Cible publique de sécurité d'un service d'administration de VPN IPsec

Netcelo, SA
18-20 rue Henri Barbusse
B.P.2501
38035 GRENOBLE CEDEX 2

Adresse de la société:
18-20 rue Henri Barbusse
BP 2501
38035 Grenoble Cedex 2
France

Téléphone : +33 (0)4 38 49 83 60
Fax : +33 (0)4 38 49 83 61
E-mail : netcelo@netcelo.com

Au sujet de ce document

Ce document : *cible publique de sécurité d'un service d'administration de VPN IPsec* rendu par un système d'administration de réseaux virtuels (Virtual Network Management System) a comme but de servir de base à une *cible d'évaluation* (TOE) en l'occurrence le système VNMS version **V2.0** pour vérifier qu'il est conforme à un niveau *d'assurance de sécurité de base*.
Pour la structure et le contenu de ce document, les directives des *Critères Communs* (CC) sont appliquées.
Les termes : *cible d'évaluation*, *cible de sécurité*, *Critères Communs* , *évaluation* et niveau *d'assurance de sécurité de base* sont définis dans le glossaire ci-après.

Documents applicables

[CCPART1]	Critères communs pour l'évaluation de sécurité des techniques de l'information Partie 1 – Introduction et modèle général - Version 2.1	CCIMB-99-031
[CCPART2]	Critères communs pour l'évaluation de sécurité des techniques de l'information Partie 2 – Besoins fonctionnels de sécurité - Version 2.1	CCIMB-99-032
[CCPART3]	Critères communs pour l'évaluation de sécurité des techniques de l'information Partie 3 – Exigences d'assurance de sécurité - Version 2.1	CCIMB-99-033

Tableau 1 : Documents applicables

Documents de référence

[15446]	Guide for the production of protection profiles and security targets	ISO/IEC PDTR 15446
[15408]	Evaluation Criteria for IT Security	ISO/IEC 15408
[EBIOS]	Expression des Besoins et Identification des objectifs de Sécurité (EBIOS)	EBIOS
[ITSEC]	Critères d'évaluation de la sécurité des systèmes informatiques	ITSEC
[SPECARC]	Spécifications d'architecture du système VNMS	DOSS/ARCH/23
[SPECFON]	Spécifications fonctionnelles du système VNMS	DOSS/ARCH/22
[GUIDGES]	Guide du gestionnaire	DOSS/INTE/29
[GUIDICA]	Guide d'installation et de configuration d'appareil VPN	DOSS/INTE/37
[GUIDABO]	Guide de l'abonné	DOSS/INTE/27
[GUIDESY]	Guide d'exploitation du système	DOSS/INTE/44
[GUIDESE]	Guide d'exploitation du service	DOSS/INTE/30
[PROCE]	Procédures d'exploitation du système VNMS	DOSS/INTE/121
[GUIDC]	Guide d'installation, de configuration et de mise en service du système VNMS	DOSS/INTE/108
[TCSEC]	Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD	TCSEC
[TMN]	Les documents ITU M-series contiennent les principaux documents relatifs au standard TMN de l'ITU.	ITU M-series

Tableau 2: Documents de référence

Définitions

Abréviations

BSS	Business System Support
CA	Certificate Authority
CC	Critères Communs
CPE	Customer Premises Equipment; Equipement VPN sur un site utilisateur par opposition à un équipement VPN sur un site opérateur (Provider Provided Equipment - PPE)
EAL	Evaluation Assurance Level – Niveau d'assurance de l'évaluation
EAL1	Niveau d'assurance d'évaluation de base
EAL1+	Niveau d'assurance d'évaluation de base augmenté du composant AVA_VLA.2
HA	High Availability; Haute disponibilité.
IKE	Internet Key Exchange.
IPSEC	IP SECurity.
IT	Information Technology – Technique de l'information (TI)
ITU	International Telecommunications Union
NTP	Network Time Protocol
OSS	Operations System Support
PKI	Public Key Infrastructure; infrastructure à clés publiques.
SAR	Security Assurance Requirement; Exigences d'assurance de sécurité
SES	Serveurs qui assurent les services BSS du système VNMS
SFR	Security Functional requirement; exigence fonctionnelle de sécurité
SMS	Serveurs qui assurent le service OSS du système VNMS
SSH	Secure SHell
SPOF	Single Point Of Failure
ST	Security Target- Cible de sécurité
TI	Technique de l'Information (sigle IT Francisé).
TMN	Telecommunications Management Network;
TOE	Target of Evaluation – Cible d 'évaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VNMS	Virtual Network Management System – Système qui rend le service VPN administré
WebUI	Web User Interface
X.509	Recommandation qui définit le format de certificats. La version X.509 V3 est supportée.

Tableau 3 : Abréviations

Glossaire

Abonné	Possesseur d'un ou de plusieurs sites qui a souscrit un abonnement auprès d'un opérateur pour s'abonner au service VPN administré.
Administrateur	Rôle affecté à du personnel du centre d'opérations Netcelo pour avoir les droits pour superviser et administrer le système VNMS et assister les utilisateurs finals ou les opérateurs (service d'assistance).
Administrateur privilégié du service	Administrateur qui dispose de droits supplémentaires pour créer des environnements de clients du service VPN administré, c'est à dire une base de données client et un rôle de gestionnaire privilégié.
Administrateur privilégié du système	Rôle affecté à un administrateur qui donne les droits maximum (root) pour intervenir sur les machine set équipements de réseau du système VNMS.
Approvisionnement	Voir Provisioning
Appareil VPN	Routeur ou passerelle qui dispose d'IPSEC
BSS	Business System Support; Sous système fonctionnel du centre d'opérations qui gère les relations avec la clientèle.
Centre d'opérations	Système VNMS connecté à Internet qui rend le service VPN administré et implanté sur un site situé chez un hébergeur. Pour des raisons de disponibilité en cas de désastre, le système est dupliqué sur un site de secours distant du site principal par quelques kilomètres. Les deux sites sont reliés par une liaison privée à haut débit. Le centre d'opération rend les services BSS (Business System Support) et OSS (Operations System Support) conformément au modèle TMN (Telecommunications Management Network).
Certificat	Fichier conforme aux recommandations X.509 V3 qui est émis par une autorité de certification. Un certificat associe une clé publique à une entité (personne humaine ou appareil). Un des modes du protocole IKE authentifie les équipements VPN à l'aide de certificats.

Cible d'évaluation	La cible d'évaluation (TOE) est la partie du système soumise à l'évaluation.
Cible de sécurité(ST)	Une cible de sécurité (ST) constitue la base de l'accord entre toutes les parties (développeurs, utilisateurs, évaluateurs et autorités d'évaluation) sur les services de sécurité offerts par une cible d'évaluation (TOE), de même que sur l'ampleur de l'évaluation.
Client VPN	Logiciel qui équipe un poste de travail pour lui apporter les fonctions d'un équipement VPN IPSEC.
Critères communs	Les critères communs (CC) définissent un ensemble d'exigences, dont la validité est reconnue, et qui peuvent être utilisés pour établir les exigences de sécurité de systèmes comme le système VNMS (Virtual Network Management System). Ils définissent aussi la structure de profils de protection (PP) qui permettent aux utilisateurs et aux développeurs potentiels de créer des ensembles d'exigences de sécurité pour répondre à leurs besoins. Les interprétations du CCIMB et notamment l'interprétation RI-008 sont également utilisées. La cible d'évaluation (TOE) est la partie du système soumise à l'évaluation. La cible de sécurité (ST) qui sera utilisée comme base de l'évaluation, contient la description des menaces et des objectifs de sécurité, les spécifications globales des fonctions de sécurité et les mesures d'assurance de la TOE. La version 2.1 des CC qui est appliquée pour la définition de la cible de sécurité du système VNMS est entièrement conforme à la norme internationale des critères communs ISO 15408.
Equipement VPN	Appareil ou client logiciel VPN qui équipe un site.
Evaluation	Une évaluation selon les CC est une évaluation des propriétés de sécurité du système (c'est à dire l'évaluation d'une TOE) faite par rapport aux critères de sécurité définis dans les Critères communs. L'évaluation d'une cible de sécurité (ST) est menée selon les critères d'évaluation des ST (partie 3 des Critères Communs). L'évaluation d'une TOE est menée selon les critères d'évaluation énoncés dans la partie 3 des Critères Communs, avec comme base une ST évaluée.
Gestionnaire	Rôle affecté à du personnel de l'opérateur en charge pour opérer une console d'exploitation du service VPN administré
Gestionnaire privilégié	Gestionnaire avec droits supplémentaires lui permettant de gérer d'autres gestionnaires.
IKE	Application qui gère la négociation d'associations de sécurité permettant la mise en place sur un équipement VPN des paramètres nécessaires à l'utilisation d'IPSEC face à un autre équipement.
IPSEC	Protocole de sécurité de niveau 3 qui sécurise des paquets IP et qui grâce à sa technique d'encapsulation de paquets qui permet de réaliser des tunnels, peut être également utilisé comme protocole VPN de niveau 3.
Niveau d'assurance de sécurité de base	Les critères communs proposent sept niveaux d'assurance (EAL1 à EAL7) constitués de composants issus des familles d'assurance. Le niveau d'assurance de sécurité de base est EAL1. Le niveau EAL1 est applicable quand une certaine confiance est exigée pour un fonctionnement correct, et que les menaces contre la sécurité ne sont pas considérées comme sérieuses. Ce niveau présente un intérêt quand une assurance, obtenue de façon indépendante, est nécessaire pour étayer l'affirmation selon laquelle un soin approprié a été exercé pour protéger les informations personnelles ou similaires. Le niveau EAL1 fournit une évaluation de la TOE , dans ses conditions d'utilisation nominale , et nécessite des tests, effectués de manière indépendante, basés sur les spécifications fonctionnelles, de même qu'une évaluation des guides, fournis avec le produit. L'évaluation à ce niveau doit pouvoir permettre de conclure que la TOE fonctionne tel que l'indique la documentation qui l'accompagne, et qu'elle offre une protection utile contre les menaces spécifiées. Le niveau EAL1+ est augmenté par le composant AVA_VLA.2
NSC	New Simple Cluster ; Service Linux qui permet de réaliser des grappes de deux machines Linux HA, l'une étant en surveillance de l'autre. NSC est appliqué aux firewalls du système VNMS.
NTP	Serveur de temps qui sert à l'horodatage des machines du système VNMS, des équipements VPN et des certificats.
Opérateur	Exploitant du service VPN administré. Un opérateur commercialise le service VPN administré auprès d' abonnés qui possèdent un ou plusieurs sites.
Opérateur système	Personnel du centre d'exploitation en charge de la supervision , des opérations de sauvegarde et d'exploitation des fichiers de log.
OSS	Operations Support Systems; Sous système fonctionnel qui gère les opérations avec des équipements VPN.
Politique de sécurité de la TOE (TSP)	La TSP définit les règles qui gouvernent l'accès à ses ressources et par conséquent toutes les informations et tous les services contrôlés par la TOE.
Politique de sécurité organisationnelle.	Une ou plusieurs règles de sécurité, de procédures, de pratiques ou de recommandations imposées par une organisation pour ses opérations.
Provisioning	Approvisionnement d'un équipement VPN. Opérations réalisées sur un site utilisateur qui dispose d'un équipement VPN afin d'installer, configurer et mettre en service cet équipement. Le provisioning est réalisé par un wizard de configuration qui interagit avec l'équipement VPN et le système VNMS.
Responsable de site	Rôle qui permet à un personnel de l'opérateur ou d'un abonné d'utiliser le wizard de configuration d'un équipement VPN permettant d'approvisionner cet équipement lors de sa première utilisation sur un site, et d'intervenir sur l'équipement VPN à la demande du support Netcelo.
Rôle	Ensemble de règles pré-définies qui établissent les interactions autorisées entre un utilisateur et la TOE
SES	Sous système technique du système VNMS qui rend des services fonctionnels de type BSS
Site	Machine ou ensemble de machines en réseau qui disposent d'un équipement VPN.

SMS	Sous système technique du système VNMS du centre d'opérations qui supporte des fonctions de type OSS.
SPOF	Single Point Of Failure. Point unique occasionnant une indisponibilité de traitement ou de communication.
TMN	Modèle d'administration de réseaux de l'ITU-T qui formalise l'administration d'un réseau en sous système fonctionnels BSS et OSS.
VNMS	Virtual Network Management System; Système qui équipe le centre d'opérations Netcelo et qui rend les services BSS et OSS.
VPN	Réseau virtuel privé dont les nœuds sont les équipements VPN de sites assignés au VPN. Un VPN peut être en étoile ou maillé. Dans le cas d'un VPN en étoile, un site joue le rôle de centre d'étoile les autres sont des sites d'extrémité de l'étoile. Les communications VPN ne peuvent s'effectuer qu'entre un site extrémité d'étoile et le site centre d'étoile. Dans le cas d'un VPN maillé, les communications VPN entre les sites sont de type Peer-to-Peer (P2P) . Chaque site peut communiquer avec un autre site. Internet est utilisé comme réseau de transport d'un VPN et se comporte de manière transparente vis à vis des machines des sites qui sont mise en relation. En particulier les espaces d'adressage privés des sites ne doivent pas se recouvrir.
Wizard de configuration	Logiciel qui tourne sur un PC. Le wizard de configuration est utilisé pour réaliser les opérations d'approvisionnement (*provisioning*) d'un équipement VPN. Le wizard de configuration est connecté localement et par réseau local à un équipement VPN de type routeur ou il est intégré à l'équipement VPN dans le cas d'un logiciel client VPN. Le *wizard* de configuration peut être opéré par un utilisateur qui a le rôle de responsable de site.

Tableau 4: Glossaire

Plan du document

Le plan du document est conforme à *l'annexe C Specifications of Security Targets* de la partie 1 des Critères Communs [CCPART1]. Il est résumé ci-après.

Introduction
Identification de la ST et de la TOE concernée, une vue d'ensemble de la ST et toute annonce de conformité aux critères communs. La vue d'ensemble s'adresse aux utilisateurs potentiels de la TOE et peut être incluse dans la liste des produits évalués. L'annonce de la conformité de la TOE aux CC, et peut inclure des PP ou un EAL. La cotation de résistance minimum des fonctions est indiquée le cas échéant.

Description de la cible d'évaluation (TOE)
Cette rubrique fournit le contexte d'application de la TOE. Elle aide à comprendre les exigences de sécurité de la TOE et décrit son type, l'utilisation envisagée et ses caractéristiques de sécurité générales.

