Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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 2002/11

Service d'administration de VPN IPSec, Netcelo

(version 2.0)

Août 2002

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma Français

d'Évaluation et de Certification

de la Sécurité des Technologies de l'Information

CERTIFICAT 2002/11

Service d'administration de VPN IPSec, Netcelo

(version 2.0)

Développeur : Netcelo

Critères Communs

EAL1 Augmenté

(AVA_VLA.2)

Commanditaire : Netcelo

Centre d'évaluation : AQL - Groupe Silicomp

Le 12 Août 2002,

le Directeur central de la sécurité
des systèmes d'information
Henri Serres

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information publié au journal officiel de la République française le 19 avril 2002.

Ce système a été évalué 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 du système 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 du système 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 du système par l'organisme de certification ou par toute autre organisation qui le reconnaît ou l'utilise.

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 du système «Service d'administration de VPN IPSec, Netcelo».

2 Ce système offre un service de VPN administré, au travers de la mise en service, la configuration, et l'administration des VPN ainsi que la supervision des équipements VPN. La cible d'évaluation est contituée par un système (appelé système VNMS) implanté sur deux sites physiques, un site principal et un site de secours. Il contribue à l'intégrité et à la confidentialité d'échanges de données sur des réseaux VPN en utilisant le protocole IPSec et en assurant la télé-administration et la supervision des équipements VPN d'abonnés au service.

3 Le développeur de la cible d'évaluation est Netcelo :

Netcelo S.A.
18-20 rue Henri Barbusse
B.P. 2501
38035 Grenoble Cedex 2
France

4 L'évaluation a été menée conformément aux Critères Communs [CC] et à la méthodologie définie dans le manuel CEM [CEM].

5 Le niveau atteint par cette évaluation est le niveau d'assurance EAL 1 augmenté du composant :

AVA_VLA.2 "Analyse de vulnérabilité indépendante".

6 Le produit satisfait aux exigences de reconnaissance mutuelle internationale [MRA] et européenne [SOG-IS].

7 L'évaluation du système a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information d'AQL - Groupe Silicomp :

AQL - Groupe Silicomp
Rue de la chataîgneraie
B.P. 127
35513 Cesson-Sévigné Cedex
France

1.2 Contexte de l’évaluation

8 L’évaluation s’est déroulée de janvier 2002 à juin 2002.

9 Le commanditaire de l’évaluation est Netcelo :

Netcelo S.A.
18-20 rue Henri Barbusse
B.P. 2501
38035 Grenoble Cedex 2
France

Chapitre 2

Description de la cible d'évaluation

2.1 Périmètre de la cible d'évaluation

10 La cible d'évaluation est contituée par le système VNMS en exploitation, implanté sur deux sites physiques, un site principal et un site de secours. Ce système permet l'administration de VPN IPSec. Il est conforme au modèle de référence TMN [ST]

11 La partie technique de la cible d'évaluation, évaluée suivant les critères communs, est composée :

- du site principal du centre d'opérations,
- du site de secours du centre d'opérations,
- du système VNMS qui équipe ces sites.

12 Le système VNMS qui équipe ces deux sites est lui-même composé de :

- pare-feux,
- sous-systèmes BSS (Business System Support),
- sous-systèmes OSS (Operations System Support),
- sous-systèmes de gestion de données,
- serveurs de sauvegarde,
- un sous-système d'administration,
- un sous-système de service de certificat,
- routeurs.

13 La partie non technique de la cible d'évaluation, auditée, est composée :

- de l'équipe d'exploitation du centre d'opérations qui est composée du personnel Netcelo ayant les rôles d'administrateur privilégié et d'administrateur du système (cf [ST]) ;
- des bâtiments qui hébergent le site principal et le site de secours du centre d'opérations.

2.2 Fonctions de sécurité évaluées

14 Les fonctions de sécurité implémentées par la partie technique du système évalué sont :

- droit d'accès :
  - identification et authentification des utilisateurs et des administrateurs,
  - droits d'accès au service en fonction des rôles (administrateurs, gestionnaires, responsables de sites et abonnés),
  - étanchéité entre les données commerciales des utilisateurs,

- règles de filtrage pour entrer ou sortir du système vers Internet ;

- imputabilité et audit :
  - enregistrement des évènements de type service (sous-systèmes OSS et BSS) et de type système (système VNMS),
  - protection des fichiers d'audit,
  - outils d'analyse des fichiers d'audits,
  - production d'événements d'alarmes ;
- intégrité des données :
  - protection des transferts de données internes à l'intérieur du système,
  - sauvegarde globale et synchronisation des sites,
  - restauration de la configuration des machines,
  - prévention et détection des erreurs d'intégrité référentielles ;
- fiabilité de service :
  - duplication des données sur deux unités de stockage,
  - fonctionnement HA (High Availability) avec basculement automatique de machine ou de site ;
- sécurisation des échanges de données entre une console Web et la TOE et entre les wizards de configuration et la TOE ;
- sécurisation des commandes et des données entre un équipement VPN et la TOE.

