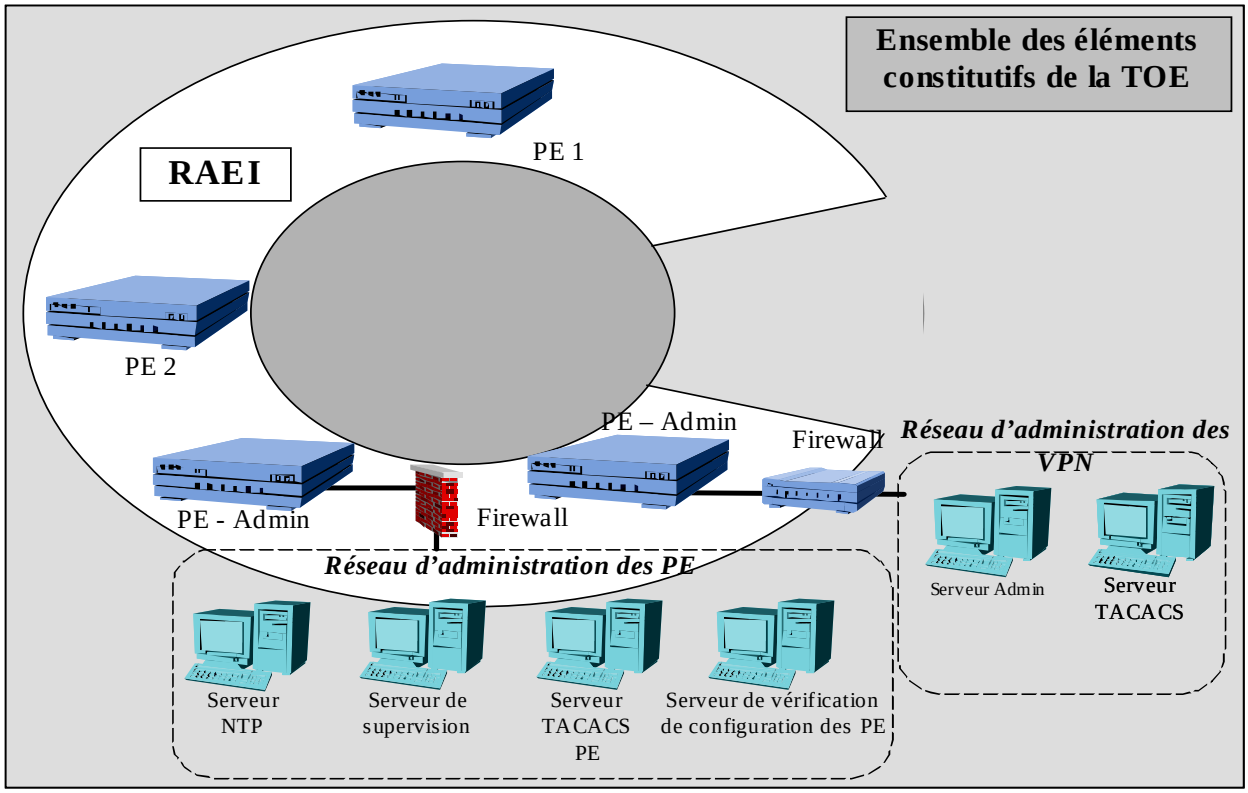
- Un premier réseau d'administration permet d'administrer les PE, il comporte :

  - un serveur TACACS pour l'authentification sur les routeurs PE,
  - un serveur de vérification de la configuration des routeurs PE,
  - un serveur de supervision qui permet le déclenchement du téléchargement de la configuration des routeurs PE,
  - un serveur NTP (Network Time Protocol) pour synchroniser les éléments de la cible d'évaluation.

- Un deuxième réseau d'administration gère l'authentification des administrateurs des flux MPLS/VPN, il comporte :

  - un serveur TACACS (Terminal Access Controller Access Control System) pour l'authentificaiton des administrateurs VPN,
  - le serveur de l'outil propriétaire d'administration des flux VPN.