Environnement de sécurité de la TOE
Cette rubrique indique les menaces, les politiques de sécurité organisationnelles auxquelles la TOE doit satisfaire et les hypothèses concernant l'environnement dans lequel la TOE sera utilisée.

Objectifs de sécurité
Les objectifs de sécurité pour la TOE et pour son environnement visent à contrer les menaces identifiées et à se conformer aux politiques de sécurité organisationnelles et aux hypothèses faites sur l'environnement.

Exigences de sécurité TI
Dans cette rubrique sont spécifiées les exigences de sécurité de la TOE comprenant les exigences fonctionnelles et d'assurance. Le cas échéant, les exigences de sécurité pour l'environnement TI de la TOE sont spécifiées ainsi que la résistance minimum annoncée des fonctions. Il n'est pas nécessaire de répéter dans la ST les exigences qui renvoient à un PP.

Spécifications résumées de la TOE
Elles offrent une définition générale des fonctions de sécurité qui sont censées satisfaire aux exigences fonctionnelles, et des mesures d'assurance prises pour répondre aux exigences d'assurance. La robustesse de chaque fonction devrait être indiquée le cas échéant.

Annonce de la conformité à un PP (Sans objet pour la cible de sécurité de la TOE)
Dans le cas ou la ST annonce que la TOE est conforme aux exigences contenues dans un ou plusieurs PP, cette rubrique apporte des explications, justifications et informations complémentaires (référence du PP, adaptations ou additions éventuelles faites au PP).

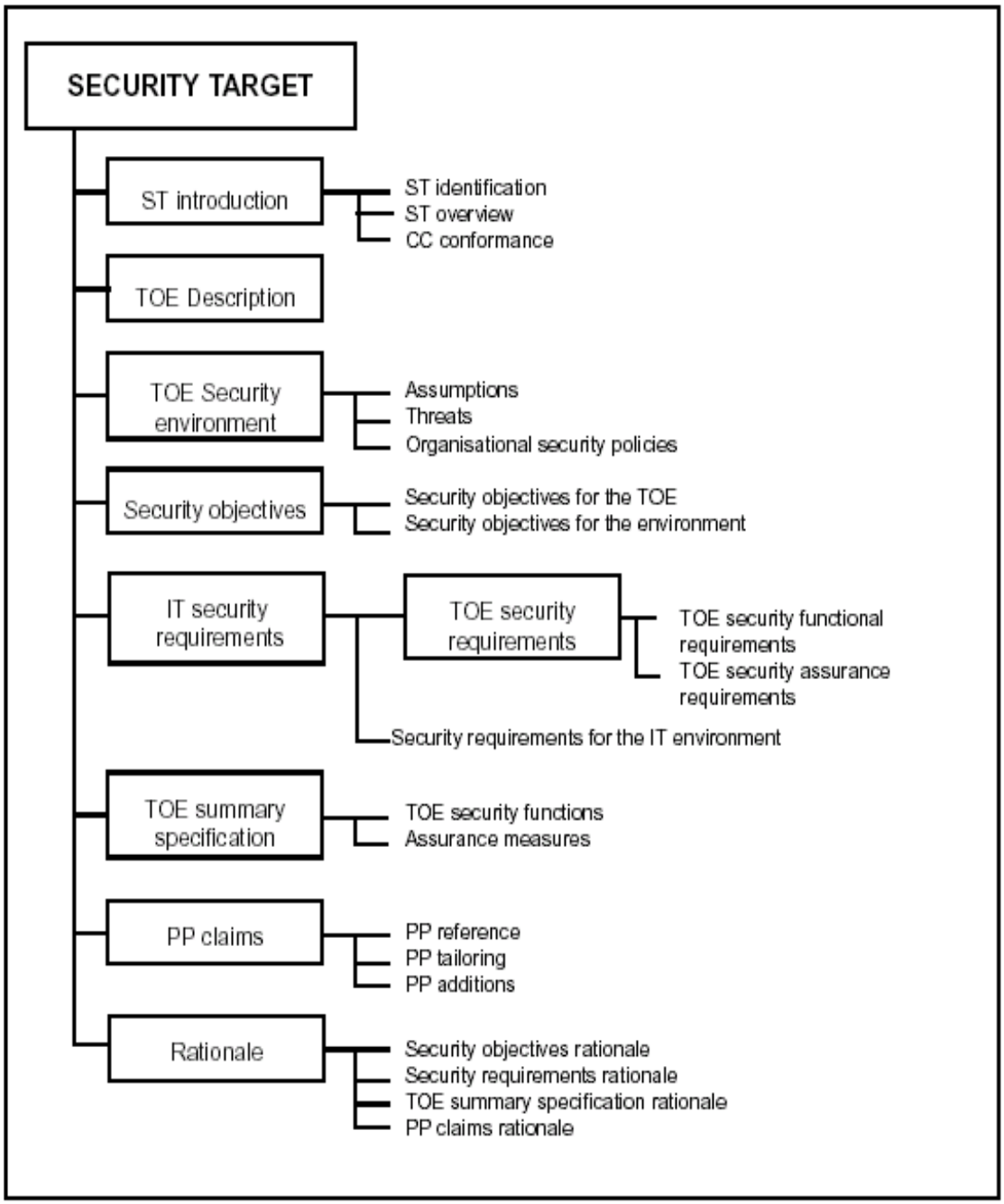

Tableau 5 : Contenu d'un document cible de sécurité

Table des matières

Figures

Tableaux

Chapitre 1

1 Introduction

1.1 Identification de la cible de sécurité

Le type de l'objet évalué est un système exploité de production de VPN appelé VNMS V2.0 (Virtual Network Management System) développé par Netcelo. Ce système exploité rend un service de VPN administré. L'objet évalué comprend également une partie environnementale non-TI (locaux, équipe d'exploitation).
Le sigle *système* identifie la partie TI de la TOE dans ce document.

1.2 But de l'évaluation

On va réaliser une évaluation du *système* pour certifier la capacité à produire des VPN administrés de façon sécurisée et récurrente pour un type d'équipement VPN donné: un routeur 6200 de la société 6wind.

1.3 Choix et justification du niveau d'assurance

Le niveau d'assurance de sécurité de base retenu dans le cadre de l'évaluation du système VNMS est EAL1. Le niveau EAL1 est applicable quand une certaine confiance est exigée pour un fonctionnement correct, et que les menaces contre la sécurité ne sont pas considérées comme sérieuses. Ce niveau présente un intérêt quand une assurance, obtenue de façon indépendante, est nécessaire pour étayer l'affirmation selon laquelle un soin approprié a été exercé pour protéger les informations personnelles ou similaires.
Le système VNMS (la TOE), agit pour mettre en service, configurer , administrer et superviser des équipements VPN qui vont inter opérer avec le protocole IPSEC dans des environnements de VPN. Quand des équipements VPN s'échangent des données, le système VNMS est externe à ces échanges (se reporter à la figure 6 paragraphe 2.2.5) car ce sont les équipements VPN qui, grâce au protocole IPSEC protègent les échanges de données des dangers qui les menacent lors de leur passage sur un réseau non sûr comme Internet. On peut ainsi considérer que les menaces contre la sécurité du système VNMS ne sont pas aussi sérieuses que les menaces contre la sécurité des données transmises par les équipements VPN.

1.4 Généralités sur la cible de sécurité

La société Netcelo a développé le système VNMS pour commercialiser un service de VPN IP administré.
Dans le cadre de l'évaluation, la société Netcelo joue le rôle de développeur, la société AQL joue le rôle d'évaluateur et la DCSSI est l'organisme de certification.

1.5 Conformité aux critères communs

Ce document est conforme à la partie 1 des Critères Communs [CCPART1], à la partie 2 des critères commune [CCPART2] et à la partie 3 augmentée des critères communs [CCPART3].
Ce document décrit les exigences de sécurité composants du niveau d'assurance de base EAL1+ (EAL1 augmenté du composant AVA_VLA.2).

Chapitre 2

2 Description de la cible d'évaluation

2.1 Introduction

La cible d'évaluation (TOE) est constituée par un *système* (le système VNMS) implanté sur deux sites physiques, un site principal et un site de secours situé à quelques kilomètres. Le site de secours est interconnecté au site principal par une liaison privée à haut débit (10 Mbps).
Le *système* est exploité. Un service d'assistance par numéro d'appel téléphonique et messagerie électronique est assuré dans des périodes (plages horaires et jours) définies contractuellement avec les clients.
La finalité du *système* est de contribuer indirectement à l'intégrité et à la confidentialité d'échanges de données sur des réseaux VPN Internet en assurant la télé administration et la supervision d'équipements VPN d'abonnés au service VPN pour qu'ils fonctionnent correctement.
Le *système* offre deux types d'interface utilisateur sous la forme :

- d'interfaces graphiques WebUI (Web User Interface) disponibles sur des consoles Web utilisées par des gestionnaires d' opérateurs et les abonnés,
- de *wizards* de configuration. Un *wizard* de configuration est utilisé par un responsable de site qui installe, configure et met en service l' équipement VPN d'un site lors de la phase d'approvisionnement.

2.2 Description du système (la TOE)

2.2.1 Le service VPN administré

Le service VPN administré est rendu par le *système* VNMS (Virtual Network Management System) d'un centre d'opérations implanté deux sites physiques (site principal et site de secours) distants de quelques kilomètres et interconnectés par une liaison privée à haut débit.
Le *système* est conforme au modèle de référence TMN et comprend deux sous systèmes fonctionnels : le BSS (Business Support System) et l'OSS (Operations Support System) . Les sous systèmes techniques qui rendent les services des sous systèmes fonctionnels BSS et OSS son appelés SES (Système d'Exploitation du Service) et SMS (Système de Mise en œuvre du Service).
Le *système* est une plate-forme située dans un centre d'opérations. C'est un système de classe opérateur sécurisé. Ce *système* peut supporter un nombre très important de sites d'abonnés. Les services rendus par le *système* sont :

- des services BSS de gestion des abonnés, des abonnements, des ressources (sites), des VPN et fournit des éléments de facturation.
- des services OSS de sécurité, de télé-administration, de supervision et d'audit d'équipements VPN,
- des services d'administration et de supervision du système,
- un service d'assistance par numéro d'appel téléphonique et messagerie électronique est assuré dans des périodes (plages horaires et jours) définies contractuellement pour assurer un support aux opérateurs et aux utilisateurs finals .

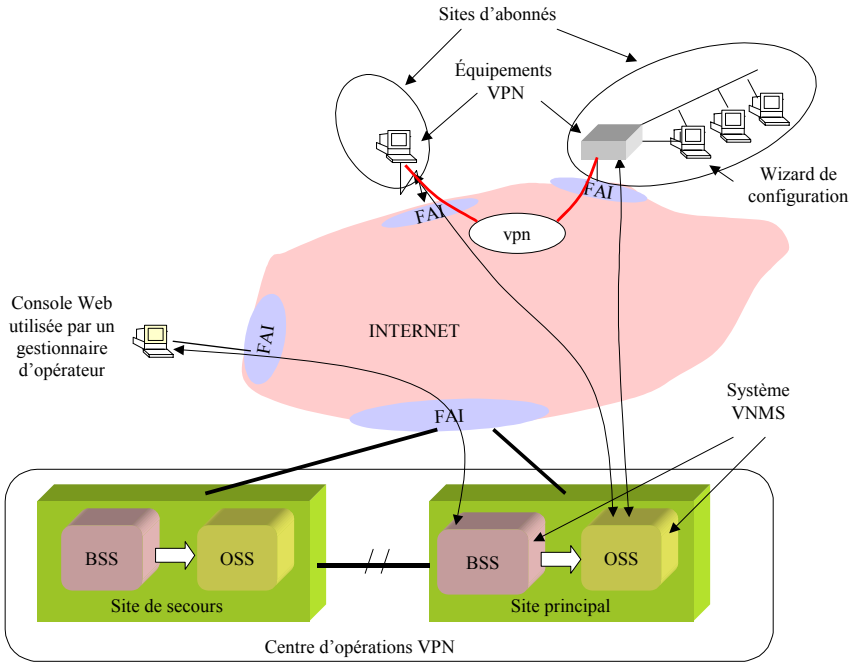

Figure 1: Centre d'opérations de réseaux virtuels

2.2.2 Les intervenants

Des rôles sont affectés aux intervenants.

Ces rôles sont décrits dans le tableau suivant avec un résumé des droits associés.
On distingue les rôles pour l'administration du système et les rôles pour l'administration du service.
Les rôles sont associés à des identifiants et des mots de passe.
Dans le cas des rôles administrateurs système, les identifiants (login) et les mots de passe sont créés par l'administrateur privilégié.
Dans le cas des rôles qui concernent l'administration du service, les identifiants et les mots de passe sont créés par le système selon l'arborescence qui est décrite dans le schéma ci-dessous.

