PROFIL DE FONCTIONNALITÉS ET DE SÉCURITÉ - SAS ET STATION BLANCHE (RÉSEAUX NON CLASSIFIÉS)

GUIDE ANSSI

ANSSI-PG-076
01/07/2020

Informations

Attention

Ce document rédigé par l'ANSSI présente les « **Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés) »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence ouverte v2.0 » publiée par la mission Etalab [6].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Ces recommandations n'ont pas de caractère normatif, elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	01/07/2020	Version initiale

Table des matières

1
Introduction

1.1 Contexte et objectif

Les menaces liées à la connexion de périphériques amovibles dans les systèmes d'information sont diverses :

- insertion d'un fichier malveillant dans le système d'information à protéger ;
- attaque en intégrité/confidentialité lors du transfert du fichier sur un média amovible ;
- média réalisant des attaques au niveau de la pile logicielle du média amovible ;
- média réalisant des attaques en déni de service au niveau du contrôleur de média ;
- média se comportant comme un périphérique de type clavier ou souris et permettant de véhiculer des fichiers malveillants sur le système d'information à protéger.

Dans certains cas, le périphérique amovible est le seul moyen de transférer des informations d'un système à un autre (cas des systèmes isolés par exemple). Ce constat impose aux entités de se protéger en installant des outils spécifiques au sein de leur système d'information pour prévenir les risques liés à ces médias.

Information

L'utilisation d'équipements de type sas ou station blanche doit se faire dans un objectif global de contrôle des médias amovibles. En effet, le déploiement de tels équipements n'est pas suffisant et doit être accompagné de mesures organisationnelles définissant la politique de gestion des médias amovibles (limitation de l'usage des médias amovibles, désactivation des ports des médias amovibles sur les postes non dédié à ces transferts, etc.).

1.2 Objet du document

Le présent document constitue le profil de fonctionnalités et de sécurité pour les sas et les stations blanches. Il a pour objectif de définir les fonctions de sécurité attendues et les exigences associées à ce type de produit. C'est un élément de doctrine destiné à aider les clients dans leur expression du besoin et les éditeurs dans la conception de leur produit.

Les éditeurs doivent l'utiliser comme profil de protection tout en respectant les exigences qui y sont décrites dès lors qu'ils souhaitent présenter ce type de produit en qualification.

Attention

Cette version traite de l'import des données sur des réseaux non classifiés. L'export des données et les réseaux classifiés ne sont pas traités dans ce document.

1.3 Définitions

Exigence

Contrainte sur une fonction.

Point d'insertion de données

Poste de travail ou serveur dont les ports de médias amovibles sont au moins en partie ouverts afin de permettre l'import de données vers le réseau opérationnel.

Station blanche

Poste de travail ou serveur isolé du réseau opérationnel, dédié à l'analyse anti-malware des médias amovibles et des données qui y sont stockées. Ce dispositif donne des garanties raisonnables quant à l'innocuité du média amovible et des données transférées vers le réseau opérationnel.

Sas d'import de données

Association d'une station blanche et d'un point d'insertion de données. Lors d'un import de données, l'utilisation de la station blanche et du point d'insertion de données est impératif. La station blanche et le point d'insertion de données sont physiquement cloisonnés. Ce dispositif, interconnecté au réseau opérationnel, garantit l'innocuité du média amovible et des données transférées à destination de ce réseau.

1.4 Abréviations

- **HID** : Human interface Device. Il s'agit d'un périphérique informatique utilisé par un humain (clavier, souris, etc.).
- **PID** : Point d'insertion de données.
- **SI** : Système d'information.

2
Descriptif du produit

2.1 Descriptif général du produit

Le produit considéré est un sas d'import de données ou une station blanche destiné à assurer un contrôle des supports amovibles et des données présentes. Seules les données sélectionnées par l'opérateur pourront être transférées vers un réseau opérationnel. Le produit doit agir en coupure pour éviter, autant que possible, l'insertion sur le réseau opérationnel d'éléments non conformes à la politique de sécurité.

2.2 Environnement d'utilisation

L'environnement du produit, ainsi que les attaquants menaçant les biens sensibles à protéger, sont décrits selon la figure 1 (les attaquants sont positionnés selon les cas d'usage conformément aux annexes B et C du présent document).

