CrossinG®

Cible de sécurité

Date : 04/08/2022
Version du produit : 2.1.2
Ref : BTSSI-CG-2-1_CSPN_Cible
Révision : U

www.chapsvision.fr

CHAPSVISION
DATA MAKE SENSE

A Révisions du document

Date	Révision	Auteur	Description
04/08/2022	U	ChapsVision	Prise en compte des remarques de l'ANSSI.
27/07/2022	T	ChapsVision	Prise en compte des remarques de l'ANSSI, mise à jour mentions & logos ChapsVision, mise à jour description matérielle D.3.1 (version legacy plus supportée, options matérielles simplifiées sans nomenclature Bertin IT).
27/11/2020	S	Bertin IT	Prise en compte des remarques de l'ANSSI
21/09/2020	R	Bertin IT	Mise à jour du numéro de version produit : v2.1.2
14/08/2020	Q	Bertin IT	Mise à jour v2.1.1-B Bertin IT suite au RTE Amossys v2.1.1-A
15/07/2019	P	Bertin IT	Mise à jour v2.1.1 finale Bertin IT
17/06/2019	O	Bertin IT	Prise en compte des remarques de l'ANSSI du 29/05/19
12/04/2019	N	Bertin IT	Modifications liées au passage en version v2.1.1 et prise en compte des remarques de l'ANSSI
25/10/2018	M	Bertin IT	Prise en compte des remarques d'AMOSSYS
05/10/2018	L	AMOSSYS	Prise en compte des remarques de l'ANSSI et Bertin IT
19/09/2018	K	Bertin IT	Prise en compte des remarques de l'ANSSI
06/08/2018	J	AMOSSYS	Prise en compte des remarques de l'ANSSI
02/08/2018	I	Bertin IT	Prise en compte des remarques de l'ANSSI
25/07/2018	H	AMOSSYS	Prise en compte des remarques de l'ANSSI
06/06/2018	G	AMOSSYS	Prise en compte des informations fournies par Bertin IT
31/05/2018	F	Bertin IT	Mise à jour
23/05/2018	E	AMOSSYS	Mise à jour
15/03/2018	D	Bertin IT	Mise à jour CrossinG v1.3
02/10/2017	C	Bertin IT	Version préliminaire
13/09/2017	B	Bertin IT	Revue interne
01/09/2017	A	Bertin IT	Version initiale

B Sommaire

C Introduction

C.1 Objectif du document

Ce document est réalisé dans le cadre de l'évaluation CSPN du produit CrossinG® version 2.1.2, développé par la société **ChapsVision**.

La TOE[1] considérée est l'appliance matérielle CrossinG v2.1.2.

Ce document est soumis au contrôle technique et qualité d'AMOSSYS ainsi qu'à la validation de **ChapsVision**. Les mises à jour de ce document sont effectuées par l'équipe projet d'AMOSSYS.

C.2 Identification du produit

Libellé	Description
Organisation éditrice	CHAPSVISION
Lien vers l'organisation	www.chapsvision.fr
Nom commercial du produit	CrossinG®
Numéro de la version évaluée	CrossinG® v2.1.2
Catégorie du produit	Communication sécurisée

C.3 Terminologie

Acronyme	Définition
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Appliance matérielle	Equipement matériel indépendant comprenant un système logiciel intégré et permettant d'effectuer une ou des tâches spécifiques.
CIFS	« Common Internet File System » est un protocole de partage de fichiers sur les réseaux locaux de PC Windows.
FTP	« File Transfert Protocol » est un protocole de transfert de fichiers.

[1] *Target Of Evaluation*

LDAP	« Lightweight Directory Access Protocol » est un protocole réseau permettant l'interrogation de services d'annuaire.
MIB	« Management Information base » est un ensemble d'informations structuré sur une entité réseau.
NFS	« Network File System » est un protocole d'accès à des fichiers distants via un réseau.
Politique de sécurité	Les politiques de sécurité du produit sont définies comme un ensemble ordonné de règles et de traitements appliqués aux fichiers en vue de déterminer s'ils sont autorisés à transiter à travers la passerelle.
Réseau de confiance	Un réseau est dit de confiance si, du fait qu'il est sous le contrôle de l'exploitant de la ToE, la politique de sécurité interne n'implique pas qu'il faille se protéger des flux qui en proviennent.
SFTP	« SSH File Transfert Protocol » est un protocole de transfert de fichiers fonctionnant au-dessus de SSH.
SI	Système d'information : ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.
SNMP	« Simple Network Management Protocol » est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
SSH	« Secure Shell » est un protocole de communication sécurisé.
SYSLOG	Syslog est un protocole définissant un service de journaux d'événements d'un système informatique. C'est aussi le nom du format qui permet ces échanges.
ToE	Target Of Evaluation. Dans le cadre du document, la ToE fait référence à CrossinG® dans une configuration particulière (précisée en section D.4.1).

C.4 Documents applicables et de références

Référence	Titre
[QUALIF_ELEM]	Référentiel général de sécurité Processus de qualification d'un produit de sécurité - niveau élémentaire version 2.0
[CROSSING_SPD]	CrossinG® : définition fonctionnelle version 2.1 révision T, ref. BTSSI-CG-2-1_DefinitionFonctionnelle

[CROSSING_DEM]	CrossinG® : guide de démarrage version 2.1 révision J, ref. BTSSI-CG-2-1_GuideDemarrage
[CROSSING_CRY]	CrossinG® : guide cryptographique version 2.1 révision H, ref. BTSSI-CG-2-1_GuideCrypto
[CROSSING_ADM]	CrossinG® : guide d'administration version 2.1 révision N, ref. BTSSI-CG-2-1_GuideAdmin
[CROSSING_SUP]	CrossinG® : guide de supervision version 2.1 révision G, ref. BTSSI-CG-2-1_GuideSupervision
[CROSSING_SPE]	CrossinG® : spécification technique version 2.1 révision L, ref. BTSSI-CG-2-1_SpecificationTechnique
[CROSSING_VER]	CrossinG® – Fiche de version du produit version 2.1.2

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur :

- Bertin-IT-Safe&SmartITSolutions_FR.pdf
- Bertin-IT-CrossinG-v1.3-short.pdf
- BTSSI-CG-2-1_DefinitionFonctionnelle

D Description du produit

D.1 Description générale du produit

CrossinG® est une passerelle d'interconnexion destinée à permettre le transfert sécurisé de fichiers entre des réseaux dont les domaines opérationnels sont différents, par exemple : réseau public (Internet) / réseau isolé (Intranet, réseau sensible), SI de gestion / Système de Contrôle Industriel, etc.

Elle se présente sous la forme d'une *appliance* matérielle, fonctionnant comme un sas et disposant de 4 interfaces réseau physiques.

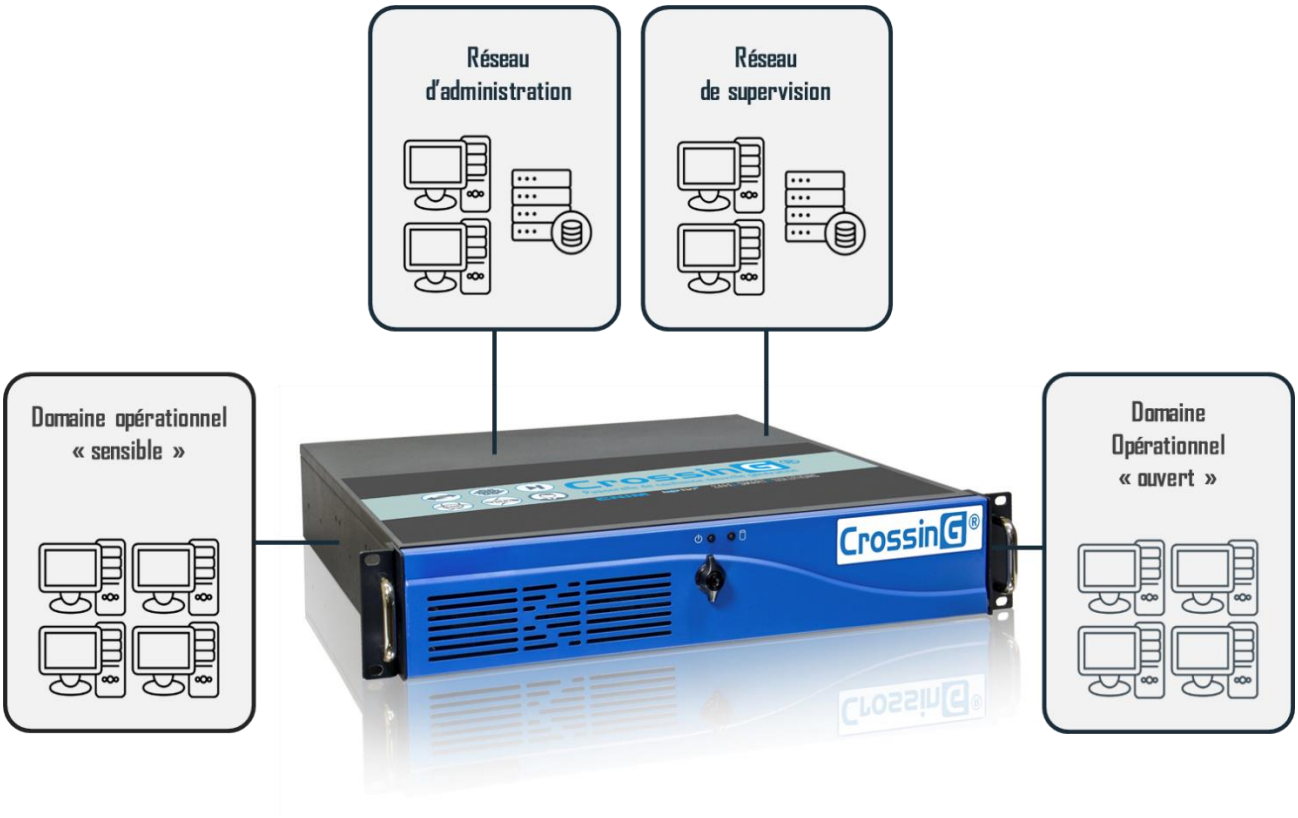

Figure 1 : Exemple de cas d'usage

Elle combine plusieurs mécanismes de sécurité durant les transferts de fichiers pour assurer la défense en profondeur des SI sensibles et des infrastructures critiques. Ces traitements visent à assurer que, d'une part, les fichiers qui entrent dans un SI sont sains et compatibles avec la politique de sécurité de l'organisation et que, d'autre part, ceux qui en sortent sont bien autorisés à sortir afin de lutter contre la fuite de données.