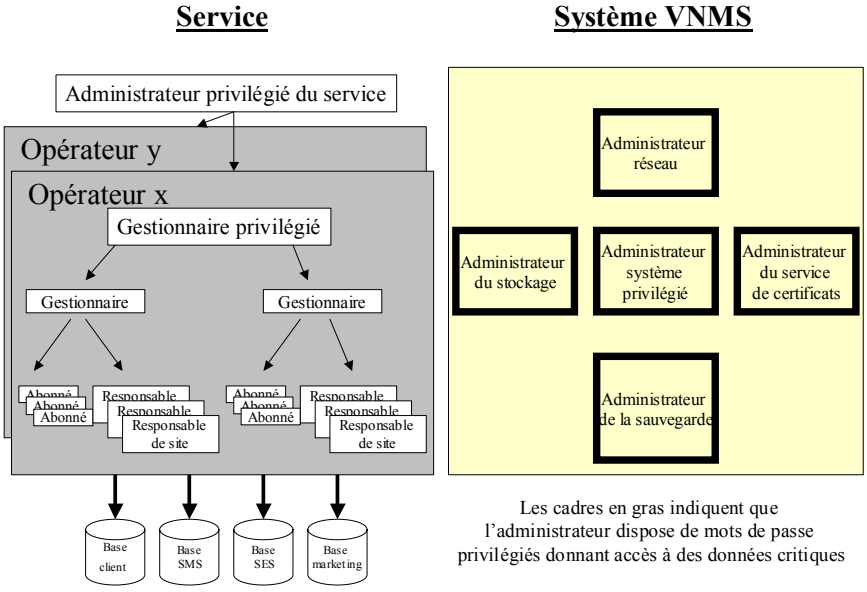

Figure 2: Schéma des rôles d'administration du système et du service

Rôle	Droits	Site concerné
Administrateur système privilégié	Droits maximum pour accéder les machines du système, les équipements de réseau et les données. Peut créer d'autres administrateurs.	Sites du centre d'opération
Administrateurs système	Droits pour administrer, superviser les services système, les machines et les réseaux du système VNMS. Il y a différents types d'administrateurs qui sont spécialisés pour des domaines d'administration bien définis : - administrateur réseau, - administrateur du stockage, - administrateur du service de certificats - administrateur de la sauvegarde.	
Administrateur privilégié du service	Droits pour administrer les bases de opérateurs et les opérateurs (exemple création de gestionnaires privilégiés)	Opérateurs, sites et VPN d'abonnés
Gestionnaire privilégié	Personnel d'un opérateur exploitant du service VPN administré et qui dispose des droits lui permettant de créer d'autres gestionnaires	Sites et VPN d'abonnés
Gestionnaire	Personnel d'un opérateur exploitant du service VPN administré..	Sites et VPN d'abonnés
Responsable de site	Personnel d'un abonné qui utilise le *wizard* de configuration d'un site d'abonné	Site d'abonné
Abonné	Souscripteur auprès d'un opérateur à un abonnement au service VPN administré. L'abonnement i concerne un ou plusieurs sites.	Site(s) de l'abonné

Tableau 6 : Intervenants

2.2.3 Le système VNMS

Le *système* est implanté dans un centre d'opérations réparti sur deux sites physiques: un site principal et un site de secours.
Le site principal et le site de secours sont distants de plusieurs kilomètres et reliés par une liaison de réseau privé à haut débit.

2.2.3.1 Système du site principal

Le *système* comprend plusieurs sous-systèmes :

- Un sous-système d'accès sécurisé à Internet, composé de garde-barrières.
- Deux sous systèmes de communications internes qui relient respectivement les machines de traitement au système d'accès sécurisé à Internet et les machines de données aux machines de traitement .
- Un sous système de communication pour accéder une liaison privée longue distance reliée à l'autre site.
- Des sous- systèmes de traitement applicatifs pour :
  - Les relations commerciales (BSS) avec les exploitants du service : les opérateurs,
  - Les opérations (OSS) avec les équipements VPN,
- Un sous-système de gestion des données,
- Un sous système d'administration,
- Un sous–système de service de certificats (PKI).

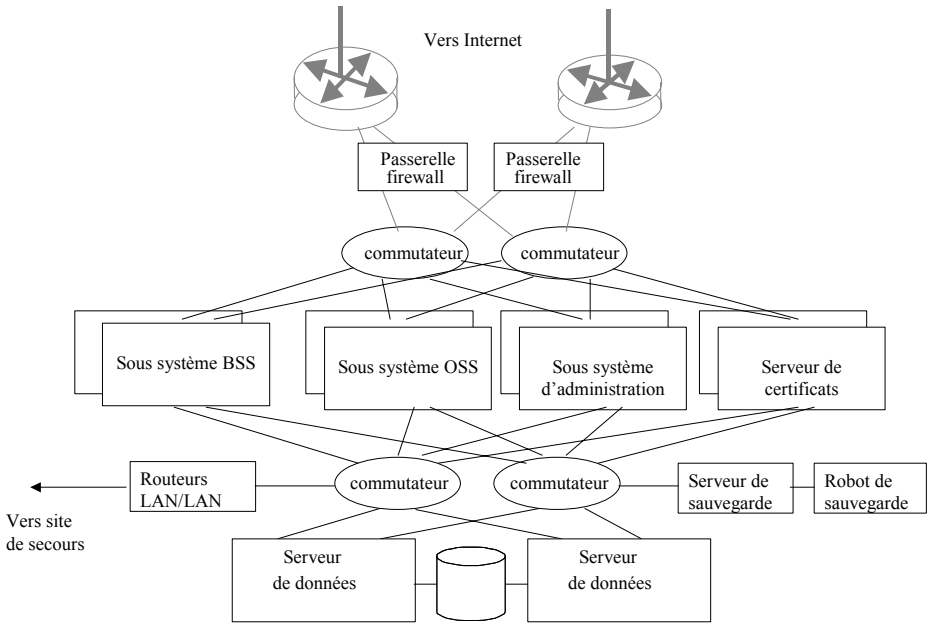

Figure 3: Système VNMS (site principal)

Pour augmenter la disponibilité du système du site principal, tous les composants matériels et logiciels ainsi que les accès aux réseaux internes et externes sont redondants. En particulier, toutes les machines sont doublées sur site excepté le serveur de sauvegarde qui est doublé à distance et

elles fonctionnent soit dans un mode, machine de secours passive, soit dans un mode haute disponibilité.

2.2.3.2 Site de secours

Le site de secours dispose des mêmes fonctions mais n'a pas le même niveau de redondance des machines et des réseaux.

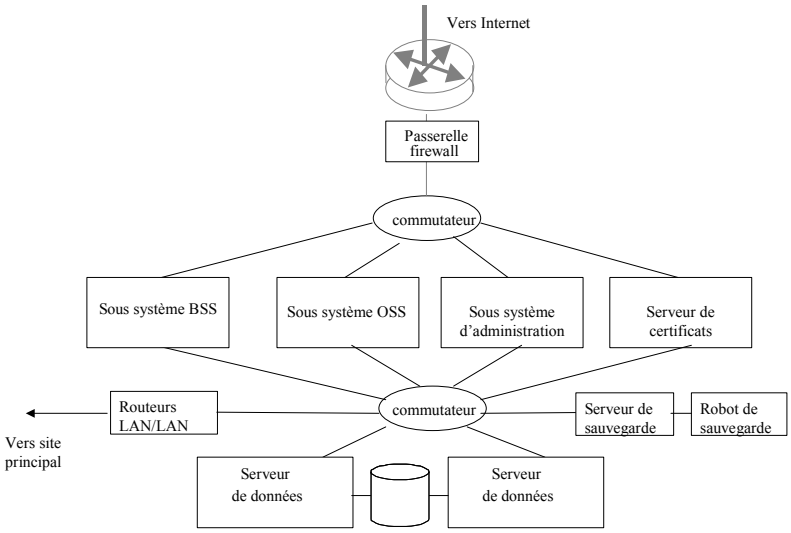

Figure 4: Site de secours

2.2.3.3 Composants matériels/logiciels du site de secours

Identiques à ceux du site principal, sauf que les machines de traitement ne sont pas doublées.

2.2.3.4 Equipement VPN supporté dans le cadre de l'évaluation

L'équipement cité est fourni à l'évaluateur pour lui permettre d'auditer le fonctionnement de la TOE.

Description	Matériel	Logiciel
Routeur	2 routeurs 6wind 6211 (série 6200)	Logiciel 6-wind 4.1.3

Tableau 7 : Caractéristiques de l'équipement VPN supporté

2.2.4 Interactions externes du système

Le système VNMS est accédé par :

- Les consoles des administrateurs du système VNMS et du service VPN administré,
- Les consoles Web d'exploitation qui permettent aux gestionnaires des opérateurs d'exploiter le service,
- Les wizards de configuration sur site des équipements VPN,
- Les consoles Web des abonnés.

Le système VNMS accède ou est accédé par les équipements VPN des abonnés.
L'utilisation des consoles par les différents administrateurs est décrite dans les tableaux ci-dessous:

Rôle	Console distante d'administration du système principal et locale du système de secours	Console locale de supervision du système principal
Administrateur système privilégié et	x	x

autres administrateurs		

Tableau 8 : utilisation des consoles par les administrateurs du système

Rôle	Console d'exploitation du service	Console d'abonné	Wizard de configuration	Console d'administration
Gestionnaire privilégié	x		x	
Gestionnaire	x		x	
Abonné		x		
Responsable de site			x	
Administrateur privilégié du service				x

Tableau 9: utilisation des consoles par les administrateurs du service

Les interfaces externes du système sont représentées sur la figure suivante.

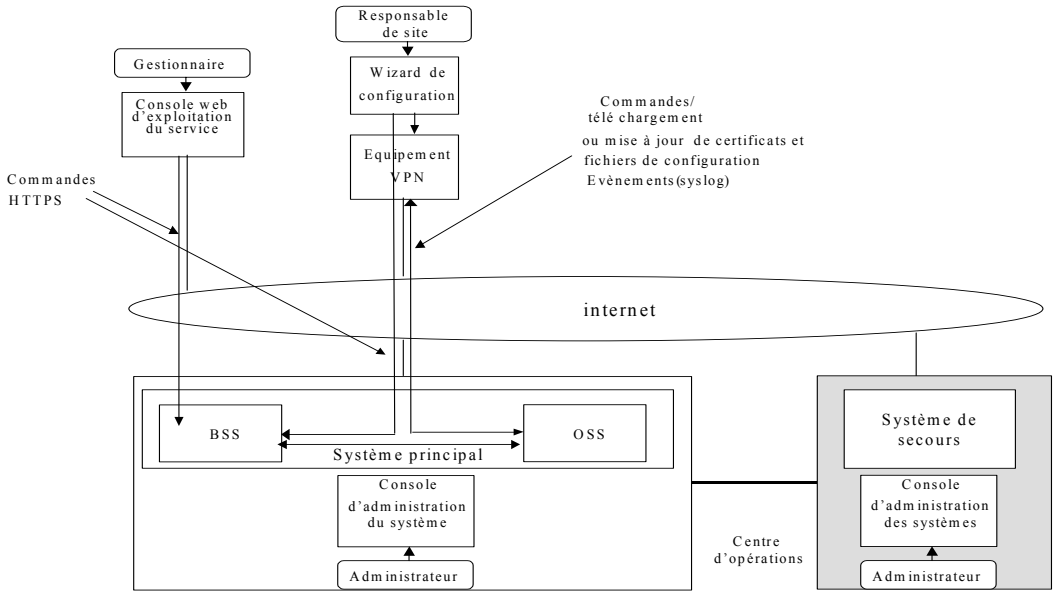

Figure 5 : Interactions externes du système (hors TOE)

2.2.5 Contribution du système à la production de VPN

Le *système* contribue indirectement à la production de VPN. Noter qu'un tunnel VPN entre deux équipements VPN ne fait pas partie de la TOE.

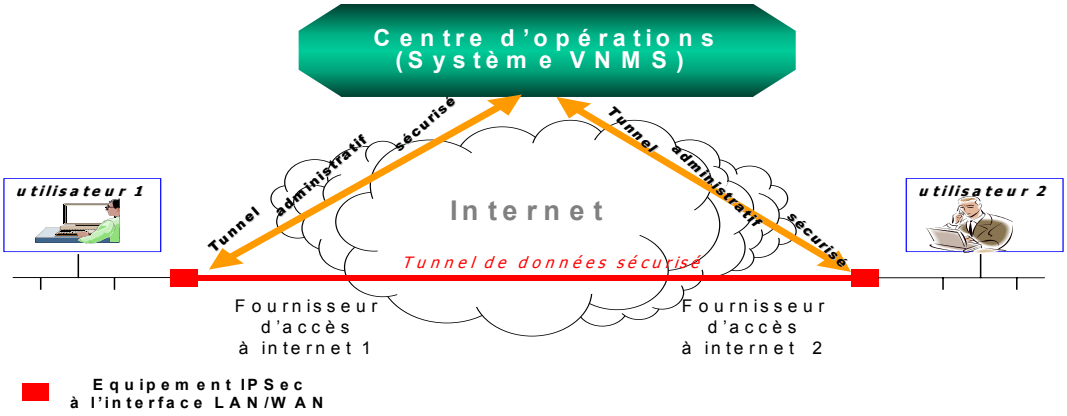

Figure 6: Contribution de la TOE à la production de VPN

La contribution du *système* pour produire des VPN est la suivante :
Dans un premier temps un gestionnaire opérateur déclare un abonné à l'aide de sa console Web d'exploitation du service, les sites de cet abonné et le ou les VPN auxquels participent les sites.
Dans un deuxième temps, les équipements VPN des sites déclarés sont rendus opérationnels par du personnel de l'opérateur qui se rend sur les sites et qui installent, configurent et mettent en service les équipements VPN des sites. L'opération d'approvisionnement (provisioning) d'un équipement VPN est réalisée à l'aide d'un wizard de configuration qui rend cette opération simple. Un VPN est automatiquement activé dès qu'au moins deux sites qui participent au VPN sont opérationnels.
Dès qu'un site envoie du trafic à un autre site, une liaison VPN appelée tunnel est établie entre les équipements VPN de chaque site.
A partir de ce moment là, le *système* n'intervient plus, excepté si :

- les équipements VPN génèrent des évènements (trap snmp) ou des fichiers de log (syslog) qui sont collectés par le sous système OSS du *système*.
- un gestionnaire modifie un VPN par exemple rajout ou suppression d'un ou plusieurs sites. Ces opérations se traduisent par des modifications de configuration dynamique des équipements VPN du VPN qui sont réalisées à distance par le sous système OSS du *système*
- une demande de renouvellement de certificat est effectuée.

Noter que dès qu'un VPN a moins de deux sites, il est désactivé.

2.2.6 Droits d'accès aux fonctions du service

Ces rôles donnent des droits à des exploitants ou administrateurs du service à pouvoir effectuer certaines opérations. Ces opérations figurent dans le tableau ci-dessous.