16 La cible d'évaluation correspond à l'ensemble de l'offre MPLS/VPN qui est sous le contrôle de l'exploitant, c'est à dire les quatre PE et les deux réseaux d'administration tel que présenté dans le schéma suivant :



2.3 Fonctions de sécurité évaluées

17 Les fonctions de sécurité évaluées sont les suivantes :

- Contrôle d'accès des flux VPN par les PE,
- Contrôle d'accès des flux non VPN par les PE,
- Echange de VRF (VPN Routing and Forwarding table) entre les PE associés au même flux MPLS/VPN,
- Intégrité des VRF échangées,
- Identification et authentification des administrateurs des VPN,
- Identification et authentification des administrateurs sur les routeurs PE,
- Contrôle d'accès aux fonctions d'administration,
- Contrôle d'accès au réseau d'administration,
- Audit des actions d'administration,
- Vérification de l'intégrité de la configuration des PE,
- Administration des PE,
- Administration des VPN,
- Synchronisation des équipements.

2.4 Documentation disponible

18 La documentation disponible dans le cadre de l'exploitation de ce réseau concerne d'une part les utilisateurs de l'offre MPLS/VPN sur le réseau RAEI :

- « Réseau d'entreprise CLIENT, Plan Qualité Services Client » [GUIDE_USR].

19 D'autre part la documentation qui concerne l'exploitant lui-même et les procédures d'administration du système qui permettent la bonne mise en oeuvre des politiques de sécurité.

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

20 La cible d'évaluation a été évaluée selon le niveau d'assurance EAL1 des Critères Communs augmentés des composants ADV_HLD.1 et AVA_VLA.2.

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	Introduction de la ST (ASE_INT.1) Description de la TOE (ASE_DES.1) Environnement de sécurité (ASE_ENV.1) Objectifs de sécurité (ASE_OBJ.1) Annonce de conformité à un PP (ASE_PPC.1) Exigences de sécurité des TI (ASE_REQ.1) Exigences de sécurité des TI explicitement énoncées (ASE_SRE.1) Spécifications globales de la TOE (ASE_TSS.1)
Gestion de configuration	Numéros de version (ACM_CAP.1)
Livraison et exploitation	Procédures d'installation, de génération et de démarrage (ADO_IGS.1)
Développement	Spécifications fonctionnelles informelles (ADV_FSP.1) Démonstration de correspondance informelle (ADV_RCR.1) **Conception de haut niveau descriptive (ADV_HLD.1)**
Guides	Guide de l'administrateur (AGD_ADM.1) Guide de l'utilisateur (AGD_USR.1)
Tests	Tests indépendants - conformité (ATE_IND.1)
Estimation des vulnérabilités	**Analyse de vulnérabilités indépendante (AVA_VLA.2)**

21 Pour tous les composants d'assurance ci-dessus, un verdict «réussite» a été émis par l'évaluateur.

22 Les travaux d'évaluation menés sont décrits dans le Rapport Technique d'Evaluation [RTE].

23 Pour cette évaluation les aspects non techniques de la cible d'évaluation ont été audités.

3.1.1 Audits

24 L'évaluation a nécessité la réalisation d'audits organisationnels qui ont permis à l'évaluateur de vérifier l'application effective des mesures de sécurité.

25 Ces audits se sont déroulés sur différents sites d'administration du système :

- un site d'hébergement des routeurs PE permettant la connexion des clients,
- le site d'administration des comptes TACACS,
- le site d'administration des routeurs PE,
- un site d'administration des VPN.

26 Ces audits ont permis de vérifier le respect des objectifs de sécurité suivants :

- génération et distribution sûres des clés utilisées pour signer les VRF échangées entre les PE,
- génération et distribution sûres des mots de passe pour l'identification et l'authentification des administrateurs des VPN,
- analyse des journaux d'audits,
- exploitation et maintenance des équipements de la cible d'évaluation.

3.2 Tests fonctionnels et de pénétration

3.2.1 Tests développeurs

27 Le niveau d'évaluation visé ne nécessite pas de prendre en compte les tests fonctionnels effectués par l'exploitant.

3.2.2 Tests évaluateur

28 L'évaluateur a effectué des tests sur la cible d'évaluation afin de s'assurer du fonctionnement correct des fonctions de sécurité.

29 L'évaluateur a également mené une analyse de vulnérabilité, confirmée par des tests de pénétration, pour s'assurer qu'un attaquant disposant d'un potentiel d'attaque élémentaire (composant AVA_VLA.2) ne peut pas remettre en cause les objectifs de sécurité de la cible d'évaluation suivants :

- cloisonnement de flux entre un flux MPLS/VPN et un autre réseau,

- échange des VRF entre les PE supportant un même flux MPLS/VPN,

- intégrité des VRF échangées entre les PE,
- administration autorisée des PE et des VPN,
- intégrité de la configuration des PE,
- journalisation des événements d’administration des PE
- administration distante sûre des VPN.