Les politiques de sécurité du produit sont définies comme un ensemble ordonné de règles et de traitements appliqués aux fichiers en vue de déterminer s'ils sont autorisés à entrer ou à sortir. CrossinG® permet de mettre en œuvre deux canaux de communication unidirectionnels indépendants et de configurer la passerelle soit en mode monodirectionnel, soit en mode bidirectionnel. Le cloisonnement en deux canaux de communication permet l'application d'une politique de sécurité distincte en fonction du sens de transfert des fichiers.

L'architecture de la passerelle peut se décomposer en 3 couches logicielles imbriquées :

- un hyperviseur de confiance assurant la gestion du matériel et les canaux de communication internes ;
- un ensemble de machines virtuelles cloisonnées, dédiées chacune à une fonction spécifique ;
- une chaîne logicielle de transferts, de traitements, d'administration et de supervision, répartie sur l'ensemble des machines virtuelles.

Bien que permettant des échanges bidirectionnels, la passerelle assure pour chaque sens de transfert un canal de communication interne unidirectionnel et une rupture protocolaire logicielle basée sur un mécanisme non réseau assuré par l'hyperviseur.

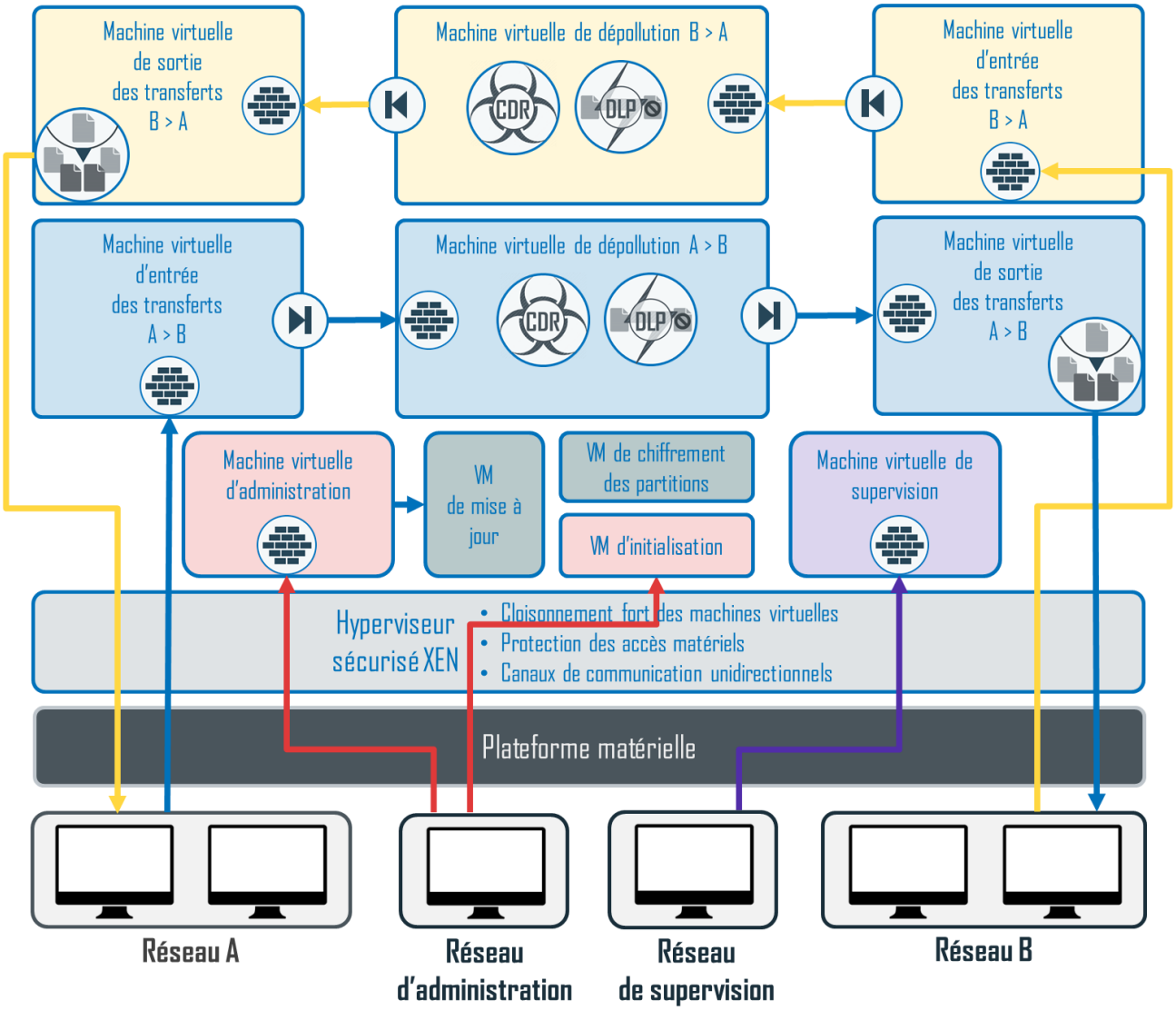

Figure 2 : Architecture logique de CrossinG (schéma simplifié)

Le socle de confiance, qui assure en particulier le cloisonnement des machines virtuelles et contrôle leurs accès aux ressources matérielles de la plateforme, est constitué d'un hyperviseur XEN configuré par ChapsVision de la manière suivante :

- utilisation de XSM FLASK ;
- retrait des modules inutiles de la configuration de Xen ;
- sécurisation du fonctionnement de Xenstore, afin d'éviter le détournement de son utilisation comme canal de communication ;
- mise en VM de Xenstore, via un stub domain.

Le mécanisme de transfert de données entre machines virtuelles est assuré par l'hyperviseur XEN et adapté par ChapsVision. Ce mécanisme, Argo, permet de fournir un support de diode logicielle acceptable aussi bien en termes de sécurité que de performance. Il est configuré par ChapsVision afin d'assurer des transferts en mode « push » unidirectionnels (en particulier, pour toutes les communications internes avec la VM d'administration, les données sont mises à disposition par la VM émettrice en entrée du mécanisme, la VM d'administration effectuant l'opération de lecture des données) :

- ce mécanisme permet à une VM source d'envoyer des données à une VM destination ;
- contrairement à d'autres méthodes de communication dans Xen, comme les communications réseau ou les vchans, il n'y a pas dans Argo de mémoire partagée entre les VM et les copies sont réalisées par l'hyperviseur. Les communications sont donc bien unidirectionnelles ;
- il existe des canaux cachés de stockage et temporels, que nous controns par des mesures appropriées :
    - canaux cachés de stockage : la structure de données utilisée par Argo entre 2 VM (VM1 émettant vers VM2 par exemple) utilise 3 identifiants : les deux identifiants de VM et un numéro de port. Ces structures sont créées dynamiquement. Le numéro de port pourrait être utilisé pour transférer de l'information. Dans CrossinG, nous contrôlons, par XSM, que seuls les triplets (VM1, VM2, ports) prévus (et hardcodés) peuvent être utilisés. De plus, nous supprimons la capacité de dés-enregistrer ces structures. Par ce biais, la VM2 peut juste transférer à VM1 un bit de présence par boot. Normalement, VM1 peut demander à Argo la taille disponible restante dans le buffer de communication avec VM2. VM2 peut moduler la taille restante dans ce buffer, ce qui fait apparaître un canal potentiel. Nous avons supprimé la possibilité de récupérer cette information ;
    - canaux cachés temporels : lorsqu'une VM1 tente d'envoyer des données alors que le buffer de communication est quasiment plein, Argo retourne une erreur à VM1 lui signifiant de retenter l'écriture plus tard. Comme VM2 contrôle la taille du buffer, cela lui permet de faire descendre de l'information vers VM1. Supprimer ce canal de retour aurait des conséquences inacceptables en termes de fiabilité de transfert et donc de performances. Nous utilisons une approche de type « Network Pump », où l'émetteur est de plus en plus ralenti au fur et à mesure que la place disponible dans le buffer d'émission diminue.

La construction des machines virtuelles est personnalisée, pour chaque machine virtuelle, sur la base d'un noyau Linux minimisé :

- les constructions des noyaux Linux sont différenciés et personnalisés pour l'ensemble des machines virtuelles ;
- minimisation des distributions *buildroot* avec sélection des paquets strictement nécessaires ;
- en post-construction, suppression des binaires, librairies et fichiers de configuration produits par *buildroot* mais non nécessaires au fonctionnement du produit ;
- suppression de l'ensemble des scripts d'initialisation engendrés par *buildroot* au profit d'un script d'initialisation unique personnalisé statique ;
- toutes les distributions sont en *squashfs* ;
- tous les noyaux et les rootfs sont signés ;
- suppression des applets non nécessaires de BusyBox ;
- minimisation et suppression des instructions de branchement du terminal Hush ;
- suppression de tous les binaires liés à la configuration réseau (ex. IfConfig) ;
- remplacement du binaire IpTables par un binaire OCaml spécifique à la plateforme.

En outre, une procédure de démarrage assure l'intégrité et l'authenticité des machines virtuelles (noyau, rootfs, configuration). Les machines virtuelles sont ensuite démarrées en RAM et aucune partition système n'est plus accessible depuis les VM (seules des partitions de configuration et de données leur sont accessibles).

Les différents services logiciels s'exécutant dans la passerelle sont intégrés dans les machines virtuelles cloisonnées par le socle de confiance, en particulier :

- une VM dédiée aux dépôts de fichiers connectée au réseau A ;
- une VM de transferts de sortie connectée au réseau A ;
- une VM dédiée aux dépôts de fichiers connectée au réseau B ;
- une VM de transferts de sortie connectée au réseau B ;
- une VM de filtrage et de traitements pour la politique de sécurité dédiée aux transferts de A vers B ;
- une VM de filtrage et de traitements pour la politique de sécurité dédiée aux transferts de B vers A ;
- une VM dédiée au service d'initialisation connectée au réseau d'administration ;
- une VM dédiée au service d'administration connectée au réseau d'administration ;
- une VM dédiée au service de supervision connectée au réseau de supervision ;
- une VM dédiée au service de déchiffrement et de vérification des mises à jour ;
- une VM dédiée au service d'application des mise à jour ;
- une VM dédiée au service de chiffrement des partitions .