Fonctions	Administrateur privilégié du service	Gestionnaire privilégié	Gestionnaire	Abonné	Responsable de site
Connexion au service	√	√	√	√	√
Modification de mot de passe	script	√	√	√	√
Création d'un administrateur	script				
Création d'un opérateur	script				
Sélectionner un opérateur	√				
Supprimer un opérateur	script				
Création d'un gestionnaire	√	√			
Sélectionner un gestionnaire	√	√			
Consulter/modifier les informations concernant un gestionnaire	√	√			
Supprimer un gestionnaire	√	√			
Consulter ses informations personnelles		√	√	√	√
Créer un abonné	√	√	√		
Supprimer un abonné	√	√	√		
Sélectionner un abonné	√	√	√		
Consulter un abonnement	√	√	√		√
Modifier un abonnement	√	√	√		
Consulter/modifier les informations concernant un abonné	√	√	√		
Créer un site	√	√	√		
Sélectionner un site	√	√	√		√
Assigner/de assigner un site à un abonnement	√	√	√		√
Activer / dé activer les fonctions VPN d'un site	√	√	√		√
Consulter les informations concernant un site	√	√	√		√
Modifier les informations concernant un site	√	√	√		
Récupérer l'adresse IP d'un site	√	√	√		
Supervision des liaisons VPN d'un équipement VPN d'un site	√	√	√		
Supprimer un site	√	√	√		
Ajouter/supprimer un site à un VPN	√	√	√	√	√
Créer un VPN local ou global	√	√	√		√
Sélectionner un VPN	√	√	√		√
Consulter/Modifier les caractéristiques d'un VPN (exemple assignation/dé assignation de site)	√	√	√		√
Supprimer un VPN	√	√	√		√
Mise à jour d'un équipement VPN centre d'étoile	√	√	√	√	
Vérification de la mise à jour d'un équipement VPN centre d'étoile	√	√	√	√	
Visualisation des rapports d'activité VPN	√	√	√	√	
Visualisation des rapports d'activité complets	√	√	√	√	
Supervision d'un VPN	√	√	√	√	
Supervision d'un équipement VPN de site	√	√	√	√	
Demander le renouvellement de certificat d'un équipement VPN de type routeur	√	√	√	√	
Récupérer les informations nécessaires à la demande de certificat pour un client VPN				√	
Récupérer la configuration VPN d'un client VPN				√	
Connexion au service	√	√	√	√	√

Tableau 10 : Fonctions de l'interface graphique d'exploitation du service

2.2.7 Règles d'accès aux fonctions du système

2.2.7.1 Domaines de responsabilité

Cinq domaines de responsabilité de type administrateur, opérateur et superviseur sont identifiés :

- Administrateur système privilégié,
- Administrateur du stockage,
- Administrateur de la sauvegarde,
- Administrateur du service de certificats,

- Administrateur réseau.

L'administrateur système privilégié dispose de l'ensemble des mots de passe.
L'administrateur de chaque domaine a la responsabilité des différents mots de passe du domaine.

2.2.7.2 Droits d'accès aux fonctions du système

Les droits pour pouvoir effectuer les opérations d'administration système portant sur les machines et leurs systèmes d'exploitation ainsi que sur les services système qui tournent sur ces machines, sont fonction de la connaissance par les administrateurs de profils de type login-mot de passe associés à des comptes administrateurs.

2.2.7.3 Définition des mots de passe

Les mots de passe sont générés selon une procédure automatisée lancée par une commande.

2.2.7.4 Renouvellement des mots de passe

Les mots de passe sont renouvelés périodiquement. Le renouvellement est effectué par l'administrateur du domaine qui renouvelle les mots de passe de l'ensemble des comptes dont il a la responsabilité.
Pour la génération d'un nouveau mot de passe, une procédure de génération automatique de mot de passe est utilisée.

2.2.8 Rôle du wizard de configuration

Le *wizard* de configuration assure le service d'approvisionnement qui consiste à installer, configurer et mettre en service sur un site d'abonné, un équipement VPN pour le rendre opérationnel. Cette opération est réalisée par du personnel de l'opérateur qui a le rôle de responsable de site.
Le wizard de configuration est un logiciel qui tourne sur un PC. Le logiciel peut être amené par le responsable de site qui effectue l'opération et ensuite être emporté par le responsable de site une fois que l'équipement VPN est opérationnel.

2.3 Description de l'environnement du système

On distingue :

- L'environnement du système non TI qui fait partie de la TOE,
- L'environnement du système hors TOE.

Composant	Dans la TOE (mais non TI)	Hors TOE
Equipe d'exploitation du centre d'opérations qui est composée de personnel Netcelo avec les rôles d'administrateur privilégié et d'administrateur	X	
Bâtiments qui hébergent le site principal du centre d'opérations	X	
Equipements VPN qui doivent disposer d'IPSEC		X
Postes de travail situés dans des locaux d'opérateurs et qui sont équipés d'un navigateur. Ces postes de travail sont utilisés par les gestionnaires d'opérateurs pour exploiter le service VPN administré		X
Les wizards de configuration utilisables avec les droits de responsable de site		X

Réseau public Internet		X
Liaison de réseau privé à haut débit qui relie le site principal du centre d'opérations au site de secours.		X

Tableau 11 : Environnement du système

2.4 Biens sensibles

Ces tableaux indiquent ce que l'on veut protéger.

Système	Contrôles d'accès	Disponibilité	Intégrité
Machines	X	X	
Applications	X	X	

Tableau 12: Biens sensibles- les machines et applications du système

Données	Confidentialité	Disponibilité	Intégrité
Clé privée du serveur de certificat	X		
Mots de passe des gestionnaires , des responsables de site et des administrateurs	X		
Données échangées entre le système et les gestionnaires, les abonnés	X		
Commandes échangées entre le système et les équipements VPN	X		X
Certificats transférés par le système aux équipements VPN	X		
Données commerciales des opérateurs gérées par le système	X		X

Tableau 13: Biens sensibles- les données du système

2.5 Portée et limites du système

Objet	TOE	Hors TOE
Site principal du centre d'opérations	X	
Site de secours du centre d'opérations	X	
Le système VNMS qui équipe ces sites	X	
Wizard de configuration		X
Console Web pour accéder au système VNMS		X
Equipements VPN des sites des abonnés		X
Réseau public Internet		X
Réseau privé inter-sites VNMS		X
Réseaux VPN dont les nœuds sont des sites des abonnés.		X

Tableau 14: Portée et limites du système

Le tableau suivant précise qui agit sur la TOE et ce sur quoi la TOE agit.

Impact	Sur le système	A l'initiative du système
Equipement VPN		X
Abonné via une console Web	X	
Gestionnaire via une console Web	X	
Responsable de site via le wizard de configuration	X	
Administrateur	X	
Internet	X	

Tableau 15: Impacts sur le système ou à l'initiative du système.

Chapitre 3

Ce chapitre décrit les dangers susceptibles d'altérer les biens sensibles.
Il faut déterminer les dangers contre lesquels on veut se protéger, quels sont ceux qui sont contrés par la TOE. On aura alors les menaces.

3 Environnement de sécurité du système

3.1 Hypothèses concernant l'environnement hors système (hors TOE)

Des hypothèses sont faites sur les dangers de l'environnement hors *système* (sur lequel l'évaluation ne porte pas) pour que le *système* fonctionne correctement. Les hypothèses doivent être reliées aux objectifs de sécurité hors TOE.

Identification	Hypothèse	Risque contré
HYP 1	Les mots de passe des routeurs sont confidentiels et ne sont pas divulgués par les gestionnaires qui disposent eux mêmes d'identifiants et de mots de passe pour se connecter au système.	Les équipements VPN qui ont un mot de passe divulgué peuvent être accédés par des hackers via le réseau interne du site de l'abonné ou internet.
HYP 2	Les équipements VPN administrés par le service VPN administré disposent du logiciel IPSEC	Un équipement VPN ne disposant pas du logiciel IPSEC ne peut pas être télé administré par le service VPN administré
HYP 3	Les équipements VPN administrés qui utilisent des clés supérieures à 128 bits (cas du 3DES) ont fait l'objet d'une autorisation de fourniture en vue d'une autorisation générale	Illégalité d'un abonné
HYP 4	L'approvisionnement d'un équipement VPN est fait de manière correcte par du personnel compétent	Impossibilité d'administrer un équipement VPN

Tableau 16: Hypothèses et risques sur l'environnement hors système

3.2 Menaces concernant le *système* et son environnement non TI

Les menaces sont décrites comme un impact sur un bien sensible réalisé par des facteurs de menace (personne humaine: opérateur, hacker sur internet, administrateur, cambrioleur ou physique : incendie, inondation, …) qui utilise un chemin d'attaque (exemple usurpation d'adresse, divulgation de mot de passe, effraction, etc.) contre lesquelles une protection est requise.

Pour identifier les menaces l'approche décrite dans [ISO/IEC 15446] est utilisée :

- Quels sont les biens sensibles qui demandent une protection
- Qui ou quels sont les agents porteurs des menaces,
- De quelles méthodes d'attaque ou d'événements indésirables, les biens sensibles doivent être protégés ?

Dans le tableau ci-dessous les chemins d'attaque et événements indésirables qui peuvent porter sur la TOE ou son environnement non TI sont listés en utilisant la classification EBIOS.

Identification	Thème	Chemin d'attaque	Atteinte
1	Accidents physiques	Incendie	
2		Dégats des eaux	
3		Pollution	
4		Accidents majeurs	
5	Evènements naturels	Phénomène climatique	
6		Phénomène sismique	Disponibilité
8		Phénomène météorologique	
10	Perte de services essentiels	Défaillance de la climatisation	
11		Perte d'alimentation énergétique	
12		Perte des moyens de télécommunications	
17	Compromission des informations	Espionnage à distance	Confidentialité
19		Vol de supports et de documents	Confidentialité
20		Vol de matériels	Confidentialité, Disponibilité
21		Divulgation externe	Confidentialité
22		Divulgation interne	Confidentialité
31		Utilisation illicite du matériel	
		. connexion frauduleuse	Confidentialité, disponibilité, intégrité
		. violation du niveau de sécurité	Confidentialité, disponibilité, intégrité
		. fouille	Confidentialité
		. mystification	Confidentialité, disponibilité, intégrité
39		Abus de droit	Confidentialité, disponibilité, intégrité
40		Usurpation de droit	
23	Défaillance technique	Panne matérielle	Disponibilité
24		Dysfonctionnement matériel	Disponibilité
25		Saturation du matériel	Disponibilité
26		Dysfonctionnement logiciel	Disponibilité, intégrité
28		Atteinte à la maintenabilité du SI	Disponibilité
27	Agression physique	Destruction de matériels	Disponibilité
39	Actions illicites	Abus de droits	Confidentialité, disponibilité, intégrité
40		Usurpation de droits	
		. mascarade	Confidentialité, disponibilité, intégrité
		. substitution	Confidentialité, disponibilité, intégrité
42		Fraude	
		. inférence sur les données	Confidentialité, anonymat
20	Compromission des fonctions	Vol de matériel	Confidentialité, Disponibilité
25		Saturation	Disponibilité
31		Utilisation illicite du matériel	
		. connexion frauduleuse	Confidentialité, disponibilité, intégrité
32		Altération du logiciel	Confidentialité, disponibilité, intégrité
33		Piégeage du logiciel	Confidentialité, intégrité
36		Altération des données	
		. interception	Intégrité
		. balayage	Confidentialité
		. virus	Confidentialité, intégrité
39		Abus de droits	Confidentialité, disponibilité, intégrité
		Fraude	
42		. inférence sur les données	Confidentialité, anonymat

43		Atteinte à la disponibilité du personnel	Disponibilité
38	Erreur	Erreur d'utilisation	Disponibilité, intégrité

Tableau 17: Chemins d'attaque génériques

La rédaction définitive des menaces tient compte des agents facteurs de menaces, des biens sensibles sujets aux attaques et aux chemins d'attaque.

Identification	Menace	Agent	Biens sensibles	Chemins d'attaque
M1	Le système est exposé à des risques physiques tels que vol de matériel, ou des risques sociaux ou naturels qui peuvent le rendre partiellement ou complètement indisponible	Personnes humaines ou évènements sociaux ou naturels	Les équipements du système	Accidents physiques Evènements naturels Perte de services essentiels (1) à (12), 20, 27
M2	Le système est exposé à des risques logiques entraînant une saturation du système qui rend le service inopérant.	Hacker	Les firewalls Les applications et les données.	Compromission des fonctions Saturation(25)
M3	Le système est exposé à des risques logiques entraînant une intrusion dans le système via l'extérieur (internet) ou l'intérieur. Les intrusions sont caractérisées par l'utilisation des services (au niveau des noyaux des systèmes d'exploitation) normalement associés aux sessions administrateur ou administrateur privilégié..	Attaquant externe ou interne	Les machines de traitement et de données Les données	Compromission des fonctions 32,33,36 Compromission des informations Divulgation externe (21) Divulgation interne(22)
M4	Le système est exposé à des risques d'utilisation excessive entraînant une saturation du système qui rend le service inopérant.	Equipement VPN	Les machines de traitement Les applications et les données.	Compromission des fonctions Saturation(25)
M5	Le système est exposé à des erreurs des administrateurs autorisés dans l'application des procédures.	Administrateur	Les machines et les logiciels du système	Erreur Erreur d'utilisation(38)
M6	Des usurpateurs de rôles : gestionnaire, responsable de site ou des équipements VPN non autorisés peuvent tenter d'utiliser le service.	Equipement VPN non autorisé Usurpateur de rôle de responsable de site. Usurpateur de rôle de gestionnaire de site	Applications-contrôles d'accès	Compromission des informations Abus de droits (39)
M7	Un CPE non autorisé peut usurper d'identité d'un CPE autorisé pour demander un certificat au service de certification du système.	Equipement VPN	Service de certificat	Compromission des fonctions utilisation illicite du matériel (31) abus de droits (39)
M8	Le système est exposé à des risques de divulgation d'informations des opérateurs ou des équipements VPN lors d'échanges sur le réseau internet avec les consoles des gestionnaires des opérateurs, le wizard de configuration, les consoles web des abonnés ou les équipements VPN.	Attaquant externe		Compromission des informations : Divulgation externe (21)
M9	Le système est exposé à des disfonctionnements liés à des problèmes ou des défaillances techniques	Matériel Logiciel	Les machines Les traitements Les réseaux Les données	Défaillance technique Panne matérielle (23) Saturation du matériel (25)

				Disfonctionnement logiciel(26) Atteinte à la maintenabilité du SI(28)
M10	Le système est exposé à des risques de modification du contenu des sessions d'approvisionnement lors d'échanges sur le réseau internet avec les équipements VPN.	Attaquant externe	Commandes échangées avec les équipements VPN – intégrité	

Tableau 18: Menaces pour le système

3.3 Politique de sécurité organisationnelle

La politique de sécurité organisationnelle décrit ce qui doit être garanti à priori.

Identification	Politique de sécurité organisationnelle	TOE non TI
OSP1	Les accès physiques au système doivent être contrôlés et protégés	X
OSP2	Les administrateurs doivent être formés pour utiliser les outils de supervision et d' administration.	X
OSP3	Dans le cas de projets particuliers ou d'opérations lourdes sur le système VNMS, une astreinte peut être mise en place pour assurer une permanence des administrateurs en dehors des heures ouvrables et des jours fériés.	X

Tableau 19: Politique de sécurité organisationnelle

Chapitre 4

4 Objectifs de sécurité

Les objectifs de sécurité fournissent un état concis de la réponse aux problèmes de sécurité.