Chapitre 4

Certification

4.1 Verdict

30 Ce présent rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL1 augmenté des composants d'assurance ADV_HLD.1 "Conception de haut niveau descriptive" et AVA_VLA.2 "Analyse de vulnérabilités indépendante" tel que décrit dans la partie 3 des Critères Communs [CC].

4.2 Recommandations

31 Afin de pouvoir propager la confiance dans le niveau de sécurité de ce service : dans le cadre d'une implémentation réelle de la solution pour le compte d'un client, il reste à la charge de l'exploitant d'apporter à son client la preuve qu'il a appliqué les mêmes techniques et méthodes de sécurité que celles validées dans le cadre de la présente certification. Néanmoins, seul un sous-ensemble représentatif du service Equant IP VPN sur le territoire français a été évalué et certifié.

4.3 Certification

32 La certification ne constitue pas en soi une recommandation de la solution. Elle ne garantit pas que la solution certifiée est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle que des vulnérabilités exploitables n'aient pas été découvertes ; probabilité d'autant plus faible que le niveau d'assurance est élevé.

33 Le certificat ne s'applique qu'à la configuration évaluée identifiée au chapitre 2 du présent rapport. La certification de toute version ultérieure de la solution, comme de toute implémentation spécifique pour un client nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	L'addition d'un ou de plusieurs composants d'assurance de la Partie 3 à un EAL ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation (TOE)	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Client	Utilisateur de l'offre VPN/MPLS.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Un paquet composé de composants d'assurance tirées de la Partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Une expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
Produit	Un ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.
Profil de protection	Un ensemble d'exigences de sécurité valables pour une catégorie de cible d'évaluation, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs.

Abréviations

CE	«Customer Edge», routeur utilisé pour connecter les réseaux clients au RAEI.
MPLS	«Multi Protocol Label Switching», un protocole de commutation de paquets. Ce protocole est expliqué à la section « 2.2.6 - Principe de fonctionnement d'un VPN / MPLS » de la cible de sécurité [ST].
P	«Provider», routeur constituant le cœur du RBCI.
PE	«Provider Edge», routeur utilisé pour connecter les routeurs CE au RBCI, et constituant le RAEI.
RAEI	«Réseau d'Accès pour les Entreprises à Internet», réseau du périmètre français d'Equant.
RBCI	«Réseau Backbone Connecté à Internet», réseau du périmètre Français d'Equant.
TACACS	«Terminal Access Controller Access Control System», un service de contrôle d'accès pour tous les équipements et serveurs réseau. Il gère les mécanismes d'authentification, d'autorisation et de gestion des droits.
VPN	«Virtual Private Network», réseau privé virtuel, un réseau privé réalisé sur un réseau public. Il repose sur une technologie de segmentation des flux qui n'est pas forcément une technologie de chiffrement / authentification.
VRF	«VPN Routing and Forwarding table», tables de routage échangées entre PE de manière dynamique permettant de créer les VPN.

Annexe B

Références

[CC] Critères communs de l'évaluation de la sécurité des technologies de l'information (Common Criteria) conforme à l'ISO/IEC 15408 :
- Part 1 : Introduction and general model, august 1999, version 2.1, réf : CCIMB-99-031 ;
- Part 2 : Security functional requirements, august 1999, version 2.1, réf : CCIMB-99-032 ;
- Part 3 : Security assurance requirements, august 1999, version 2.1, réf : CCIM-99-033.

[CEM] Méthodologie d'évaluation :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

[ST] - Cible de sécurité - Projet VIOLETTE, GlobalOne, version 1.7 du 19.10.2001, référence : SDS/DGP STB 001 *(document non public)*
- Security Target (public version) - Virtual Private Networks isolation in Equant IP VPN Service, France telecom transpac et Equant, version 1.0 du 15/11/2001, réf : DCQP/DR NT 002.

[RTE] Rapport Technique d'Evaluation, AQL, version 1.01 du 12.11.2001, référence : TPC232-RTE0-1.01*(document non public).*

[GUIDE_USR] Réseau d'entreprise « CLIENT », Plan Qualité Services Client, France Telecom, réf : Ixxx/AQ PQSC 001, version 01 du 01/10/1999. Guide personnalisé en fonction du client xxx.

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information (D.C.S.S.I.) à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Bureau certification
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

certification.dcssi@sgdn.pm.gouv.fr