L'ensemble des machines virtuelles disposant d'une interface réseau sont protégées par un pare-feu logiciel.

Les distributions des machines virtuelles sont construites par ChapsVision selon les principes suivants :

- le système Linux est configuré pour chaque machine virtuelle de la passerelle via un « buildroot 2019 » spécifiquement adapté intégrant uniquement la chaîne logicielle requise pour ses fonctions ;
- mise en cage (sandboxing) systématique des processus exécutés ;
- aucune communication réseau (et aucune pile logicielle réseau) pour les communications internes ;
- filtrage IpTables pour les communications réseaux externes (machines virtuelles de dépôts, sorties, d'administration et de supervision) ;
- séparation stricte des rôles et application du principe de moindre privilège (définition stricte des droits d'accès aux fichiers, configurations, communications) ;
- snapshots des machines virtuelles protégés en authenticité et intégrité ;
- distributions en SquashFS ;
- configuration logicielle protégée en authenticité et intégrité ;
- chaîne de transferts, d'administration et de dépollution développée par ChapsVision en OCaml.

CrossinG® met en œuvre des mécanismes de protection internes contre le déni de service :

- contrôle en intégrité et authenticité de tout le logiciel ChapsVision et de sa configuration par un mécanisme de « snapshots » signés des machines virtuelles, contrôlés au démarrage de la passerelle ;
- montage et exécution de la chaîne logicielle de chaque machine virtuelle dans un « SquashFS » ;
- contrôle des droits, accès et de l'exécution des logiciels dans les VM, gestion de la reprise sur erreur ;
- disponibilité des journaux archivés au-delà de 24h sur la VM d'administration de la passerelle.

Les services hébergés dans les différentes machines virtuelles sont les suivants :

- des services de **dépôt**, dans lesquels les fichiers à acheminer à travers la passerelle doivent être déposés via un client SFTP (SSH FTP) ou FTP. Par défaut, aucun compte n'est configuré sur la passerelle. L'administrateur dispose des possibilités suivantes (cumulables) pour configurer l'authentification des utilisateurs en entrée :
  - activation de l'authentification des utilisateurs via un serveur LDAP (auquel cas les comptes sont engendrés dynamiquement suite aux authentifications effectives) ;
  - création en nombre "illimité" (limites système Linux) de comptes utilisateurs statiques sur la passerelle.
- des unités de **filtrage** et de **traitement** qui intègrent l'ensemble des processus de sécurité mis en œuvre afin de déterminer si le fichier est conforme à la politique de sécurité définie et donc autorisé à être mis à disposition du SI de destination. Ces unités ne sont ni visibles, ni accessibles aux utilisateurs ;
- des services de **mise à disposition** correspondant aux zones où les fichiers autorisés sont stockés avant d'être acheminés vers le(s) serveur(s) de fichiers localisé(s) sur le réseau cible. Les protocoles SFTP et FTP/FTPS peuvent être mis en œuvre pour assurer la liaison entre le service de mise à disposition de la passerelle et le serveur de fichiers. Des règles permettent à CrossinG® de transférer les fichiers, en sortie, vers de multiples serveurs destinataires, de configurer un nombre d'essais de transfert en cas d'échec ou d'émettre des rapports d'analyse au format XML, et de configurer la signature ou le chiffrement des fichiers avant leur transfert de sortie ;
- des services d'**administration** permettant aux administrateurs, en local ou à distance, de configurer la passerelle (paramètres systèmes, réseaux et politiques de sécurité) ;
- des services de **supervision** permettant aux superviseurs d'accéder aux journaux d'activité et à la supervision SNMP/SYSLOG.

Les mécanismes de filtrage et de traitements sur les fichiers intégrés dans les machines virtuelles de dépollution sont les suivants :

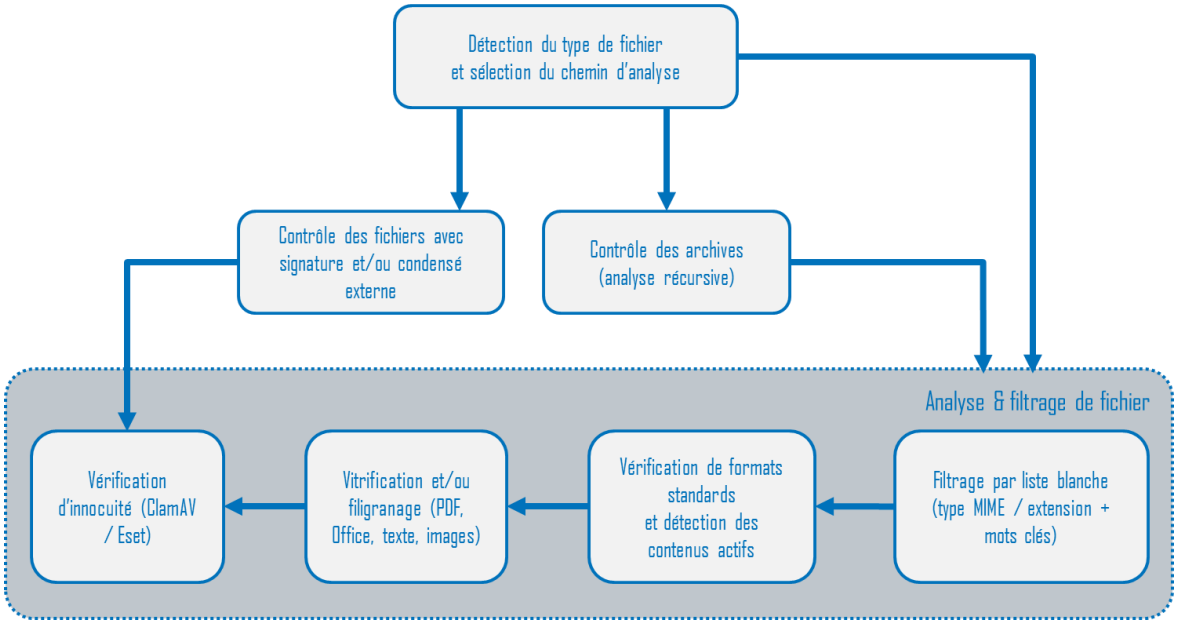

Figure 3 : Mécanismes de filtrage des fichiers

Chaque VM de dépollution combine plusieurs mécanismes de sécurité durant les transferts de fichiers pour assurer la défense en profondeur des SI sensibles et des infrastructures critiques :

- **Vérification de signatures et/ou d'empreintes externes**[2] destinée à la vérification d'authenticité et d'intégrité d'un fichier transféré réputé sûr. Dans ce cas, le fichier d'origine signé n'est sujet à aucun contrôle d'archive, de liste blanche, de vérification de format ou de vitrification. L'activation du contrôle antiviral est possible pour ces fichiers ;
- **Contrôle des archives** : lorsque ce contrôle est activé, toutes les archives soumises en entrée sont analysées récursivement, et refusées si le nombre d'imbrication d'archives ou le nombre de fichiers autorisés par répertoire est trop important. Les archives non conformes sont rejetées (suppression). Les archives protégées par un mot de passe sont systématiquement rejetées. L'administrateur a la possibilité de configurer le rejet complet des archives dont l'un des fichiers est vérolé ou non conforme à la politique de sécurité ;
- **Filtrage des fichiers par liste blanche** de formats, basé sur l'extension du fichier et le type MIME ;
- **Analyse des fichiers :**
    - **Vérification de format et de contenus actifs** : cette vérification consiste en l'analyse structurelle et la recherche de contenus actifs (macros, charges cachées) dans des types de fichiers connus (documents de type Office, PDF, archives, images, audio/video). Les fichiers dont la structure n'est pas conforme au format sont systématiquement rejetés. Sont exclus de la vérification de format les fichiers labellisés ou soumis à une règle de vérification de signature externe ;
    - **Vitrification** : afin de supprimer le code malveillant des fichiers de formats standards conformes, la vitrification leur fait subir une conversion de format (documents Office, PDF et autres formats texte convertis en PDF/A, images converties en PNG ou JPEG). L'opération de conversion a pour but de neutraliser les contenus actifs suspects. Seuls les éléments valides et sains du format d'origine seront transposés vers le format cible neutralisé ;
    - **Filigranage de documents PDF** : la politique de sécurité peut être configurée pour insérer automatiquement un filigrane dans tous les documents de type PDF. Le filigrane peut être personnalisé et contenir par exemple, automatiquement, le nom de l'utilisateur ayant poussé le fichier en entrée.
- **Vérification d'innocuité** : les analyses antivirales de Eset Nod32 et ClamAV peuvent être activées ou désactivées par l'administrateur. Par défaut, seul l'antivirus ClamAV est activé . Si une analyse antivirale est activée, les fichiers vérolés sont détruits (ils ne sont jamais transmis en sortie). Dans le cas d'une archive contenant un fichier vérolé, selon la configuration choisie par l'administrateur pour le traitement des archives, soit le fichier est détruit et le reste du contenu de l'archive est ré-archivé, soit l'archive est intégralement détruite.

[2]Signature engendrée dans l'infrastructure du client sous la forme d'un fichier de signature accompagnant le fichier d'origine à vérifier.

La politique de sécurité par défaut configurée pour les deux canaux de traitements de la passerelle est la suivante :

- Aucun compte d'entrée des fichiers n'est configuré, et aucun serveur d'entrée n'est activé pour l'ensemble des protocoles supportés ;
- Le contrôle des archives est actif ;
- Le filtrage par liste blanche est activé et aucun type de fichier n'est autorisé ;
- Analyse des fichiers activée et configurée de la manière suivante :
    - Fichiers Office & PDF : analyse de format, vitrification systématique. Tous les fichiers de type PDF ou Office sont systématiquement convertis en fichiers PDF/A sans contenu actif. Les fichiers sont systématiquement rejetés si leur format est invalide ;
    - Fichiers textes : vitrification systématique. Tous les fichiers détectés comme du texte (plaintext) sont systématiquement convertis au format PDF/A ;
    - Fichiers images : analyse de format et d'intégrité, vitrification en PNG. Tous les fichiers de type image sont systématiquement convertis en fichiers PNG neutres (encapsulés dans une archive tar) après vérification de leur format et de leur intégrité. Les fichiers sont systématiquement rejetés si leur format est invalide ou leurs données corrompues ;
    - Fichiers audio & video : ces fichiers sont systématiquement rejetés par la passerelle ;
    - Autres fichiers : tous les autres types de fichiers sont systématiquement rejetés par la passerelle.
- L'anti-virus Clam AV est activé par défaut, l'anti-virus Eset Nod32 est désactivé par défaut ;
- Aucune règle de vérification de signatures externe n'est définie.