4.1 Objectifs de sécurité TI pour le système

Les objectifs de sécurité du *système* doivent établir quelle est la responsabilité du *système* pour contrer les menaces et en supportant les politiques des objectifs de sécurité. Trois types d'objectifs de sécurité peuvent être identifiés pour traiter les menaces identifiées : prévention, détection et correction.

Objectif	Description de l'objectif
OST 1	La TOE assurera que chaque gestionnaire et responsable de site est identifié de manière unique, et que l' identification qu'il fournit est authentifiée avant de permettre à l'utilisateur d'accéder les ressources de la TOE.
OST 2	La TOE fournira des services pour permettre à un administrateur autorisé d'administrer effectivement la TOE et ses fonctions de sécurité et assurera que seuls les administrateurs autorisés sont capables d'accéder ces fonctions.
OST 3	La TOE fournira les moyens de protéger 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.
OST 4	La TOE mettra en œuvre un contrôle de l'utilisation de ses ressources de la part de ses utilisateurs et des équipements VPN administrés afin d'empêcher un refus de service non autorisé
OST 5	La TOE fournira les moyens pour garantir une étanchéité entre les données commerciales des opérateurs .
OST 6	La TOE garantira aux opérateurs l'intégrité de leurs données
OST 7	La TOE fournira les moyens pour que soient enregistrés (audit), les évènements qui surviennent lors du fonctionnement des fonctions de sécurité.
OST 8	La TOE fournira les moyens de créer et de maintenir une trace d'audit sûre
OST 9	La TOE fournira les moyens pour s'assurer qu'un équipement VPN émetteur d'une requête d'approvisionnement est bien autorisé à bénéficier de ce service.
OST 10	La TOE fournira les moyens pour s'assurer qu'un équipement VPN est autorisé à demander un certificat.
OST 11	La TOE sera dotée de mécanismes permettant de surveiller sa disponibilité 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.
OST 12	La TOE fournira les moyens pour se protéger des attaques via Internet.
OST 13	La clé secrète du serveur de certificats ne doit pas être divulguée
OST 22	La TOE disposera d'un site de secours capable de reprendre l'activité du site principal.

Tableau 20: Objectifs de Sécurité TI pour la TOE (OST)

4.2 Objectifs de sécurité non TI pour le système

C'est l'ensemble des objectifs de sécurité que les aspects organisationnels devraient garantir.
Il faut identifier des mesures de sécurité à mettre en face de ces objectifs.

Objectif	Description de l'objectif
OSNT 14	Les services d'audit sont utilisés et administrés effectivement par les administrateurs du système.
OSNT 15	Un service d'assistance par numéro d'appel téléphonique et messagerie électronique est assuré pendant des périodes (plages horaires et jours) définies en fonction du contrat du client.
OSNT 16	L'accès physique au système est strictement limité aux personnes autorisées.
OSNT 17	Les informations sensibles du système (systèmes d'exploitation, configurations, certificats, clé secrète du serveur de certificat) ainsi que les données commerciales des opérateurs ne sont pas perdues.
OSNT 18	La TOE est installée, configurée et mise en service d'une manière qui assure la sécurité du système.
OSNT 19	Les administrateurs supervisent (suivi des incidents de sécurité) et administrent (réaction vis à vis de l'évolution de la sécurité du système, exemple paramétrage des fonctions de sécurité) la TOE d'une manière correcte vis à vis de la sécurité du système.
OSNT 20	L'architecture du système est conçue pour faciliter la disponibilité du système

Tableau 21: Objectifs de Sécurité Non TI pour la TOE (OSNT)

4.3 Objectifs de sécurité hors système

Objectif	Description de l'objectif
OSHT 20	Les équipements VPN administrés par le service supportent des protocoles sécurisés comme SSH et SCP pour permettre leur télé-administration sécurisée par le système dans le cadre de la production et l'exploitation de VPN IPSEC. Les équipements VPN supportent le protocole IPSEC car la TOE produit uniquement des fichiers de configuration IPSEC pour les équipements VPN qu'elle administre.
OSHT 21	Les utilisateurs de consoles Web ou de Wizards de configuration ne ne divulguent pas les identifiants et mots de passe qui leur seront communiqués pour se connecter au système.

Tableau 22: Objectifs de Sécurité Hors TOE (OSHT)

Chapitre 5

5 Exigences de sécurité

Ce chapitre décrit :

- Les exigences fonctionnelles de sécurité (SFR) TI et non TI pour le *système*.
  Elles identifient les exigences pour des fonctions de sécurité que le *système* doit fournir pour assurer que les objectifs de sécurité définis pour le *système* sont atteints.
- Les exigences d'assurance de sécurité (SAR) pour le *système*.
  Elles identifient le niveau d'assurance exigé dans l'implémentations des SFRs.

5.1 Exigences fonctionnelles de sécurité pour le système

Ce chapitre décrit les politiques de sécurité mises en œuvre par les fonctions de sécurité :

- Politique technique de sécurité au niveau services
  - contrôle d'accès aux services applicatifs
  - maintien de l'intégrité des données opérateurs
  - disponibilité des services
- Politique technique de sécurité au niveau système
  - contrôle d'accès aux fonctions système
- Politique technique de sécurité au niveau réseau
  - contrôle des flux d'information Internet au niveau réseau/transport
  - authentification/chiffrement des accès Internet à la TOE

Pour des raisons de lisibilité, les exigences fonctionnelles de sécurité ont été écrites en français, et on a opéré à des re formulations une fois les opérations effectuées. L'existence d'opérations effectuées est signalée à l'aide de caractères gras dans le texte des éléments. L'annexe 2 fournit le détail des opérations effectuées sur le texte anglais d'origine des composants des Critères Communs V2.1 [CCPART2].

5.1.1 Exigences générales (domaine TOP)

Le domaine TOP est un domaine général qui s'applique à tous les autres domaines de la TOE : domaines système et service.

TOP/FMT.SMR.1	**Rôles de sécurité**
TOP/FMT_SMR.1.1	La TSF doit tenir à jour les rôles : **- administrateur privilégié,** **- administrateur,** **- gestionnaire privilégié,** **- gestionnaire,** **- responsable de site,** **- abonné.**
TOP/FMT_SMR.1.2	La TSF doit être capable d'associer des rôles aux utilisateurs.
Audit:	*Les modifications du groupe des utilisateurs correspondant à un rôle*

TOP/FIA_UID.2	Identification de l'utilisateur avant toute action
TOP/FIA_UID.2.1	La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.
Audit:	*Utilisation infructueuse du mécanisme d'identification de l'utilisateur, avec l'identité de l'utilisateur fournie*

TOP/FIA_UAU.2	Authentification de l'utilisateur avant toute action
TOP/FIA_UAU.2.1	La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.
Audit:	*Utilisation infructueuse du mécanisme d'authentification*

TOP/FIA_UAU.6	Réauthentification
TOP/FIA_UAU.6.1	La TSF doit réauthentifier les utilisateurs **lorsque leur console a dépassé le délai maximum d'inactivité**. **- Pour les utilisateurs distants (console Web, wizard de configuration), le délai maximum d'inactivité est de trois minutes.** **- Pour les consoles des administrateurs sur le site principal ou le site de secours, le délai maximum d'inactivité est de trois minutes.**
Audit:	*Échec de réauthentification*

TOP/FAU_GEN.1	Génération de données d'audit
TOP/FAU_GEN.1.1	La TSF doit pouvoir générer un enregistrement d'audit pour les événements auditables suivants : a) démarrage et arrêt des fonctions d'audit ; b) **(sans objet)** ; c) et **les événements figurant dans la rubrique 'audit' associée à chaque composant d'exigence fonctionnelle de sécurité inclus dans cette cible de sécurité.**
TOP/FAU_GEN.1.2	La TSF doit enregistrer au minimum les informations suivantes dans chaque enregistrement d'audit : a) date et heure de l'événement, type d'événement, identité du sujet, ainsi que le résultat (succès ou échec) de l'événement ; b) et, pour chaque type d'événement d'audit, **les informations d'audit mentionnées dans les rubriques 'audit' associées aux composants d'exigence fonctionnelle de sécurité inclus dans cette cible de sécurité.**
Audit:	*(néant)*

TOP/FAU_SAR.1	Revue d'audit
TOP/FAU_SAR.1.1	La TSF doit offrir aux **administrateurs privilégiés** la capacité de lire **la totalité des informations d'audit** à partir des **fichiers de log**.
TOP/FAU_SAR.1.2	La TSF doit présenter **les fichiers de log** d'une façon permettant aux **opérateurs système** et aux **administrateurs privilégiés** de les interpréter.
Audit:	*Lecture d'informations à partir des enregistrements d'audit.*

TOP/FAU_STG.2	Garanties de disponibilité des données d'audit
TOP/FAU_STG.2.1	La TSF doit protéger les enregistrements d'audit stockés contre une suppression non autorisée.
TOP/FAU_STG.2.2	La TSF doit pouvoir **empêcher** les modifications effectuées sur les enregistrements d'audit.
TOP/FAU_STG.2.3	La TSF doit garantir que **les volumes suivants** d'enregistrements d'audit seront maintenus quand **un dépassement de capacité du stockage de l'audit** apparaîtra : **- pour le serveur de certificats : les enregistrements d'audit les plus récents,** **- pour les serveurs de données : les derniers enregistrements d'audit avant l'arrêt des fonctions d'audit.**
Audit:	*(néant)*

TOP/FAU_STG.4	Prévention des pertes de données d'audit
TOP/FAU_STG.4.1	Si les **fichiers de log** sont pleins, la TSF doit **- ignorer les événements auditables (cas des serveurs de données),** **- écraser les enregistrements d'audit les plus anciennement stockés et remonter une alarme (cas du serveur de certificats).**
Audit:	*Actions entreprises à la suite d'une défaillance dans le stockage de l'audit.*

TOP/FAU_SAA.1	Analyse de violation potentielle
TOP/FAU_SAA.1.1	La TSF doit pouvoir appliquer un ensemble de règles en surveillant les événements audités et indiquer, en fonction de ces règles, une violation potentielle de la TSP.

TOP/FAU_SAA.1.2	La TSF doit appliquer les règles suivantes pour la surveillance des événements audités : a) aucun événement b) **- Détection des défaillances par 'ping' : la TSF vérifie l'activité des machines et des équipements du système à l'aide de requêtes ICMP de type 'echo'. Une machine ou un équipement qui ne répond plus est présumé défaillant.** **- Le firewall (stateful) enregistre dans ses fichiers de log des enregistrements qui concernent les état s de connexion du trafic autorisé ainsi que du trafic refusé. Les fichiers de log sont analysés manuellement.** **- Les erreurs d'intégrité détectées par Oracle se traduisent par des codes d'erreur transmis aux émetteurs des requêtes.**
Audit:	*Activation et désactivation des outils d'analyse* *Violations potentielles détectées par les outils.*

TOP/FAU_ARP.1	**Alarmes de sécurité**
TOP/FAU_ARP.1.1	La TSF doit **afficher un message d'alerte sur la console système ou envoyer un mail aux administrateurs** dès la détection d'une violation potentielle de la sécurité.
Audit:	*(néant)*

TOP/FPT_STM.1	**Horodatage fiable**
TOP/FPT_STM.1.1	La TSF doit être capable de fournir un horodatage fiable pour son propre usage.
Audit:	*Modifications de la date.*

TOP/FRU_FLT.2	**Tolérance vis-à-vis des pannes**
TOP/FRU_FLT.2.1	La TSF doit garantir le fonctionnement de toutes les capacités de la TOE lorsque les défaillances suivantes surviennent : **- défaillance des unités de stockage des machines critiques (Firewall, SES, SMS, Serveur de données SGD),** **- panne des machines critiques (Firewall, SES, SMS, Serveur de données SGD),** **- indisponibilité du site principal.**
Audit:	*Toute défaillance détectée par la TSF.*

TOP/FPT_FLS.1	**Défaillance avec préservation d'un état sûr**
TOP/FPT_FLS.1.1	La TSF doit préserver un état sûr quand les types de défaillances suivants se produisent : **- défaillance des unités de stockage des machines critiques (Firewall, SES, SMS, Serveur de données SGD),** **- panne des machines critiques (Firewall, SES, SMS, Serveur de données SGD),** **- indisponibilité du site principal.**
Audit:	*Toute défaillance détectée par la TSF.*

5.1.2 Exigences sur les services applicatifs (domaine SRV)

Note d'application : les services sont utilisés par des utilisateurs distants, à l'aide de consoles Web et de wizards de configuration. Les opérations sont effectuées à l'aide d'une interface Web présentée par le serveur BSS. Le serveur BSS traduit les opérations et les relaie vers les autres serveurs, et implémente la majorité du contrôle d'accès aux services.