2.3 Mesures de sécurité non techniques

15 Les mesures de sécurité qui ont été auditées dans le cadre de l'évaluation concernent les aspects suivants :

- contrôle d'accès physique aux sites,
- formation des administrateurs,
- astreintes à la demande du client,
- procédures de sauvegarde et synchronisation,
- procédures de restauration,
- procédures en cas d'indisponibilité du site principal,
- réplication des équipements "spare",
- gestion des mots de passe,
- gestion des audits et des alarmes,
- administration des fonctions de sécurité.

2.4 Documentation disponible

16 Les guides de l'administrateur permettent une utilisation sûre du système, ils ont été audités.

17 Les guides d'utilisation [GUIDE] concernent les utilisateurs du service, comme les gestionnaires ou les responsables de site [ST].

Chapitre 3

Résultats de l'évaluation

3.1 Exigences d'assurance

18 Le système a été évalué au niveau EAL 1 augmenté du composant AVA_VLA.2 :

Classes d'Assurance	Composants d'Assurance
Cible de sécurité	ASE : Evaluation de la cible de sécurité
Gestion de configuration	ACM_CAP.1 : Numéros de version
Livraison et exploitation	ADO_IGS.1 : Procédures d'installation, de génération et de démarrage
Développement	ADV_FSP.1 : Spécifications fonctionnelles informelles ADV_RCR.1 : Démonstration de correspondance informelle
Guides	AGD_ADM.1 : Guide de l'administrateur AGD_USR.1 : Guide de l'utilisateur
Tests	ATE_IND.1 : Tests indépendants - conformité
Analyse de vulnérabilité	AVA_VLA.2 : Analyse de vulnérabilité indépendante

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

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

21 Dans le cadre des travaux d'évaluation, un audit organisationnel a été réalisé sur les deux sites de Netcelo :

- le site de secours (aussi siège social de la société Netcelo)
- le site principal (local technique)

22 Cet audit a permis de s'assurer de l'application des mesures de sécurité, concernant les aspects de sécurité physique, les aspects organisationnels et les mesures de

sécurité liées au personnel, identifiées dans la cible de sécurité. Cet audit a aussi permis de vérifier l'existence de procédures et leur mise en application.

3.2 Tests fonctionnels et de pénétration

23 L'évaluateur a mené une analyse de vulnérabilités, confirmée par des tests de pénétration sur site, 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 :

- chaque gestionnaire et responsable de site est identifié de manière unique,
- seuls les administrateurs autorisés sont capables d'accéder aux fonctions de sécurité,
- protection de la confidentialité de l'information transférée sur un réseau à destination d'une console d'exploitation ou d'administration du service, d'un wizard de configuration ou d'un équipement VPN,
- étanchéité entre les données commerciales des opérateurs,
- intégrité des données des opérateurs,
- enregistrement (audit) des événements qui surviennent lors de l'utilisation des fonctions de sécurité,
- protection des traces d'audit,
- s'assurer qu'un équipement VPN émetteur d'une requête d'approvisionnement est bien autorisé à bénéficier de ce service,
- s'assurer qu'un équipement VPN est autorisé à demander un certificat,
- mise en place de mécanismes permettant de surveiller la disponibilité du système et de minimiser les effets de problèmes ou de défaillances matérielles ou logicielles qui se traduisent par des disfonctionnements, d'indisponibilité du service ou de fonctionnement illégal du service,
- être protégé des attaques opérées via Internet.

Chapitre 4

Certification

4.1 Verdict

24 Ce rapport certifie que la cible d'évaluation satisfait aux exigences du niveau EAL 1 augmenté du composant AVA_VLA.2, tels que décrits dans la partie 3 des Critères Communs [CC] :

- AVA_VLA.2 "Analyse de vulnérabilité indépendante".