NOTE : Les types MIME supportés par la passerelle pour la fonction de liste blanche et l'identification des fichiers en entrée des analyses de format sont spécifiés dans le document de spécification technique ([CROSSING_SPE]).

Par défaut, aucun fichier n'est donc accepté par la passerelle. Si l'administrateur active certains formats en liste blanche, ceux-ci seront alors soumis aux analyses de format, à la vitrification et à la vérification d'innocuité. La vitrification peut être désactivée ou configurée :

- en mode systématique (ie. quel que soit le résultat de l'analyse de format), configuration par défaut ;
- en cas de suspicion uniquement. La vitrification n'est alors réalisée que si l'analyse de format détecte le fichier comme valide mais avec des contenus actifs. Les fichiers de formats standards sans contenu actif détecté sont dans ce cas acceptés tels quels. Pour éviter les cas de faux négatifs (le contenu actif d'un fichier n'est pas détecté et donc le fichier n'est pas suspecté ni vitrifié) cette configuration n'est pas retenue par défaut.

De manière générale, l'IHM du produit affiche systématiquement un avertissement visuel sur chaque option de configuration non supportée par le périmètre de sécurité de cette cible. Le guide d'administration du produit en fait également clairement état.

D.2 Description du principe de fonctionnement du produit

La passerelle CrossinG® est livrée préinstallée avec une configuration par défaut décrite dans [CROSSING_ADM].
La procédure de premier démarrage est décrite dans [CROSSING_DEM].
Le démarrage de la passerelle requiert quelques minutes afin d'initialiser et configurer (de manière totalement automatique) l'ensemble des environnements virtuels et services logiciels. À l'issue de ce premier démarrage, il est nécessaire que l'administrateur accède à l'IHM locale HTTPS d'initialisation via le connecteur d'administration, en utilisant un certificat HTTPS ChapsVision. Un assistant de première configuration permet :

- de configurer l'accès à l'administration distante (HTTPS/LDAP/OCSP) ;
- de configurer la protection par mot de passe de l'accès local à l'IHM d'initialisation et aux fonctions de réinitialisation.

L'administration distante est accessible de manière sécurisée depuis un navigateur web. L'authentification est effectuée à l'aide d'un certificat et optionnellement via un serveur LDAP externe. Un seul et unique rôle est défini et permet d'accéder à l'ensemble des paramètres de configuration.

Via l'IHM web distante, l'administrateur peut configurer :

- l'ensemble des services d'administration et de supervision (NTP, SYSLOG, SNMP, comptes système SFTP d'administration, accès HTTPS pour la supervision) ;
- pour les chaînes de transferts AB et BA :
  - l'activation des serveurs d'entrée, des comptes d'entrée des fichiers et de leurs clefs SSH ;
  - l'ensemble des règles de sortie « multichaînes », le serveur de failover et les options de sortie ;
  - la politique de sécurité associée (liste blanche, analyses, ...).

Rupture protocolaire sur les transferts de fichiers :

La passerelle autorise uniquement les transferts de fichiers. Sur ses interfaces d'entrée, la passerelle permet d'activer des serveurs de dépôt des fichiers pour chaque protocole supporté. Sur ses interfaces de sortie, la passerelle dispose de clients lui permettant de transférer les fichiers sains vers les serveurs du réseau destinataire.

Les communications entre la machine virtuelle connectée au réseau émetteur et celle de dépollution, et entre la machine virtuelle de dépollution et celle connectée au réseau destinataire, sont gérées par la passerelle à l'aide d'un mécanisme mettant en œuvre un canal unidirectionnel non réseau géré par l'hyperviseur.

En outre, la séparation des traitements pour chaque sens de transfert des fichiers via deux chaînes de machines virtuelles (entrée, dépollution, sortie) permet d'assurer deux canaux de communication internes unidirectionnels cloisonnés.

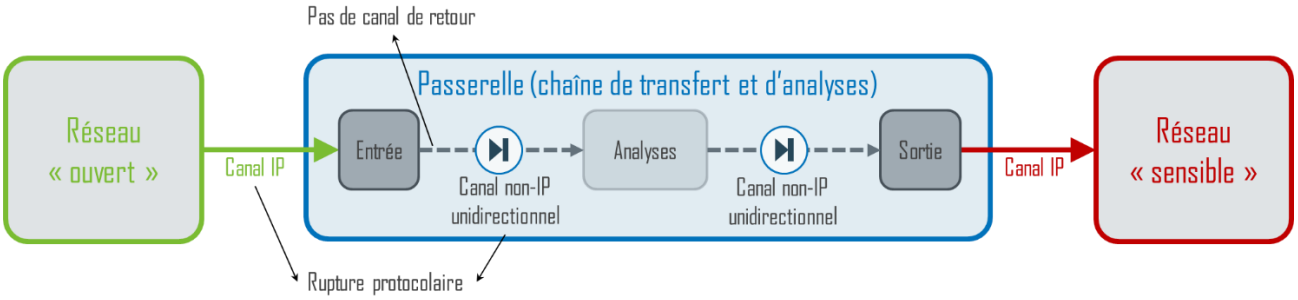

Figure 4 – Principe d'une chaîne de transfert (schéma simplifié)

Deux modes de fonctionnement sont possibles pour la passerelle :

- Le mode **monodirectionnel** autorise uniquement le transfert de fichiers d'un réseau A à un réseau B (ou d'un réseau B à un réseau A) selon une politique de sécurité configurable via l'interface d'administration.

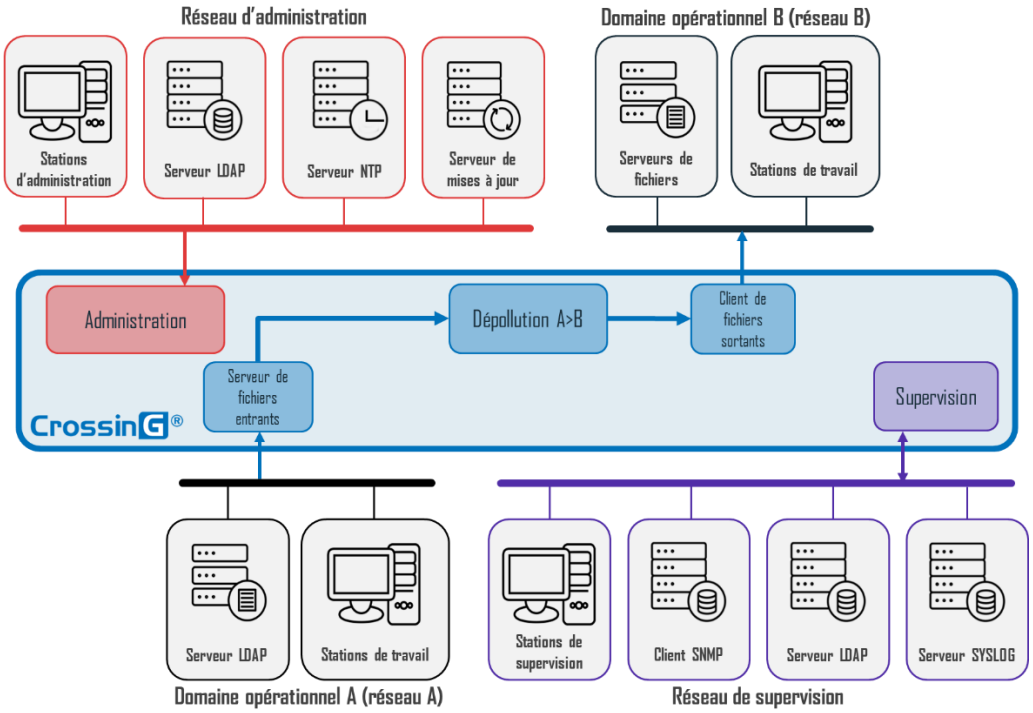

Figure 5 – Fonctionnement monodirectionnel

- Le mode **bidirectionnel** autorise le transfert de fichiers d'un réseau A vers un réseau B selon une politique de sécurité P-AB, ainsi que le transfert de fichiers d'un réseau B vers un réseau A selon une politique de sécurité P-BA via des VM distinctes (une par sens de communication). Les politiques de sécurité sont configurables via l'interface d'administration.

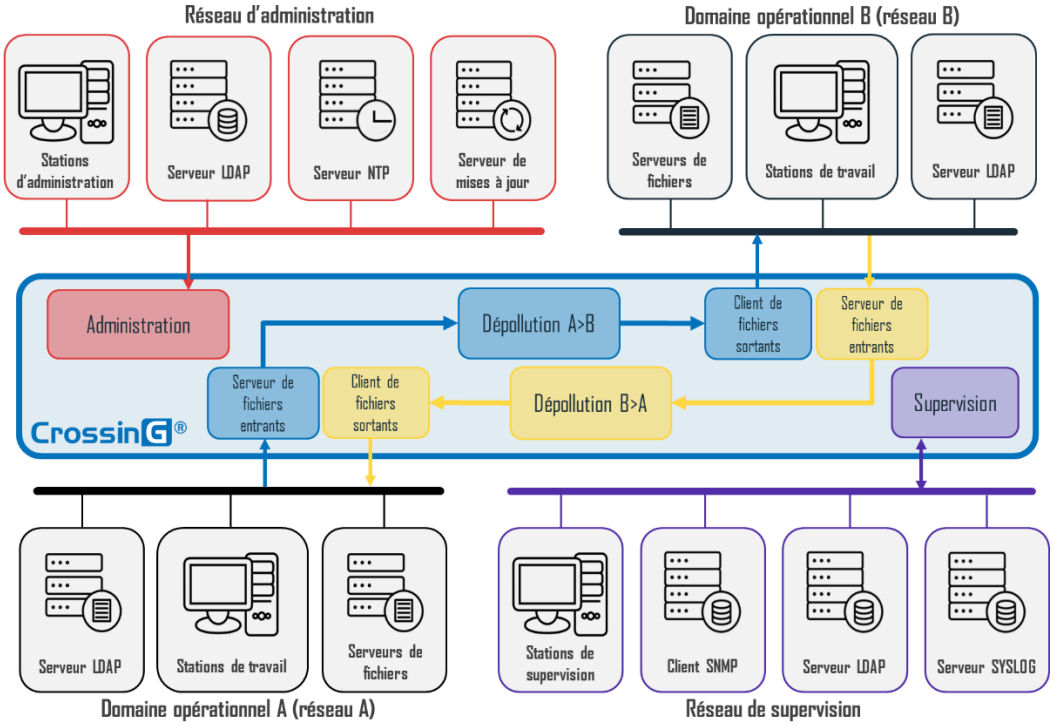

Figure 6 – Fonctionnement bidirectionnel

Une fois configuré, CrossinG® fonctionne en trois grandes étapes :