SRV/FIA_ATD.1	**Définition des attributs des gestionnaires privilégiés, gestionnaires, responsables de site et abonnés.**
SRV/FIA_ATD.1.1	La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant aux **gestionnaires privilégiés, gestionnaires, responsables de site et abonnés** : **- préfixe d'opérateur,** **- pour les abonnés : identité de l'abonné.**
Audit:	*(néant)*

SRV/FDP_ACC.1	Contrôle d'accès partiel aux services applicatifs
SRV/FDP_ACC.1.1	La TSF doit appliquer **la politique de contrôle d'accès aux services applicatifs** aux **opérations effectuées par les utilisateurs à l'aide des services applicatifs des sous-systèmes suivants: les serveurs de données gérant les bases opérateurs, le sous système SES (BSS), le sous système SMS (OSS) et le serveur de certificat.**
Audit:	*(néant)*

SRV/FDP_ACF.1	Contrôle d'accès aux services applicatifs basé sur les attributs de sécurité
SRV/FDP_ACF.1.1	La TSF doit appliquer **la politique de contrôle d'accès aux services applicatifs** en se basant sur: **- le rôle des utilisateurs,** **- le préfixe d'opérateur des gestionnaires privilégiés, gestionnaires, responsables de site et abonnés,** **- l'identité des abonnés.**
SRV/FDP_ACF.1.2	La TSF doit appliquer **les règles décrites dans le tableau 14** pour déterminer si une opération effectuée par **un utilisateur contrôlé** sur **un service applicatif contrôlé** est autorisée.
SRV/FDP_ACF.1.3	**(sans objet)**.
SRV/FDP_ACF.1.4	La TSF doit refuser explicitement l'accès des gestionnaires privilégiés, gestionnaires, responsables de site et abonnés aux bases opérateurs en fonction **des règles suivantes:** **- les gestionnaires privilégiés, gestionnaires et responsables de site d'un opérateur n'ont pas accès aux bases des autres opérateurs,** **- les abonnés n'ont pas accès aux informations des autres abonnés**.
Audit:	*Demandes réussies d'exécution d'une opération.*

SRV/FDP_ITT.1	Protection élémentaire des transferts entre les serveurs applicatifs et les serveurs de données.
SRV/FDP_ITT.1.1	La TSF doit appliquer **la politique de maintien de l'intégrité des données opérateurs** pour empêcher **la modification ou la perte d'utilisation** de données **des opérateurs** au cours de leur transmission entre **les sous systèmes techniques SES (BSS) et SMS (OSS) et le sous système de gestion des données.**.
Audit:	*Transferts de données opérateurs ainsi que toutes les erreurs qui sont survenues.*

SRV/FDP_SDI.2	Contrôle de l'intégrité référentielle des données opérateurs stockées et action à entreprendre
SRV/FDP_SDI.2.1	La TSF doit contrôler les données **des opérateurs** stockées **au sein des serveurs de données** à la recherche **d'erreurs d'intégrité référentielle** sur **toutes les bases opérateurs**, en fonction des attributs suivants : "primary keys", "foreign keys", "check constraints" définies dans le schéma de la base .
SRV/FDP_SDI.2.2	En cas de détection d'une **erreur d'intégrité référentielle**, la TSF rend un code retour exploité par le sous système technique SES.
Audit:	*Toutes les vérifications de l'intégrité des données opérateurs, ainsi qu'une indication de leur résultat.*

5.1.3 Exigences au niveau système (domaine SYS)

SYS/FIA_ATD.1	Définition des attributs des administrateurs et administrateurs privilégiés
SYS/FIA_ATD.1.1	La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant aux **administrateurs et administrateurs privilégiés** : **- compte utilisé pour effectuer des opérations.**
Audit:	*(néant)*

SYS/FDP_ACC.1	Contrôle d'accès partiel aux fonctions système
SYS/FDP_ACC.1.1	La TSF doit appliquer **la politique de contrôle d'accès aux fonctions système** aux **opérations effectuées par les administrateurs à l'aide des fonctions des systèmes d'exploitations des machines composant la TOE**.
Audit:	*(néant)*

SYS/FDP_ACF.1	Contrôle d'accès aux fonctions système basé sur les attributs de sécurité
SYS/FDP_ACF.1.1	La TSF doit appliquer **la politique de contrôle d'accès aux fonctions systèmes** en se basant sur: **- le rôle des administrateurs,** **- les comptes qu'ils utilisent pour effectuer les opérations.**
SYS/FDP_ACF.1.2	La TSF doit appliquer **les règles décrites dans le tableau 14** pour déterminer si une opération effectuée par **un administrateur contrôlé** sur **un système d'exploitation contrôlé** est autorisée.
SYS/FDP_ACF.1.3	**(sans objet).**
SYS/FDP_ACF.1.4	**(sans objet)**
Audit:	*Toutes les demandes d'exécution d'une opération.*

5.1.4 Exigences au niveau réseau (domaine NTW)

NTW/FDP_IFC.1	Contrôle de flux d'information partiel au niveau réseau/transport
NTW/FDP_IFC.1.1	La TSF doit appliquer **la politique de contrôle des flux d'information Internet au niveau réseau/transport** aux **datagrammes IP d'Internet vers la TOE ou de la TOE vers Internet**.
Audit:	*(néant)*

NTW/FDP_IFF.1	Attributs de sécurité simples
NTW/FDP_IFF.1.1	La TSF doit appliquer **la politique de contrôle des flux d'information Internet au niveau réseau/transport** en fonction des types suivants d'attributs de sécurité des **machines émettrices et destinataires de part et d'autre du firewall et des datagrammes IP** : **- adresse IP,** **- type de protocole transport,** **- numéro de port TCP ou UDP.**
NTW/FDP_IFF.1.2	La TSF doit autoriser **un datagramme IP à transiter à travers le firewall d'une machine émettrice vers une machine destinataire** si les règles suivantes s'appliquent : **- les trafics entrants UDP/514, HTTP, HTTPS et FTP (port 21) sont les seuls autorisés,** **- les trafics sortants HTTPS, FTP, SSH et SCP sont seuls autorisés.**
NTW/FDP_IFF.1.3	**(sans objet)**
NTW/FDP_IFF.1.4	**(sans objet)**
NTW/FDP_IFF.1.5	La TSF doit autoriser explicitement **un datagramme IP à transiter à travers le firewall d'une machine émettrice vers une machine destinataire** en fonction des règles suivantes : **- une connexion de donnée FTP peut passer à travers le firewall si elle est correcte vis-à-vis du contexte d'une session FTP active.**
NTW/FDP_IFF.1.6	La TSF doit interdire explicitement **un datagramme IP à transiter à travers le firewall d'une machine émettrice vers une machine destinataire** en fonction de la règle **"tous les flux d'information qui ne sont pas explicitement autorisés sont interdits".**
Audit:	*Décisions de rejeter les datagrammes IP.*

NTW/FTP_ITC.1	Canal de confiance entre la TSF et les consoles Web, les wizards de configuration et les équipements VPN administrés
NTW/FTP_ITC.1.1	La TSF doit fournir un canal de communication entre elle-même et **les consoles Web, les wizards de configuration et les équipements VPN administrés** distants qui soit logiquement distinct des autres canaux de communication et qui fournisse une **authentification mutuelle** de ses extrémités et la protection des données transitant par le canal contre la modification ou la divulgation.
NTW/FTP_ITC.1.2	La TSF doit permettre **à la TSF, aux consoles Web, aux wizards de configuration et aux équipements VPN administrés** distants d'initier la communication via le canal de confiance.
NTW/FTP_ITC.1.3	La TSF doit initier la communication via le canal de confiance pour **les sessions d'administration des équipements VPN**.
Audit:	*Défaillance des fonctions du canal de confiance (échec à l'authentification mutuelle, modification des données transitant par le canal, ...), avec l'identification de l'initiateur et de la cible des fonctions défaillantes du canal de confiance*

5.2 Exigences d'assurance pour le système

Le niveau d'assurance visé pour le système VNMS est le niveau EAL1+ c'est à dire EAL1 augmenté du composant AVA_VLA.2.

Le niveau EAL1 + fournit un niveau d'assurance de base par une analyse des fonctions de sécurité qui utilisent une spécification fonctionnelle et d'interface et des guides pour comprendre le comportement de la sécurité.
L'analyse indépendante de vulnérabilité est supportée par des tests indépendants des fonctions de sécurité de la TOE.

Composant	Description
ACM_CAP.1	Gestion de numéros de versions
ADO_IGS.1	Installation, génération, et procédures de démarrage
ADV_FSP.1	Spécification fonctionnelle informelle
ADV_RCR.1	Démonstration de correspondance informelle
AGD_ADM.1	Guide de l'administrateur

AGD_USR.1	Guide de l'utilisateur
ATE_IND.1	Test indépendant- Conformité
ATE_VLA.2	Analyse indépendante de vulnérabilité

Tableau 23: Composants d'assurance EAL1+

5.3 Exigences de sécurité non TI

Ce chapitre décrit les exigences de sécurité non techniques mises en œuvre par des mesures de sécurité décrites au paragraphe 6.4 :

- Exigences de sécurité au niveau des accès physiques,
- Exigences de sécurité au niveau de l'exploitation du système,
  - Procédures d'exploitation,
  - Formation des administrateurs,
  - Assistance aux utilisateurs,
  - Procédures de sauvegardes et restaurations,
  - Réaction en cas d'indisponibilité du site principal,
  - Mise à jour d'un équipement de secours (spare),
  - Mise en service d'un équipement de secours (spare),
  - Gestion des mots de passe,
  - Gestion des audits et des alarmes,
  - Lignes directrices pour administrer les fonctions de sécurité.

5.3.1 Exigences de sécurité au niveau des accès physiques

TOP/PAC_APH	**Contrôle et protection des accès physiques au système**
TOP/PAC_APH.1	Les accès physiques au système doivent être contrôlés et protégés
Audit:	*Accès contrôlé et protection des accès physiques du système.*

5.3.2 Exigences de sécurité au niveau de l'exploitation du système

TOP/OPE_PRO.1	**Contrôle de l'existence des procédures d'exploitation**
TOP/OPE_PRO.1.1	Toutes les procédures d'exploitation doivent être décrites.
Audit:	*Toutes les procédures d'exploitation.*

TOP/OPE_FOR.1	**Contrôle de la formation des administrateurs aux procédures d'exploitation.**
TOP/OPE_FOR.1.1	Les procédures d'exploitation doivent être connues et appliquées par les administrateurs.
Audit:	*Connaissance et application des procédures d'exploitation par les administrateurs..*

TOP/OPE_AST.1	**Permanence des administrateurs**
TOP/OPE_AST.1.1	Un service d'assistance par numéro d'appel téléphonique et messagerie électronique est assuré pendant des périodes (plages horaires et jours) définies en fonction du contrat du client.
Audit:	*Demande d'assistance par numéro d'appel téléphonique et messagerie électronique.*

TOP/OPE_SSY.1	**Procédures de sauvegarde des données.**
TOP/OPE_SSY.1.1	Une procédure de sauvegarde synchronisée des données du système et des données de clients doit être mise en place.
Audit:	*Existence et application de cette procédure.*

TOP/OPE_RES.1	**Procédures de sauvegarde et restauration des données.**
TOP/OPE_RES.1.1	Une procédure de restauration des données du système et des données de clients doit être mise en place.
Audit:	*Existence et application de cette procédure.*

TOP/OPE_IND.1	Réaction en cas d'indisponibilité du site principal.
TOP/OPE_IND.1.1	Le système d'administration et de supervision doit détecter l'indisponibilité du site principal, Une procédure de basculement du site principal sur le site de secours doit exister, fonctionner et être appliquée par les administrateurs.
Audit:	*Détection, application de la procédure de basculement du site principal sur le site de secours.*

TOP/OPE_REP.1	Réplication des équipements en secours (spare).
TOP/OPE_REP.1.1	La modification d'un équipement doit être répercutée sur l'équipement en secours (*spare*).
Audit:	*application de la procédure de mise à jour.*

TOP/OPE_MIS.1	Mise en service d'un équipement en secours (spare).
TOP/OPE_MIS.1.1	La défaillance d'un équipement doit entraîner la mise en service de l'équipement en secours (*spare*).
Audit:	*application de la procédure de mise en service d'un équipement en secours (spare).*

TOP/OPE_GMP.1	Gestion des mots de passe.
TOP/OPE_GMP.1.1	La gestion des mots de passe doit couvrir tous les comptes, avec des règles sur la syntaxe des mots de passe et leur renouvellement pour ne pas faciliter leur découverte par des attaquants.
Audit:	*Existence et application des procédures de gestion des mots de passe.*

TOP/OPE_GAA.1	Gestion des audits et des alarmes.
TOP/OPE_GAA.1.1	La gestion des audits et des alarmes doit être accompagnée par des actions des administrateurs : contrôle du service, basculement sur un équipement spare.
Audit:	*Existence et application des procédures d'analyse des audits et de traitement des alarmes.*

TOP/OPE_LDA.1	Lignes directrices pour l'administration des fonctions de sécurité.
TOP/OPE_LDA.1.1	Un ensemble de document régissent l'administration des fonctions de sécurité: : • Procédure de consultation des fichiers de log des firewalls • procédure de création d'un compte administrateur • réglementation des accès physiques aux sites • liste des personnels habilités aux interventions sur le système, • réglementation de l'hébergeur pour l'accès au site principal.
Audit:	*Existence et application des procédures et des documents.*

Chapitre 6

6 Spécifications résumées du système

Ce chapitre comprend :
- Une définition des fonctions de sécurité TI qui satisfont les SRF identifiées,
- En option, des références aux mécanismes ou techniques de sécurité utilisées pour implémenter les fonctions de sécurité TI,
- Une définition des mesures d'assurance qui satisfont les exigences d'assurance identifiées.

Le document [15408] exige que ces spécifications fournissent un moyen de tracer les fonctions de sécurité TI vis à vis de tous les mécanismes ou fonctions de sécurité référencées par la cible de sécurité.

6.1 Fonctions de sécurité TI du système

Les fonctions de sécurité TI doivent couvrir toutes les SFR et chaque fonction de sécurité TI doit pouvoir être mise en correspondance avec au moins une SFR.
Les fonctions de sécurité sont spécifiées en utilisant les rubriques recommandées par [ITSEC] , à un niveau de détail équivalent de celui des classes de fonctionnalité présentées dans ce document.
Les fonctions de sécurité peuvent porter sur le service et sur le système.
- Le service comprend les applications qui rendent le service VPN administré, c'est à dire principalement les applications BSS, OSS et gestion des données (ORACLE).
- Le système comprend les matériels (machines de traitement, équipements réseaux) et les logiciels (exemple systèmes d'exploitation, système d'administration, sauvegarde, etc.) qui supportent les applications.

6.1.1 Identification-authentification

Identification	Fonction	Identification et authentification
IAU.1	Identification et authentification d'un utilisateur du service (gestionnaire, responsable de site, abonné, administrateur)	Avant toute action. Les utilisateurs du service (i.e. gestionnaires, responsables de site, abonnés) doivent s'identifier avant que toute action soit autorisée par les fonctions de sécurité du système.
IAU.2	Identification et authentification d'un administrateur du système et des services système.	Avant toute action. Les utilisateurs doivent s'authentifier avant que toute action soit autorisée par les fonctions de sécurité de la TOE.
IAU.3	Re-authentification d'un utilisateur du service (ex gestionnaire, responsable de site, abonné).	Les utilisateurs doivent se ré-authentifier au bout d'un délai maximum d'inactivité du poste de travail.
IAU.4	Re-authentification d'un administrateur du système et des services système.	Les utilisateurs doivent se ré-authentifier au bout d'un délai maximum d'inactivité du poste de travail.

Tableau 24 : Identification et authentification

6.1.2 Contrôle d'accès

Les fonctions décrites sont au niveau des spécifications de la classe F-C1 dérivée des exigences fonctionnelles de la classe C1 du TCSEC Américain [TCSEC] augmentées par les fonctions de contrôle d'accès au système .