4.2 Recommandations

25 Le système doit être exploité conformément aux procédures d'utilisation et d'administration prescrites dans la cible de sécurité [ST] et dans les guides [GUIDE].

4.3 Certification

26 Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information, publié au journal officiel de la République française le 19 avril 2002.

27 La certification ne constitue pas en soi une recommandation du système. Elle ne garantit pas que le système certifié 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.

4.4 Reconnaissance internationale

28 Afin de d'éviter les certifications multiples d'un même produit dans différents pays, il existe des accords de reconnaissance des certificats ITSEC et Critères Communs.

29 Ce certificat répond aux exigences des accords suivants :

4.4.1 SOG-IS

30 L'accord SOG-IS [SOG-IS] sur la reconnaissance des certificats ITSEC est applicable depuis mars 1998. Cet accord a été signé par l'Allemagne, l'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse. Cet accord a ensuite été étendu aux certificats Critères Communs pour tous les niveaux d'évaluation (EAL1 - EAL7).

4.4.2 CC MRA

31 Un arrangement (Common Criteria Arrangement) [MRA] sur la reconnaissance des certificats basés sur les évaluations jusqu'au niveau EAL4 a été signé en mai 2000. Cet arrangement a été signé par l'Allemagne, le Canada, l'Espagne, les Etats-Unis, la Finlande, la France, la Grèce, Israël (en novembre 2000), l'Italie, la Norvège, la Nouvelle-Zélande, les Pays-Bas, le Royaume-Uni et la Suède (juin 2002).

Annexe A

Glossaire

Assurance	Fondement de la confiance dans le fait qu'une entité satisfait à ses objectifs de sécurité.
Augmentation	Addition d'un ou de plusieurs composants d'assurance de la partie 3 des CC à une échelle prédéfinie d'assurance ou à un paquet d'assurance.
Biens	Informations ou ressources à protéger par la cible d'évaluation ou par son environnement.
BSS	Business Support System; Sous-système fonctionnel qui gère les relations avec la clientèle.
Cible d'évaluation	Produit ou système et documentation associée pour (administrateur et utilisateur) qui est l'objet d'une évaluation.
Cible de sécurité	Ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'un PP ou d'une cible d'évaluation par rapport à des critères définis.
Niveau d'assurance de l'évaluation (EAL)	Paquet de composants d'assurance extraits de la partie 3 qui représente un niveau de l'échelle d'assurance prédéfinie des CC.
Objectif de sécurité	Expression de l'intention de contrer des menaces identifiées ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses.
OSS	Operations Support System; Sous-système fonctionnel qui gère les opérations avec les équipements VPN.
Produit	Ensemble de logiciels, microprogrammes ou matériels qui offre des fonctionnalités conçues pour être utilisées ou incorporées au sein d'une multiplicité de systèmes.

Système	Une installation TI spécifique, avec un objectif et un environnement opérationnel particuliers.
TMN	Modèle d'administration de réseau de l'ITU-T, qui formalise l'administration d'un réseau en sous-systèmes OSS et BSS.
VNMS	Virtual Network Management System; Système qui équipe le centre d'opération de Netcelo.
VPN	Virtual Private Network ou Réseau Privé Virtuel.

Annexe B

Références

[CC] Critères Communs pour l'évaluation de la sécurité des technologies de l'information :
- 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 : CCIMB-99-033.

[CEM] Méthodologie commune pour l'évaluation de la sécurité des technologies de l'information :
- Part 2 : Evaluation Methodology, august 1999, version 1.0, réf : CEM-99/045.

[ST] Cible de sécurité du système VNMS, Netcelo S.A., version 2.0.5, avril 2002 (document non public), référence DOSS/ARCH/30
Cible publique de sécurité d'un service d'admnistration de VPN IPSec, Netcelo S.A., référence DOSS/ARCH/40

[GUIDE] Guide des gestionnaires du service VPN administré v2.0.4, référence DOSS/INTE/29
Guide du Netcelo Set-Up Wizard Version V2.0, référence DOSS/INTE/37

[RTE] Evaluation Technical Report STATUS, AQL, version 1.01, juin 2002, réf: NTC001-RTE01-1.01. (document non public)

[MRA] ARRANGEMENT on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mai 2000.

[SOG-IS] «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

Ce rapport de certification est disponible sur le site internet de la Direction centrale de la sécurité des systèmes d'information 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