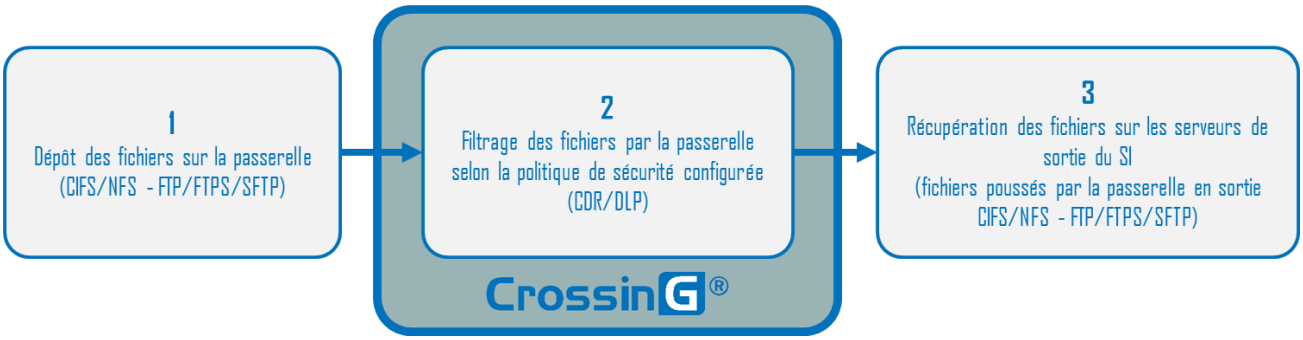

Figure 7 – Fonctionnement de CrossinG

Etape 1 – Dépôt des fichiers

Cette étape permet à l'utilisateur de déposer, à l'aide d'un client de transfert de fichiers, les fichiers qu'il souhaite faire transiter d'un réseau A vers un réseau B, à travers la passerelle.

Etape 2 – Traitement des fichiers

Durant cette seconde étape, les fichiers déposés en entrée sont automatiquement transférés vers un environnement de traitement correspondant au sens du canal de communication. La conformité des fichiers par rapport à la politique de sécurité est vérifiée et validée. Les fichiers autorisés à entrer sont automatiquement envoyés vers le service de mise à disposition (avec ou sans transformation) et ceux refusés sont détruits.

Etape 3 – Transfert des fichiers autorisés

Les fichiers autorisés à circuler sont automatiquement poussés vers un serveur de fichiers situé dans l'infrastructure cible. L'utilisateur peut ensuite se connecter au serveur de fichiers de son infrastructure, afin de récupérer les fichiers.

Par défaut, un rapport d'analyse est généré par la passerelle CrossinG® pour chaque fichier transmis en entrée. Tous les rapports de sortie sont enregistrés au même niveau que les fichiers auxquels ils se réfèrent avec le nom du fichier analysé suffixé par **« XXXXXXXX_report.xml »** où « XXXXXXXX » est un condensé unique identifiant la transaction sur la passerelle. Ceci permet d'assurer la présence de tous les rapports de sortie même dans le cas où un fichier de même nom serait transmis plusieurs fois.

Ce rapport permet à l'utilisateur de disposer d'informations relatives au succès ou à l'échec du transfert telles que :

- l'ID unique de la transaction interne ;
- l'heure UTC de la fin de l'analyse ;
- le nom complet du fichier analysé ;
- l'état de l'analyse :
  - **valide** : le fichier a été transmis correctement ;
  - **converti** : le fichier a été converti via la méthode de vitrification configurée ;
  - **archive convertie** : l'archive a été ré-archivée après modification de son contenu - vitrification de fichier(s), suppression de fichier(s) invalide(s) ;
  - **authentifié** : fichier ou archive signée dont la signature est reconnue lors de la vérification de label ou de signature externe ;

- **non autorisé** : fichier non autorisé en liste blanche ;
- **non conforme** : fichier dont l'extension ou le type MIME ont été détectés comme non conformes au type autorisé attendu ;
- **contenu malveillant** : fichier contenant une charge active cachée ;
- **trop d'imbrications dans l'archive** : archive ne respectant pas le paramétrage d'imbrications maximum ;
- **mauvaise signature** : fichier ou archive signée dont la signature n'est pas reconnue lors de la vérification de label ou de signature externe ;
- **fichiers manquants** : des fichiers attendus pour l'analyse par lots (vérification de signature externe par exemple) sont manquants ;
- **erreur système** : mauvaise prise en compte par le système du fichier transmis ;
- **erreur inconnue** : erreur non prise en charge par le système.

À noter que tous les événements de traitements sont également logués pour la supervision syslog. La passerelle n'émet pas de statut pour l'utilisateur ayant poussé le fichier en entrée, cette opération étant contraire au principe d'unidirectionnalité de chaque canal de transfert.

En outre, CrossinG® permet de s'interfacer avec :

- un serveur SNMP permettant la supervision à distance de la passerelle. A l'aide d'une MIB dédiée à la passerelle, un agent externe de supervision peut surveiller l'activité de la passerelle et déclencher des alertes sur des événement précis (état des chaînes de traitement, statistiques sur les fichiers traités, ...) ;
- un serveur NTP externe afin de synchroniser la passerelle CrossinG® sur une référence de temps propre au système d'information provenant du réseau d'administration. CrossinG® peut également agir comme serveur NTP sur chacune des machines virtuelles connectées aux réseaux A et B afin de propager cette référence vers ces réseaux ;
- un serveur de centralisation des journaux. CrossinG® maintient localement un journal d'activité de la passerelle au format SYSLOG. L'interface d'administration permet de configurer la redirection automatique et sécurisée des journaux au format SYSLOG, vers un serveur distant. La machine virtuelle d'administration de la passerelle assure une rétention des journaux calibrée pour une utilisation intensive critique pendant 24h : un maximum de 64 archives de 20Mo chacune sont conservées ; la rotation des journaux est basée sur la taille des archives de logs et non sur le timestamp, l'espace disque ne peut donc pas être saturé ; la passerelle émet un log SYSLOG à chaque rotation (aucun seuil n'est configurable, il reste à la charge de l'administrateur de veiller à récupérer les logs ; ceci est décrit dans le guide d'administration).

NOTE : Pour les fonctions d'administration SYSLOG, HTTPS et LDAP, la passerelle permet la connexion des équipements supportant TLS v1.2 à v1.0 (TLS v1.2 est sélectionné en priorité). Les algorithmes standards suivants sont supportés : openssl ciphers 'HIGH' et openssl ciphers 'MEDIUM'.

D.3 Description de l'environnement prévu pour son utilisation

D.3.1 Matériel compatible ou dédié

Nouvelles configurations matérielles

La passerelle CrossinG® est disponible dans les configurations matérielles décrites ci-dessous.

Ces configurations offrent une base matérielle commune en termes de processeur, carte mère et environnement d'utilisation, et des options permettant la sélection d'une configuration adaptée au besoin (performance, réseaux de transfert fibrés, alimentation redondante, configuration des disques pour les transferts).

Caractéristiques communes :

- **Chassis** : KONTRON PC 2U KISS
- **Carte mère :** Supermicro X10SRM-F
- **Processeur :** 1 x Intel® Xeon E5 2620v4 2.1-3.0 GHz, 8c/16t, cache 20Mo
- **Mémoire RAM :** 4 x 16Go DDR4 ECC
- **Disques :**
  - 1 x SSD M2 128Go interne, non extractible
  - 2 x SSD 860 Evo extractibles (1 To par défaut), configurés en RAID 1 par défaut
- **Réseau :** 2 ports Lan Gigabit Intel i350 comp PXE (dédiés à l'administration et la supervision)
- **Température de stockage :** -20 à +70°C
- **Température d'utilisation :** 0°C à +50°C
- **Chocs :** 15 g. 11ms
- **Vibrations :** 1 g. 10-500Hz
- **Altitude :** 2000m
- **Dimensions (W x H x D) :** 482mm x 88mm x 472mm
- **MTBF :** 85 000h à 25°C
- **Type de ventilation :** avant vers arrière
- **Certifications :** CE, UL, FCC

Les options matérielles suivantes sont disponibles :

- **Alimentation :** simple, 400 W / 500 W ou redondée 2 x 380 W 80+ ou 2 x 500 W
- **Connecteurs réseaux A & B :** 2 x RJ45 1 Gbits, 2 x RJ45 10 Gbits ou 2 x fibre 10 Gbits

D.3.2 Système d'exploitation retenu

La passerelle CrossinG® est une appliance autonome, embarquant son propre système d'exploitation, basé sur XEN v4.12 adapté et sécurisé par ChapsVision.

Les machines virtuelles utilisent un système Linux basé sur un noyau 4.19 LTS. Le système Linux est configuré pour chaque machine virtuelle de la passerelle via un « buildroot 2019 » spécifiquement adapté intégrant uniquement la chaîne logicielle requise pour ses fonctions. Les machines virtuelles sont diversifiées via des options de compilation différentes.

D.3.3 Description des dépendances

La passerelle CrossinG® est une *appliance* autonome, constituée du matériel et de l'ensemble de ses éléments logiciels.

Les logiciels externes compatibles validés sont spécifiés dans le document de spécification technique ([CROSSING_SPE]).