Identification	Fonction	Contrôle d'accès
CAC.1	Les droits d'accès au service des administrateurs, des gestionnaires, responsables de sites et abonnés sont gérés en fonction de leur rôle.	Les différents rôles avec des droits croissants sont : • Abonné • Responsable de site • Gestionnaire • Gestionnaire privilégié • Administrateur • Administrateur privilégié Les fonctions du service accessibles par les différents rôles sont décrites dans le tableau 12.
CAC.2	Etanchéité entre les données commerciales des utilisateurs	• Une base de données est définie par opérateur, avec un profil de gestion associé. L'étanchéité est garantie par les fonctions de contrôle d'accès aux bases effectué par Oracle.

CAC.3	Les droits d'accès au système des administrateurs ou administrateurs privilégiés sont gérés en fonction de leur rôle et des comptes administrateurs qui leurs sont attribués.	Les différents rôles avec des droits croissants sont :
		• Administrateur
		• Administrateur privilégié
		
		Les fonctions du système accessibles par les différents rôles sont décrites dans le tableau 14.
		
		• Supervision.
		  • Surveillance de l'activité des machines et des équipements de réseau
		  • Consultation des fichiers de log.
		• Administration
		  • Configuration des paramètres de fonctions de sécurité
		  • Création de comptes administrateurs
		  • Consultation des fichiers de log
		  • Modification des fichiers de log
		  • Administration des services système .
		  • Supervision des services système

CAC.4	Les droits pour un paquet Internet d'entrer ou sortir du système sont définis sous la forme de règles de filtrage .	• Seuls les trafics entrants UDP/514, HTTP, HTTPS et FTP sont autorisés • Seuls les trafics sortants HTTPS, FTP, SSH et SCP sont autorisés

Tableau 25: Contrôle d'accès

6.1.3 Imputabilité

Identification	Fonction	Imputabilité
IMP.1	Enregistrement des évènements auditables de type service.	A chaque événement doivent être associés la date et l'heure de son occurrence, ainsi que l'identité de l'entité l'ayant engendré.
IMP.2	Enregistrement des évènements auditables de type système.	A chaque événement doivent être associés la date et l'heure de son occurrence, ainsi que l'identité de l'entité l'ayant engendré.
IMP.5	Protection des fichiers d'audit de type service en cas de saturation.	• Sous systèmes techniques SES (BSS) et d'administration (SSA) • Sous système technique SMS (OSS) • Sous système de gestion des données Oracle. • Firewall • Serveur de certificats
IMP.6	Protection des fichiers d'audit de type système en cas de saturation.	• Systèmes Linux (machines de traitement, firewalls, machines • Système AIX • Système HACMP • Système Windows 2000

Tableau 26: Imputabilité

6.1.4 Audit

Outils d'analyse et alarme

Identification	Fonction	Audit
AUD.1	Outils d'analyse des audits de sécurité de type service	• Systèmes techniques SES (BSS) et SMS (OSS) • Oracle • Serveur de certificat • Firewall
AUD.2	Outils d'analyse des audits de sécurité de type système	• Système UNIX AIX • Système HACMP • Systèmes Linux • Système Windows
AUD.3	Supervision des machines des équipements de réseau et des services système.	• Système UNIX AIX • Système HACMP • Systèmes Linux • Système Windows
AUD.4	Surveillance mutuelle et basculement automatique HACMP	• Système HACMP
AUD.5	Production d'évènements d'alarmes	• Machines Linux et équipements de réseau • Machines AIX • Oracle • Windows 2000.

Tableau 27: Audit

6.1.5 Réutilisation d'objet

Problème d'informations critiques rémanentes: mots de passe déchiffrés, clés privées

Identification	Fonction	Réutilisation d'objet

Tableau 28 : Réutilisation d'objet

6.1.6 Fidélité

Identification	Fonction	Fidélité
FID.1	Protection des transferts de données internes à l'intérieur du système.	Le protocole Net8 d'Oracle garantit l'intégrité des données transférées entre les machines de traitement et les machines de gestion des données .
FID.2	Sauvegarde globale et synchronisation des sites	Une sauvegarde des systèmes et des données du site principal et du site de secours est réalisée chaque nuit localement et à distance.
FID. 3	Restauration de la configuration des machines	Des fonctions de restauration permettent de restaurer partiellement ou en totalité les configurations des machines et des services d'un site à l'aide des données de sauvegarde des sites
FID.4	Prévention et détection des erreurs d'intégrité référentielles	Supervision de l'intégrité des données rangées dans des bases.

Tableau 29: Fidélité

6.1.7 Fiabilité de service

La classe de référence est F_AV [TCSEC]

Identification	Fonction	Fiabilité de service
FDS.1	Dans chaque machine, duplication des données systématique sur deux unités de stockage ; technique RAID1	La défaillance d'une unité de stockage est transparente au service.
FDS.2	Fonctionnement HA (High Availability) avec basculement automatique	La défaillance d'une machine de traitement applicatif, firewall, machine de gestion des données, machine d'administration entraîne le basculement automatique sur une machine de secours en service.
FDS.3	Réplication	Une machine ou un équipement de réseau en secours pré-configurée est prévu en cas de défaillance du matériel en fonctionnement.
FDS.4	Basculement de site	En cas de détection d'indisponibilité du site principal, la procédure de basculement sur le site de secours est appliquée, une procédure doit également être appliquée sur les équipements VPN qui modifie les adresses IP du serveur de certificat et du serveur NTP pour fournir les adresses IP du serveur de certificat et du serveur NTP du site de secours.

Tableau 30: Fiabilité de service

6.1.8 Echanges de données

Les échanges de données entre le système et l'extérieur sont sécurisés par des fonctions d'authentification, confidentialité réalisées par l'utilisation de fonctions cryptographiques.
Ces échanges concernent :

- Les échanges entre les abonnés, gestionnaires et responsables de site et le système via des consoles Web ou des *wizards* de configuration.
- Les échanges entre les équipements VPN et le système.

Identification	Fonction	Echange de données
ECD.1	Fonction de sécurisation des échanges de données entre une console Web et la TOE	• Ces fonctions sont utilisées pour les échanges commerciaux entre les gestionnaires et gestionnaires privilégiés et la TOE. .
ECD.2	Fonction de sécurisation des échanges de données entre les wizards de configuration et la TOE	• Ces fonctions sont utilisées pour les échanges effectués lors de l'approvisionnement d'un équipement VPN.
ECD.3	Fonction de sécurisation des commandes et des données entre un équipement VPN et la TOE	• Ces fonctions sont utilisée pour sécuriser la connexion de la TOE à un équipement VPN

Tableau 31: Echange de données

6.2 Mécanismes et techniques de sécurité

6.2.1 Protection des usagers

Lorsqu'un utilisateur se connecte au système via une console Web, le système lui communique son certificat pour lui permettre une vérification lui assurant qu'il s'adresse bien au système VPN administré.

6.2.2 Protection des accès au système

Cette protection est basée sur :
- Des droits assignés à des rôles : administrateur privilégié, administrateur, gestionnaire privilégié, gestionnaire, responsable de site, abonné.
- Le protocole de sécurité *SSL* utilisé par le protocole *HTTPS* de communication mis en œuvre respectivement entre :
  - des consoles *Web* et le système. Ces consoles sont opérées par des administrateurs privilégiés du service, des gestionnaires privilégiés, des gestionnaires, des responsables de site et des abonnés.
  - des *wizards* de configuration d'équipement *VPN* et le système.
    Noter que les *wizards* de configuration sont utilisés par des responsables de site.

6.2.3 Administration du système

L'administrateur privilégié peut créer plusieurs administrateurs. Quand un administrateur est créé, le système génère un identifiant unique et un mot de passe qui doit être communiqué par l'administrateur privilégié à l'administrateur qui vient d'être créé.

6.2.4 Administration du service

Pour créer une étanchéité entre les opérateurs, l'administrateur privilégié du service crée un gestionnaire privilégié pour chaque opérateur. Un gestionnaire privilégié peut créer via une console Web connectée au système, un ou plusieurs gestionnaires et il doit communiquer à chaque gestionnaire un identifiant et un mot de passe qui sont générés par le système pour ce gestionnaire lors de sa création.

Chaque gestionnaire peut créer à partir d'une console Web connectée au système, un ou plusieurs abonnés et un ou plusieurs sites pour chaque abonné. Pour chaque abonné ou site créé, le système retourne au gestionnaire un identifiant et un mot de passe que le gestionnaire devra communiquer à l'abonné et au responsable de site.
En effet un abonné ou un responsable de site a besoin d'un identifiant et d'un mot de passe pour se connecter au système.

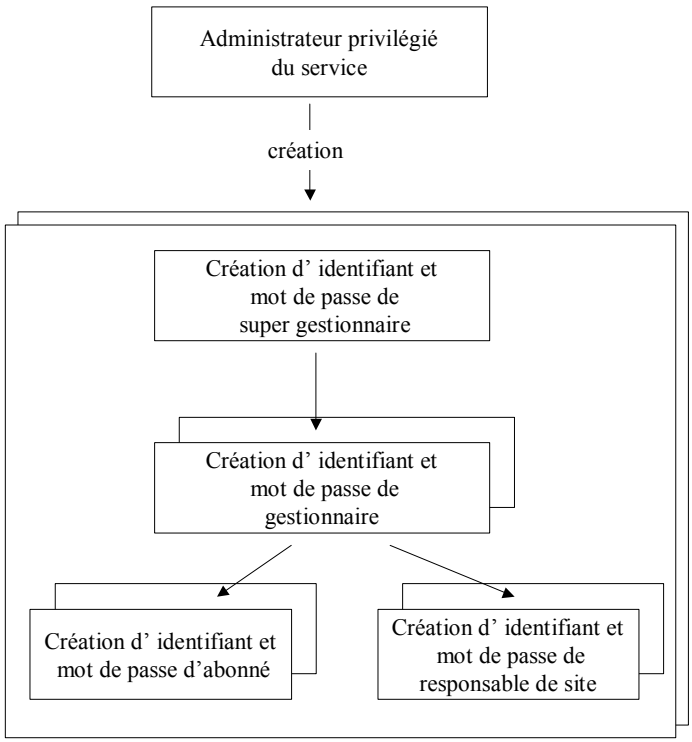

Tableau 32 : Relations entre les acteurs et leurs dispositifs de protection

6.2.5 Authentification des équipements VPN par la TOE

Lorsqu'un gestionnaire crée un site, il fournit au système une identification unique (ID) du routeur ainsi que son login et mot de passe.

6.2.6 Approvisionnement sécurisé d'un équipement VPN

Le système fournit un service d'approvisionnement pour les équipements VPN.
Ce service est utilisé pour permettre la mise en service sur site d'un équipement VPN.
Ce service est fourni par un wizard de configuration qui se connecte localement et via une interface LAN à l'équipement VPN.

6.2.7 Disponibilité des matériels du système

Pour augmenter la disponibilité du système en cas de défaillance ponctuelle d'un matériel (machine, composant ou équipement de réseau), toutes les machines, les consoles, les contrôleurs et les unités de stockage ainsi que tous les équipements de réseau sont doublés soit sur site soit à distance pour éviter des SPOF (Single Point of Failure).

Pour minimiser le temps d'indisponibilité lié à une défaillance, la grappe de machines de gestion de données utilise une technique HA basée sur une surveillance mutuelle et un dispositif de détection de défaillance. En cas de détection de défaillance d'une machine de la grappe, la gestion des bases de données de la machine défaillante bascule sur la machine en état de marche.

6.2.8 Etanchéité des données utilisateurs

- Les machines bases de données ne sont pas accessibles de l'extérieur.
- Chaque opérateur a ses données dans une base qui lui est affectée.
  L'accès à une base est protégé en interne par un login/mot de passe utilisé par les programmes du serveur applicatif.

6.3 Mesures d'assurance

Le document ISO [15408] exige de la spécification résumée de la TOE que soient tracées les mesures d'assurance vis à vis des exigences d'assurance afin qu'il soit démontré que toutes les exigences d'assurance sont satisfaites. L'approche recommandée par [15446] est de fournir une mise en correspondance de la documentation ou de preuves que le développeur a l'intention de fournir avec les exigences appropriées.

Exigences appropriées	Composant	Documentation et preuves fournies
Gestion de numéros de versions	ACM_CAP.1	Document de gestion de configuration
Installation, génération, et procédures de démarrage	ADO_IGS.1	Document des procédures d'installation, configuration et démarrage
Spécification fonctionnelle informelle	ADV_FSP.1	Document spécifications fonctionnelles
Démonstration de correspondance informelle	ADV_RCR.1	
Guides de l'administrateur	AGD_ADM.1	Guide d'exploitation du système [GUIDSY] Guide d'exploitation du service [GUIDESE]
Guides utilisateur	AGD_USR.1	Guide du gestionnaire [GUIDGES] Guide d'installation et de configuration d'appareil VPN [GUIDICA] Guide de l'abonné [GUIDABO]
Test indépendant- Conformité	ATE_IND.1	Mise à disposition du système VNMS avec deux équipements VPN 6wind
Analyse indépendante de vulnérabilité	ATE_VLA.2	Document chemins d'attaque et vulnérabilités

Tableau 33 : Documentation et preuves pour les mesures d'assurance

6.4 Mesures de sécurité non TI

Les mesures de sécurité permettent de garantir les objectifs non techniques.

Identification	Mesures de sécurité non TI	Description
APH.1	Accès physiques	Les accès physiques au système doivent être contrôlés et protégés
FOR.1	Formation	Les administrateurs doivent être formés pour utiliser les outils de supervision d' administration et de maintenance.
AST.1	Astreintes	Actuellement aucune astreinte n'est mise en œuvre pour le système VNMS. Lors de projets particuliers ou lors d'opérations lourdes sur la plate forme VNMS, un mécanisme d'astreinte peut être mis en place,. Ces astreintes permettent alors d'assurer une permanence des administrateurs en dehors des heures ouvrables et des jours fériés.
SSY.1	Procédures de sauvegarde et synchronisation	Tous les jours l'ensemble des serveurs de la plate forme du site principal stockent leurs données sur le serveur de sauvegarde.
RES.1	Procédures de restauration	Les procédures de restauration d'une machine sont partielles et nécessitent un système d'exploitation minimum sur CD_ROM
IND.1	Réaction en cas d'indisponibilité du site principal	En cas de non réponse sur une console d'administration à distance, la liaison inter site est vérifiée.