D.4 Définition du périmètre de l'évaluation

D.4.1 Périmètre

L'évaluation porte sur la passerelle CrossinG®, considérée en « boîte noire » sous l'angle de ses quatre interfaces. Dans le schéma suivant, chaque boîte interne, « Administration », « Supervision », « Serveur de fichiers entrants », « Client de fichiers sortants » et « Dépollution » représente une machine virtuelle dédiée à ce service :

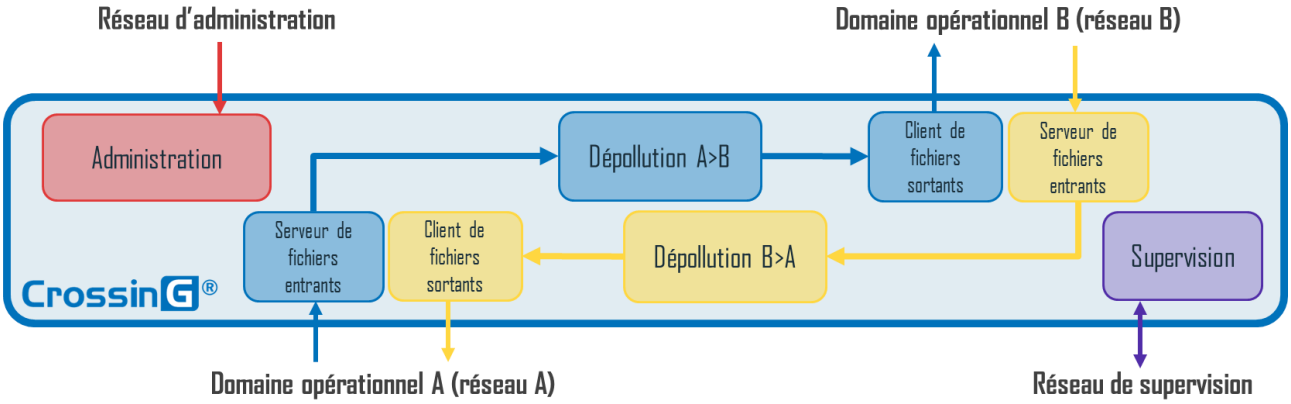

Figure 8 – Périmètre de l'évaluation (schéma simplifié)

La configuration et les modes de fonctionnement soumis à l'évaluation sont les suivants :

- Passerelle en mode bidirectionnel (les filtrages A->B et B->A sont assurés par deux VM monodirectionnelles distinctes, cloisonnées et déconnectées des interfaces réseau physiques de la passerelle) ;
- Services d'échange de fichiers utilisant le protocole SFTP avec authentification soit par identifiant et mot de passe, soit par clé publique, soit via un annuaire LDAP sécurisé, et la configuration de règles de sortie « multi-chaînes » utilisant le protocole SFTP et utilisant ou non les options de chiffrement et de signature des fichiers en sortie ;
- Politiques de sécurité configurées de la façon suivante :
  - Activation des deux chaînes de traitement (mode bidirectionnel) ;
  - Filtrage par liste blanche des formats autorisés (type MIME et extension) ;
  - Analyse des fichiers configurée pour :
    - rejeter systématiquement les fichiers de formats standards non conformes (Office, PDF, texte, images) ;
    - vitrifier systématiquement les fichiers de formats standards conformes (Office, PDF, texte, images) en PDF/A et PNG, quel que soit le résultat de l'analyse de format sur la détection de contenus actifs ;

        - rejeter systématiquement les fichiers de formats audio/video ou inconnus ;
        - filigraner automatiquement les documents PDF après vitrification.
    - Analyse d'innocuité active mettant en œuvre les antivirus Eset Nod32 et ClamAV ;
    - Vérification récursive des archives ;
    - Vérification des fichiers transmis avec une politique de vérification de signatures externes.
- Journalisation locale et export sécurisé des journaux d'activité SYSLOG sécurisé par TLS v1.2 ou par SSH ;
- Supervision de la passerelle via le protocole SNMP v3 uniquement, sur la base de la MIB CrossinG®. En particulier, SNMP GET et traps sont désactivés par défaut. La passerelle n'autorise pas les commandes SNMP SET et ne gère pas la communauté publique ;
- Administration distante sécurisée via canal TLS v1.2 et authentification LDAP sécurisé des administrateurs ;
- Synchronisation NTP de la passerelle depuis le réseau d'administration puis activation des serveurs NTP sur les VM A et B pour leur réseau respectif ;
- Mise à jour distante (hyperviseur, machines virtuelles, logiciel de traitement et bases antivirales) par SFTP ;
- Administration HTTPS par IHM web distante de la passerelle CrossinG® ;
- Fonctions d'import/export de configuration au format JSON chiffrées par un secret client.

Sont exclus du périmètre de l'évaluation les services ou options de configuration suivants :

- Options d'analyse des fichiers identifiés comme suspects ;
- Vérifications d'empreintes de fichiers configurées sans vérification de signatures associée ;
- Utilisation des options de hachage MD5 et SHA-1 pour les vérifications d'empreintes ;
- Analyse des fichiers audio/video configurée pour accepter les formats valides ;
- Protocole SFTP configuré sans vérification de l'empreinte du serveur distant pour les transferts en sortie de la passerelle ;
- Protocole FTP/FTPS pour les transferts de fichiers en entrée et en sortie. Ce service n'est présent que pour assurer la compatibilité avec certains anciens équipements ;
- Support des disques réseau CIFS/NFS ;
- Activation des logs de DEBUG (cette fonction est disponible pour les phases d'intégration client afin de faciliter l'analyse en cas de problème. Les logs de DEBUG sont toujours désactivés par défaut) ;
- Activation des traps SNMP ;
- Activation du PING des interfaces réseaux.

Le guide d'administration [CROSSING_ADM] de la passerelle ainsi que les IHM d'administration du produit indiquent clairement à l'administrateur sa responsabilité pour toute modification du paramétrage activant des fonctions exclues du périmètre de sécurité. Par souci d'homogénéité, le comportement est le même pour l'ensemble des fonctions hors cible: une icône de type "Warning" avec une bulle d'aide indiquant "Attention: l'activation de certaines

fonctionnalités n'est pas couverte par la cible de sécurité du produit." est systématiquement affichée dans l'IHM pour les états à risque et indique clairement à l'administrateur quelles fonctions sont en cause.