		Si la liaison inter site ne fonctionne plus, un basculement manuel de la liaison inter site sur une liaison RNIS est effectué. Si le problème persiste, une intervention sur site est entreprise. Si sur le site, un incident majeur est constaté, une procédure de basculement est entreprise sur le site de secours
REP.1	Réplication des équipements « spare »	Dès qu'un équipement est modifié, la mise à jour est systématiquement effectuée sur l'équipement « spare », conformément au processus de mise en production de toute modification logicielle.
MIS.1	Mise en service d'un équipement « spare »	Une procédure de basculement manuel est appliquée.
GMP.1	Gestion des mots de passe système	La liste des comptes système et services système est décrite dans le tableau 14. La longueur des mots de passe est de 12 caractères pour les compte système privilégié et système. Sur la plate forme d'exploitation, les mots de passe de root sont les mêmes pour tous les systèmes et sont renouvelés tous les trois mois.
GAA.1	Gestion des audits et des alarmes	Les alarmes de fonctionnement possèdent 3 niveaux : normal, avertissement(Warning) ou critique. Ces alarmes sont centralisées sur une console reliée à tous les équipements réseaux et systèmes.
LDA.1	Lignes directrices pour administrer les fonctions de sécurité ; elle sont consignées dans le guide administrateur ;	Les logs du firewall sont consultés tous les matins. La création d'un compte nécessite une demande formelle auprès de l'administrateur privilégié. Dans le cadre de la protection industrielle, les accès sur le site principal et de secours sont réglementés.

Tableau 34 : Mesures de sécurité non TI

Annexe 1: Réglementation des prestations et moyens de cryptologie

Ce tableau fait une synthèse de la réglementation Française actuellement en vigueur pour l'utilisation de clés cryptographiques.

Opérations	Applications			
	Authentification Signature Intégrité	Confidentialité *Longueur de clé*		
		< ou = 40 bits	< ou = 128 bits	>128 bits
Fourniture	Soumise à déclaration simplifiée	Soumise à déclaration	Soumise à déclaration	Soumise à autorisation
Importation*	LIBRE	LIBRE	LIBRE*	Soumise à autorisation
Utilisation	LIBRE	LIBRE	LIBRE*	AUTORISEE*

*
Libre dans tous les cas si provenance d'un Etat appartenant à la Communauté européenne ou étant partie à l'accord instituant l'Espace économique européen.

*
A condition, soit que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, un fournisseur ou un importateur, soit que lesdits matériels ou logiciels soient exclusivement destinés à l'usage privé d'une personne physique ;

Sinon, une déclaration d'utilisation personnelle doit être adressée à la DCSSI

*
A condition que lesdits matériels ou logiciels aient fait l'objet d'une autorisation de **fourniture en vue d'une utilisation générale** ;

Sinon, une demande d'autorisation d'utilisation personnelle doit être adressée à la DCSSI

Annexe 2 : Identification des opérations effectuées sur les composants d'exigences fonctionnelles de sécurité des TI

Classe FAU

FAU_ARP.1 : : Security alarms

FAU_ARP.1.1 The TSF shall take [assignment: list of the least disruptive actions] upon detection of a potential security violation.

Itération SYS
Affectation list of the least disruptive actions := **afficher un message d'alerte sur la console système ou envoyer un mail aux administrateurs**

FAU_GEN.1 : : Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection: minimum, basic, detailed, not specified] level of audit; and
c) [assignment: other specifically defined auditable events].

Itération TOP
Sélection minimum, basic, detailed, not specified := **not specified**
Affectation other specifically defined auditable events := **les événements figurant dans la rubrique 'audit' associée à chaque composant d'exigence fonctionnelle de sécurité inclus dans cette cible de sécurité**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: other audit relevant information]

Itération TOP
Affectation other audit relevant information := **les informations d'audit mentionnées dans les rubriques 'audit' associées aux composants d'exigence fonctionnelle de sécurité inclus dans cette cible de sécurité**

FAU_SAA.1 : : Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

Itération SYS
pas d'opérations effectuées

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation;
b) [assignment: any other rules].

Itération SYS
Affectation subset of defined auditable events := **aucun événement**
Affectation any other rules := **- Détection des défaillances par 'ping' : la TSF vérifie l'activité des machines et équipements du système à l'aide requêtes ICMP de type 'echo'. Une machine ou un équipement qui ne répond plus est présumé défaillant.** **- Alarmes de sécurité : la TSF remonte une alarme pour les événements paramétrés comme tels au niveau du firewall,** **- Erreurs d'intégrité Oracle : En cas de détection d'erreur d'intégrité référentielle, Oracle rend un code retour exploité par le sous système technique SES.**

6.4.1 FAU_SAR.1 : Audit review

FAU_SAR.1.1 The TSF shall provide [assignment: authorised users] with the capability to read [assignment: list of audit information] from the audit records.

Itération TOP
Affectation authorised users := **administrateurs privilégiés (voir tableau 13)**
Affectation list of audit information := **la totalité des informations d'audit**
Raffinement audit records := **fichiers de log**

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the users to interpret the information.

Itération TOP
Raffinement audit records := **fichiers de log**
Raffinement the user := **Tous les administrateurs (voir tableau 13).**

6.4.2 FAU_STG.2 : Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

Itération TOP
Pas d'opérations effectuées

FAU_STG.2.2 The TSF shall be able to [selection: prevent, detect] modifications to the audit records.

Itération TOP
Sélection prevent, detect := **prevent**

FAU_STG.2.3 The TSF shall ensure that [assignment: metric for saving audit records] audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, attack].

Itération TOP
Affectation metric for saving audit records := **les volumes suivants : - pour le serveur de certificats : les enregistrements d'audit les plus récents, - pour les serveurs de données : les derniers enregistrements d'audit avant l'arrêt des fonctions d'audit.**
Sélection audit storage exhaustion, failure, attack := **audit storage exhaustion**

6.4.3 FAU_STG.4: Prevention of audit data loss

FAU_STG.4.1 The TSF shall [selection: *'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records*'] and [assignment: *other actions to be taken in case of audit storage failur*e] if the audit trail is full.

Itération TOP
Sélection 'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records' := **ignore, overwrite**

Itération TOP
Affectation *other actions* := **le serveur de certificats émet un message d'alarme quand le fichier log approche de la saturation** Raffinement *the audit trail is full* := **fichier de log**

Classe FDP

FDP_ACC.1 : Subset access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

Itération SRV
Affectation access control SFP := **la politique de contrôle d'accès aux services applicatifs**
Affectation list of subjects, objects, and operations among subjects and objects covered by the SFP := **les opérations effectuées par les utilisateurs à l'aide des services applicatifs des sous-systèmes suivants: les serveurs de données gérant les bases opérateurs, le BSS, l'OSS et le serveur de certificat**

Itération SYS
Affectation access control SFP := **la politique de contrôle d'accès aux fonctions système**
Affectation list of subjects, objects, and operations among subjects and objects covered by the SFP := **les opérations effectuées par les administrateurs à l'aide des fonctions des systèmes d'exploitations des machines composant la TOE**

FDP_ACF.1 : Security attribute based access control

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

Itération SRV
Affectation access control SFP := **la politique de contrôle d'accès aux services applicatifs**
Affectation security attributes, named groups of security attributes:= **- le rôle des utilisateurs, - le préfixe d'opérateur des gestionnaires privilégiés, gestionnaires, responsables de site et abonnés, - l'identité des abonnés.**

Préciser rapidement voir 5.1.3

Itération SYS
Affectation access control SFP := **la politique de contrôle d'accès aux fonctions système**
Affectation security attributes, named groups of security attributes := **- le rôle des administrateurs, - les comptes qu'ils utilisent pour effectuer les opérations.**

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

Itération SRV
Affectation rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects := **les règles décrites dans le** Erreur ! Source du renvoi introuvable.
Raffinement controlled subjects := **un utilisateur contrôlé**
Raffinement controlled objects := **un service applicatif contrôlé**

Itération SYS
Affectation rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects := **les règles sont décrites dans le tableau 14.**
Raffinement controlled subjects := **un administrateur contrôlé**
Raffinement controlled objects := **un système d'exploitation contrôlé**

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

Itération SRV
Affectation rules, based on security attributes, that explicitly authorise access of subjects to objects := **aucune règle**

Itération SYS
Affectation rules, based on security attributes, that explicitly authorise access of subjects to objects := **aucune règle**

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

Itération SRV
Affectation rules, based on security attributes, that explicitly deny access of subjects to objects := **Les règles suivantes: - les**

gestionnaires privilégiés, gestionnaires et responsables de site d'un opérateur n'ont pas accès aux bases des autres opérateurs, - les abonnés n'ont pas accès aux informations des autres abonnés. Raffinement subject : opérateur Raffinement object : les bases opérateur

Itération SYS
Affectation rules, based on security attributes, that explicitly deny access of subjects to objects := **aucune règle**

FDP_IFC.1 : Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

Itération NTW
Affectation information flow control SFP := **la politique de contrôle des flux d'information Internet au niveau réseau/transport**
Affectation list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP := **les datagrammes IP d'Internet vers la TOE ou de la TOE vers Internet**

FDP_IFF.1 : Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes].

Itération NTW
Affectation information flow control SFP := **la politique de contrôle des flux d'information Internet au niveau réseau/transport**
Raffinement subject := **les machines émettrices et destinataires de part et d'autre du firewall**
Raffinement information := **les datagrammes IP**
Affectation the minimum number and type of security attributes := **- adresse IP, - type de protocole transport, - numéro de port TCP ou UDP**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

Itération NTW
Raffinement controlled subject := **une machine émettrice**
Raffinement controlled information := **un datagramme IP à transiter à travers le firewall d'une machine émettrice vers une machine destinataire**
Affectation for each operation, the security attribute-based relationship that must hold between subject and information security attributes := **- les trafics entrants UDP/514, HTTP, HTTPS et FTP (port 21) sont les seuls autorisés, - les trafics sortants HTTPS, FTP, SSH et SCP sont seuls autorisés.**

FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].

Itération NTW
Affectation additional information flow control SFP rules:= **aucune règle**

FDP_IFF.1.4 The TSF shall provide the following [assignment: list of additional SFP capabilities].

Itération NTW
Affectation list of additional SFP capabilities := **aucune capacité de traitement**

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

Itération NTW
Raffinement information flow:= **un datagramme IP transitant à travers le firewall d'une machine émettrice vers une machine destinataire**
Affectation rules, based on security attributes, that explicitly authorise information flows := **une connexion de donnée FTP peut passer à travers le firewall si elle est correcte vis-à-vis du contexte d'une session FTP active.**

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

Itération NTW
Raffinement information flow:= **un datagramme IP transitant à travers le firewall d'une machine émettrice vers une machine destinataire**
Affectation rules, based on security attributes, that explicitly deny information flows := **"tous les flux d'information qui ne sont pas explicitement autorisés sont interdits".**

FDP_ITT.1 : Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.

Itération SRV
Affectation access control SFP(s) and/or information flow control SFP(s) := **la politique de maintien de l'intégrité des données opérateurs**
Sélection disclosure, modification, loss of use := **modification**
Raffinement user := **opérateurs**
Raffinement physically-separated parts of the TOE := **les serveurs applicatifs (OSS et BSS) et les serveurs de données**

FDP_SDI.2 : Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [assignment: integrity errors] on all objects, based on the following attributes: [assignment: user data attributes].

Itération SRV
Raffinement user := **opérateurs**
Raffinement within the TSC := **au sein des serveurs de données**
Raffinement on all objetcs : sur toutes les bases opérateur
Affectation integrity errors := **erreurs d'intégrité référentielle**
Affectation user data attributes := “primary keys”, “foreign keys”, “check constraints” définies dans le schéma de la base .

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

Itération SRV
Raffinement data integrity error:= **une erreur d'intégrité référentielle**
Affectation action to be taken:= En cas de détection d’erreur d’intégrité référentielle, Oracle rend un code retour exploité par le sous système technique SES.

Classe FIA

FIA_ATD.1 : User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

Itération SRV
Raffinement individual users := **les gestionnaires privilégiés, gestionnaires, responsables de site et abonnés**
Affectation list of security attributes := **- préfixe d'opérateur, - pour les abonnés : identité de l'abonné**

Itération SYS

Raffinement individual users := **les administrateurs et administrateurs privilégiés**
Affectation list of security attributes := **compte utilisé pour effectuer des opérations**

FIA_UAU.2 : User authentication before any action

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

Itération TOP
pas d'opérations effectuées

FIA_UAU.6 : Re-authenticating

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

Itération TOP
Affectation list of conditions under which re-authentication is required := **lorsque leur console a dépassé le délai maximum d'inactivité**
Raffinement ajout de **- Pour les utilisateurs distants (console Web, wizard de configuration), le délai maximum d'inactivité est de cinq minutes - Pour les consoles des administrateurs sur le site principal ou le site de secours, le délai maximum d'inactivité est de trois minutes**

FIA_UID.2 : User identification before any action

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

Itération TOP
pas d'opérations effectuées

Classe FMT

FMT_SMR.1 : Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles].

Itération TOP
Affectation the authorised identified roles := **- administrateur privilégié, - administrateur, - gestionnaire privilégié, - gestionnaire, - responsable de site, - abonné.**

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

Itération TOP
pas d'opérations effectuées

Classe FPT

FPT_FLS.1 : Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF].

Itération TOP
Affectation list of types of failures in the TSF := **- défaillance des unités de stockage de toutes les machines, - panne des machines de traitement applicatif HA (les serveurs de données et le firewall), - panne des machines ou des**

équipements non HA, - indisponibilité du site principal.

FPT_STM.1 : Reliable time stamps

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

Itération TOP
pas d'opérations effectuées

Classe FRU

FRU_FLT.2 : Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur :[assignment: list of type of failures].

Itération TOP
Affectation list of type of failures := **- défaillance des unités de stockage de toutes les machines, - panne des machines de traitement applicatif HA (les serveurs de données et le firewall), - panne des machines ou des équipements non HA, - indisponibilité du site principal.**

Classe FTP

FTP_ITC.1 : Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

Itération NTW
Raffinement trusted IT product := **les consoles Web, les wizards de configuration et les équipements VPN administrés**
Raffinement assured identification := **authentification mutuelle**

FTP_ITC.1.2 The TSF shall permit [selection: the TSF, the remote trusted IT product] to initiate communication via the trusted channel.

Itération NTW
Sélection the TSF, the remote trusted IT product := **the remote trusted IT product** suivi de Raffinement the remote trusted IT product := **les consoles Web, les wizards de configuration et les équipements VPN administrés**

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

Itération NTW
Affectation list of functions for which a trusted channel is required := **les sessions d'administration des équipements VPN**