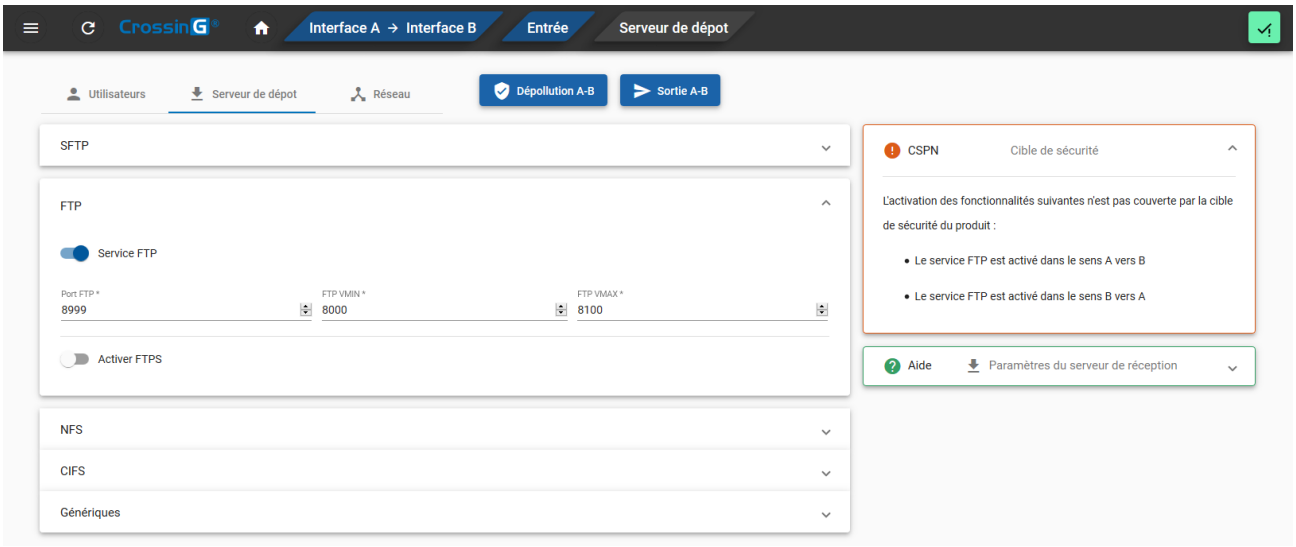

Figure 9 – Exemple d'alerte CSPN dans l'IHM du produit

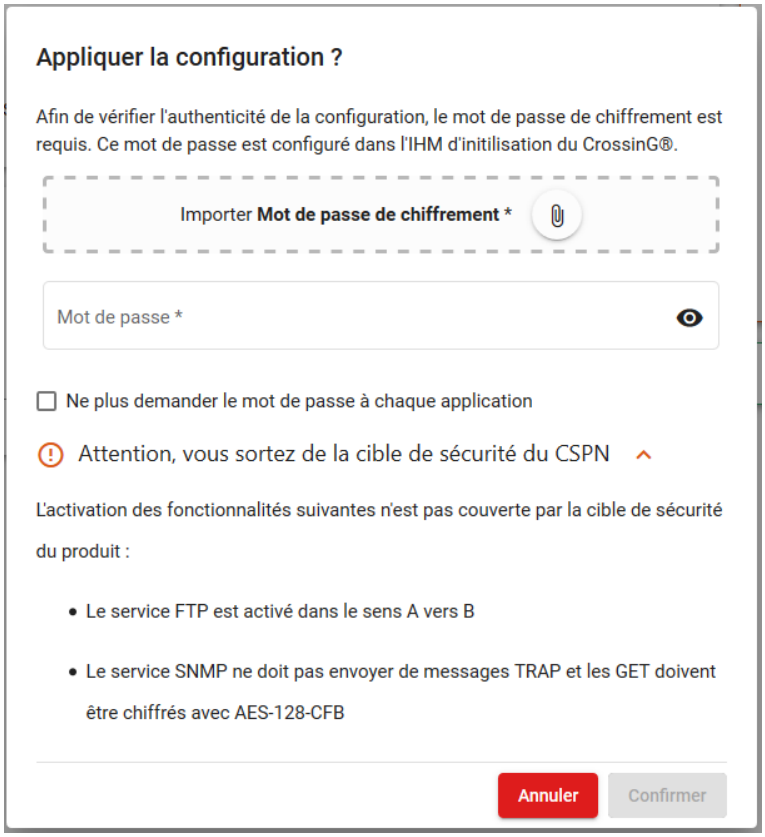

Figure 10 – Alerte avant soumission de configuration dans l'IHM du produit

D.4.2 Plateforme d'évaluation

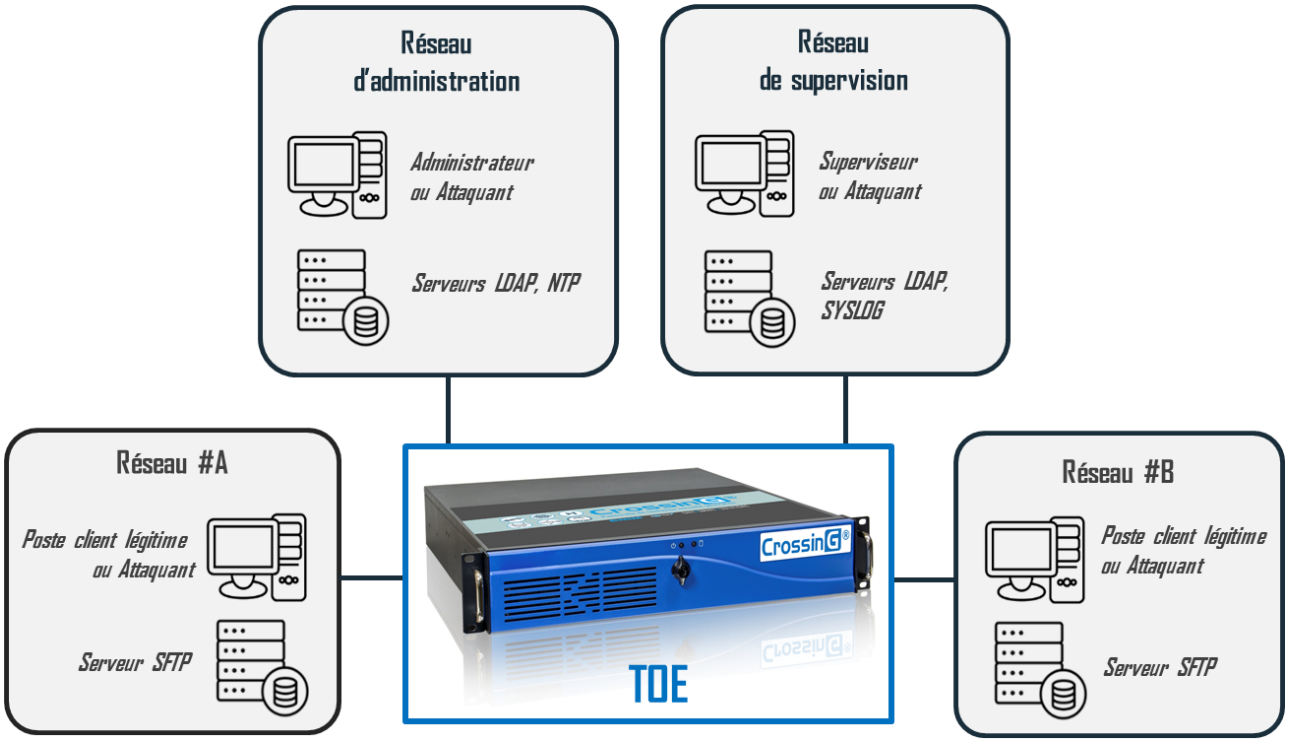

Figure 11 - Plateforme d'évaluation

E Problématique de sécurité

E.1 Description des utilisateurs typiques concernés

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants doivent être pris en considération dans le cadre de l'évaluation de sécurité :

Libellé	Description
Administrateur	Utilisateur ayant les droits de modifier une partie de la configuration de la ToE : ▪ Politique de sécurité ; ▪ Paramètres système ; ▪ Comptes utilisateurs.
Superviseur	Utilisateur ayant les autorisations d'accès en lecture aux journaux du système et de la solution logicielle de ChapsVision.
Utilisateur	Utilisateur ayant les autorisations pour se connecter à la passerelle et transférer des fichiers, depuis le réseau A ou le réseau B.

E.2 Description des biens sensibles

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité.

Les biens à protéger sont les suivants :

E.2.1 Biens sensibles de l'environnement

Identifiant	Description
[B.RESEAUX]	Les réseaux A et B dont les domaines opérationnels sont différents, isolés par la ToE.
[B.ECHANGES]	L'ensemble des canaux de communication réseaux (échanges entre les réseaux A et B, exports SYSLOG, LDAP, flux d'administration et de supervision…). Les échanges sont soumis à une contrainte préalable d'authentification des utilisateurs et administrateurs. Les échanges sont soumis à une contrainte de traçabilité.
[B.MISES A JOUR]	Les mises à jour de la ToE (logiciels et bases virales). Le dépôt des mises à jour sur la passerelle est soumis à une contrainte d'authentification. L'application des mises à jour est soumise à des contraintes de vérification d'intégrité et de traçabilité.
[B.ADMIN]	Les réseaux d'administration et de supervision.

E.2.2 Biens sensibles de la ToE

Identifiant	Description
[B.LOGICIELS]	Les logiciels embarqués dans la ToE.
[B.BASES AV]	Les bases de signatures virales embarquées dans la ToE.
[B.CONFIGURATION]	Le(s) fichier(s) de configuration et de paramétrage des politiques de sécurité pour les communications A vers B et B vers A. Les modifications de la configuration de la passerelle sont soumises à une contrainte de traçabilité.
[B.AUTHENTIFIANTS]	Les certificats et mots de passe utilisés dans les processus d'authentification des utilisateurs et administrateurs. Les échanges de données avec l'extérieur de la ToE (les réseaux A et B, les accès d'Administration et de la supervision) sont authentifiés. Un annuaire d'identité extérieur de la ToE peut être utilisé pour l'authentification des utilisateurs et des administrateurs (administration et supervision).

[B.JOURNAUX]	Les journaux engendrés par la ToE (évènements système, actions des utilisateurs/administrateurs et événements de supervision). La journalisation permet d'assurer la traçabilité des échanges, mises à jour et actions d'administration : ▪ transferts de fichiers entrants et sortants ; ▪ actions d'administration (modifications de configuration, imports/exports, transferts SFTP…) ; ▪ mises à jour de la passerelle.

E.2.3 Besoins de sécurité associés

Les besoins de sécurité pour les biens sensibles de la ToE et de son environnement sont les suivants :

	Bien sensible	Disponibilité	Confidentialité	Intégrité	Authenticité
Biens de l'environnement	[B.RESEAUX]		X	X	
	[B.ECHANGES]		X	X	X
	[B.MISES A JOUR]			X	X
	[B.ADMIN]		X	X	
Biens de la ToE	[B LOGICIELS]	X		X	X
	[B.BASES.AV]	X		X	X
	[B.CONFIGURATION]	X	X	X	X
	[B.AUTHENTIFIANTS]	X	X	X	
	[B.JOURNAUX]	X		X	

X : obligatoire

E.3 Description des hypothèses sur l'environnement

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement.

Les hypothèses sur l'environnement de la TOE suivantes doivent être considérées :

Identifiant	Description
[H.SECURITE PHYSIQUE]	La ToE est utilisée dans un environnement considéré comme physiquement sûr (local à accès contrôlé, de même niveau de confiance que le réseau le plus sensible).
[H.INTEGRITE]	La ToE est à jour de l'ensemble des correctifs de sécurité en vigueur et des dernières versions des bases des antivirus embarqués. La configuration usine est également intègre par hypothèse.
[H.ADMINISTRATEUR]	Les administrateurs de la ToE et les opérateurs de la supervision sont compétents, formés et non hostiles. Les administrateurs sont compétents pour la génération et l'utilisation des objets cryptographiques, en connaissance des causes pouvant réduire la sécurité de la ToE. Les fichiers de configuration exportés de la ToE sont sauvegardés sur un espace de stockage protégé en intégrité par l'administrateur.
[H.ENV.RESEAU.ADM]	Les réseaux d'administration et de supervision sont isolés et accessibles uniquement sur un poste spécifique non accessible pour les agents de menace. Les réseaux d'administration et de supervision doivent être déconnectés d'internet.
[H.STATION.ADM]	Les stations d'administration et de supervision sont sécurisées et maintenues à jour de toutes les vulnérabilités connues concernant les systèmes d'exploitation et les applications utilisées. Elles sont installées dans un local à accès protégé.
[H.INTERFACE ADMISTRATION]	Les interfaces réseau d'administration et de supervision sont connectées à des réseaux dédiés. Ces réseaux doivent être soit physiquement disjoints des réseaux de production (A et B), soit cloisonnés par un mécanisme logique (ex : VLAN). Les réseaux d'administration et de supervision sont eux même cloisonnés entre eux. L'ensemble des réseaux sont isolés deux à deux.
[H.COUPURE]	La ToE est installée conformément à la politique d'interconnexion des réseaux en vigueur et est le seul point de passage entre les réseaux A et B, sur lesquels il faut appliquer la politique de contrôle des fichiers transférés.
[H.POLITIQUES]	Les politiques de sécurité configurées dans la ToE sont considérées comme adaptées aux cas d'usages.
[H.JOURNAUX]	Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par l'équipement.

[H.INSTALLATION]	L'installation de la ToE respecte les préconisations issues de la documentation du développeur.
[H.SERVICES DESACTIVES]	Les services de la passerelle en dehors du périmètre de l'évaluation (cf. section D.4.1) sont désactivés.
[H.AUTHENTIFICATION]	Les serveurs d'authentification utilisés pour authentifier les administrateurs sont considérés comme sains et configurés correctement.
[H.APPLIANCE PRODUCTION]	Les appliances fournies sont configurées en "mode production", c'est-à-dire que les utilisateurs et administrateurs n'ont pas accès au système par d'autres canaux que ceux prévus pour son utilisation (interfaces web et SFTP). En particulier, les administrateurs n'ont pas accès à une invite de commande (ni SSH, ni en port série). Cela est en opposition au "mode debug" qui permet un accès au système en SSH pour les administrateurs.

E.4 Description des menaces

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la cible évaluée.

Les agents menaçants à considérer pour l'évaluation de sécurité doivent être les suivants :

- **Entités non autorisées** : un attaquant humain ou entité qui interagit avec la TOE mais ne dispose pas d'accès légitime à la ToE (poste client non autorisé ou usurpé sur les réseaux A ou B) ;
- **Entités autorisées** : les utilisateurs, sans droits d'administration, ayant un accès légitime à la TOE.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

Identifiant	Description
[M.CONTOURNEMENT FILTRAGE]	Un attaquant parvient à transférer des données de manière non autorisée en contournant la politique de sécurité opérée par la ToE.
[M.TRANSFERT MALVEILLANT]	Un attaquant parvient à contourner les contrôles réalisés par la ToE sur le contenu à transférer et, par suite, à transférer des données non autorisées contenant des logiciels malveillants.
[M.CORRUPTION CAGE]	Un attaquant parvient à exécuter du code arbitraire au sein d'une cage.
[M.CORRUPTION FLUX]	Un attaquant parvient à modifier un flux légitime afin d'accéder voire modifier de l'information de manière illicite (canal de communication entre les réseaux de domaines opérationnels différents, flux de mise à jour, flux de journalisation, etc.).
[M.CORRUPTION MISE A JOUR]	Un attaquant parvient à corrompre une mise à jour dans le but d'altérer le fonctionnement de la ToE (injection de code dans le firmware, corruption des bases virales par exemple).
[M.CORRUPTION ADMIN]	Un attaquant parvient à exécuter du code dans la VM d'administration depuis une autre VM.
[M.CORRUPTION CONFIGURATION]	Un attaquant parvient à modifier la configuration de la ToE dans le but d'altérer son fonctionnement (rendre les politiques de sécurité des échanges entre les réseaux plus permissives par exemple).
[M.USURPATION]	Un attaquant parvient à usurper l'identité d'un utilisateur dans le but d'élever ses privilèges sur la ToE (utilisateur ou administrateur).
[M.CORRUPTION JOURNAUX LOCAUX]	Un attaquant parvient à masquer une opération sur la ToE.
[M.CORRUPTION EXPORT]	Un attaquant parvient à modifier les journaux déportés (ou la configuration exportée) de la ToE dans le but de masquer une opération sans que le destinataire ne puisse s'en rendre compte.
[M.PERTE DISPONIBILITE]	Un attaquant parvient à effectuer un déni de service sur la ToE en effectuant une action imprévue ou en exploitant une vulnérabilité.

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "D", "I", "C" et "A" représentent respectivement les besoins de Disponibilité, Intégrité, Confidentialité et Authenticité) :

	[B.RESEAUX]	[B.ECHANGES]	[B.MISES A JOUR]	[B.ADMIN]	[B.LOGICIELS]	[B.BASES AV]	[B.CONFIGURATION]	[B.AUTHENTIFIANTS]	[B.JOURNAUX]
[M.CONTOURNEMENT FILTRAGE]	I								
[M.TRANSFERT MALVEILLANT]	CI	I							
[M.CORRUPTION CAGE]		I			IA	I	I	IC	
[M.CORRUPTION FLUX]	I	ICA	IA						I
[M.CORRUPTION MISE A JOUR]			IA		IA	IA			
[M.CORRUPTION ADMIN]				CI					
[M.CORRUPTION CONFIGURATION]							ICA		
[M.USURPATION]		IC					IC		I
[M.CORRUPTION JOURNAUX LOCAUX]									I
[M.CORRUPTION EXPORT]							I		I
[M.PERTE DISPONIBILITE]					D	D	D	D	D

E.5 Description des fonctions de sécurité du produit

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et mécanismes mis en œuvre dans la TOE pour protéger de façon proportionnée les biens sensibles de la TOE contre les menaces identifiées.

Les fonctions de sécurité essentielles de la TOE sont les suivantes :

Identifiant	Description
[F.FILTRAGE]	La ToE protège l'accès direct au réseau A depuis le réseau B et réciproquement, ainsi que l'accès au réseau d'administration vis-à-vis des réseaux A et B. Les mécanismes mis en œuvre sont les suivants : ▪ l'ensemble des réseaux sont isolés deux à deux ; ▪ le socle de confiance assure la mise en œuvre de canaux de communication non réseaux unidirectionnels entre les machines virtuelles ; ▪ les logiciels clients/serveurs assurant l'échange des données sont écrits en langage OCaml et les données transmises sur le canal de communication sont des objets OCaml ; ▪ les machines virtuelles d'entrées ou de sorties des fichiers mettent en œuvre un filtrage IpTables n'autorisant que les protocoles de transfert configurés par l'administrateur sur les ports spécifiés ; ▪ les communications réseau internes entre machines virtuelles sont désactivées.
[F.TRAITEMENT.ENTREE]	La ToE opère divers contrôles sur les données à transférer : ▪ vérification des types de fichiers non autorisés à partir d'une liste blanche ; ▪ vitrification systématique PDF/A et PNG ; ▪ filigranage automatique des fichiers PDF ; ▪ recherche de codes malveillants (analyse antivirale) ; ▪ vérification de signature externe ; ▪ filtrage « multichaînes » des fichiers pour la redirection en sortie. La TOE assure la continuité du droit entre un réseau bas et un réseau haut en transférant les métadonnées ou enveloppes liées à chaque transfert (contenant en particulier la politique de sécurité applicable au transfert et les identifiants de l'utilisateur à l'origine du transfert) au sein d'un objet OCaml transféré d'un bout à l'autre de la chaine de traitement.
[F.CLOISONNEMENT]	La ToE opère les processus de filtrage et de traitement au sein de machines virtuelles dédiées (une par sens de circulation des fichiers) fortement cloisonnées et inaccessibles à l'utilisateur. La ToE assure le cloisonnement interne de tous les processus exécutés dans l'ensemble de ses machines virtuelles. Les mécanismes de cloisonnement mis en œuvre sont les suivants : ▪ cloisonnement des machines virtuelles par le socle de confiance ; ▪ cloisonnement des processus internes aux machines virtuelles par des cages logicielles basées sur le chroot Linux ;

	▪ protection des accès internes aux machines virtuelles par la suppression des outils système Linux standards et la suppression par défaut des droits.
[F.COMMUNICATIONS SECURISEES]	Les échanges entre les différents réseaux interfacés avec la ToE sont protégés en authenticité (les communications sont authentifiées), confidentialité et intégrité.
[F.MAJ SECURISEE]	La ToE vérifie l'intégrité et l'authenticité des mises à jour reçues.
[F.AUTHENTIFICATION]	La ToE authentifie les utilisateurs et administrateurs au moyen d'un certificat ou mot de passe.
[F.CONTROLE ACCES]	La ToE restreint l'accès à son fichier de configuration et empêche la modification de ses journaux locaux.
[F.JOURNALISATION LOCALE]	La ToE journalise les évènements (rotation ≥ 24h). La machine virtuelle d'administration de la passerelle assure une rétention des journaux calibrée pour une utilisation intensive critique pendant 24h : un maximum de 64 archives de 20Mo chacune sont conservées ; la rotation des journaux est basée sur la taille des archives de logs et non sur le timestamp, l'espace disque ne peut donc pas être saturé. La ToE assure en particulier la journalisation des événements suivants : ▪ transferts de fichiers entrants et sortants ; ▪ statut de dépollution des fichiers ; ▪ actions d'administration (modifications de configuration, imports/exports, transferts SFTP…) ; ▪ mises à jour de la passerelle.
[F.EXPORT SECURISE]	La ToE permet de transmettre les journaux déportés à un équipement tiers de manière intègre et authentifiée. Elle permet également d'exporter la configuration (sur un compte de la VM admin) au format JSON et protégé en intégrité. La transmission des journaux à un équipement tiers est protégée par [F.COMMUNICATIONS SECURISEES]. La confidentialité des journaux en transit est ainsi garantie. Dans le cas des fonctions d'export et d'import de la configuration de la passerelle, cette dernière peut être intégralement chiffrée : l'administrateur a le choix d'importer ou d'exporter la configuration chiffrée ou en clair.
[F.PROTECTION DISPONIBILITE]	La ToE met en œuvre des mécanismes de protection internes contre les cas de perte de disponibilité suivants : ▪ l'arrêt brutal des logiciels et processus mis en œuvre dans la chaîne de traitements. Les mécanismes suivants sont mis en œuvre: ▪ un processus dédié dans chaque machine virtuelle a pour objectif de détecter les erreurs d'exécution et de relancer les processus fautifs.
[F.AUTOPROTECTION]	La ToE met en œuvre des mécanismes d'autoprotection contre :

- l'accès en lecture et en écriture sur la configuration ou les données par les processus n'en ayant pas le besoin (moindre privilège) ;
- l'exécution interne de code malveillant au sein de ses machines virtuelles.

Les mécanismes mis en œuvre sont les suivants :

- configuration des droits d'accès à la configuration et aux données pour chaque binaire ;
- chiffrement des partitions ;
- montages RAM squashFS des machines virtuelles au démarrage ;
- snapshots des machines virtuelles protégés en authenticité et intégrité.

En particulier, la ToE stocke les secrets de connexion des utilisateurs et administrateurs sur le disque interne de l'appliance auquel aucun utilisateur ou administrateur n'a accès. Ces secrets sont protégés par le chiffrement et le montage en RAM des partitions, et par le chiffrement du fichier de configuration avant son partage entre les VM.

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	[F.FILTRAGE]	[F.TRAITEMENT.ENTREE]	[F.CLOISONNEMENT]	[F.COMMUNICATIONS SECURISEES]	[F.MAJ SECURISEE]	[F.CONTROLE ACCES]	[F.AUTHENTIFICATION]	[F.JOURNALISATION LOCALE]	[F.EXPORT SECURISE]	[F.PROTECTION DISPONIBILITE]	[F.AUTOPROTECTION]
[M.CONTOURNEMENT FILTRAGE]	√										
[M.TRANSFERT MALVEILLANT]	√	√						√			
[M.CORRUPTION CAGE]			√		√						√
[M.CORRUPTION FLUX]				√							
[M.CORRUPTION MISE A JOUR]				√	√			√			
[M.CORRUPTION ADMIN]	√		√								
[M.CORRUPTION CONFIGURATION]			√			√		√			√
[M.USURPATION]		√					√	√			
[M.CORRUPTION JOURNAUX LOCAUX]			√			√	√				
[M.CORRUPTION EXPORT]				√				√	√		
[M.PERTE DISPONIBILITE]		√	√			√				√	

Fin du document