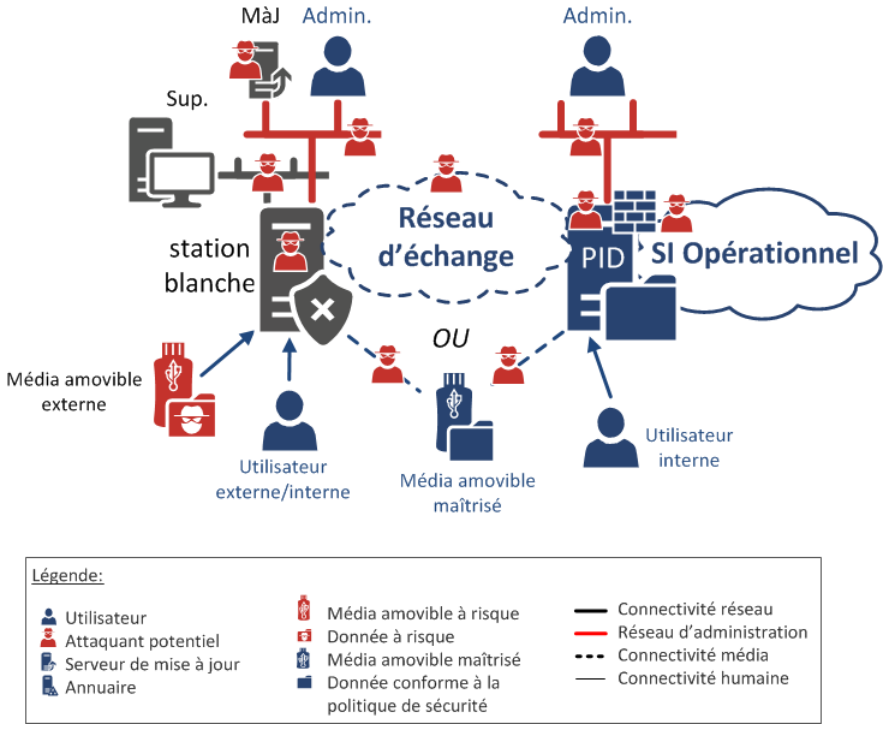

FIGURE 1 – Architecture de l'environnement du produit et présence de l'attaquant

2.3 Périmètre du produit

2.3.1 Matériel

Le périmètre matériel du produit contient :

- la station blanche ;
- le PID éventuel s'il est spécifique à la solution.

2.3.2 Logiciel

Le périmètre logiciel du produit contient :

- le système d'exploitation de la station blanche ;
- le système d'exploitation du PID si ce dernier est spécifique à la solution ;
- les fonctions de la station blanche ;
- les fonctions éventuellement présentes sur le PID.

2.4 Descriptif des utilisateurs

La liste des types d'utilisateurs susceptibles d'interagir avec le produit est la suivante :

- **Administrateur** : Utilisateur ayant les droits de modifier une partie de la configuration du produit. Il ne peut pas modifier les comptes d'administrateurs ;
- **Super-administrateur** : Utilisateur ayant tous les droits sur le produit et qui peut également créer, modifier ou supprimer les comptes d'administrateurs ;
- **Utilisateur** : Utilisateur ayant les droits nécessaires pour se connecter au réseau opérationnel et également pour transférer des données depuis le produit vers ce réseau.

3
Hypothèses

3.1 Hypothèses sur l'environnement

Les hypothèses sur l'environnement du produit sont les suivantes :

H1 Local

Le produit n'est pas nécessairement dans un local sécurisé et l'attaquant peut avoir accès à toutes les interfaces physiques (Médias et Ethernet). De façon similaire, l'attaquant peut arriver à faire brancher un dispositif piégé (par exemple une clé USB) sur n'importe quel port physique du produit. Il est considéré que l'attaquant ne peut pas démonter le produit ou effectuer d'attaque physique (soudure, etc.).

En revanche, des exemplaires identiques au produit étant disponibles dans le commerce, l'attaquant peut acheter un tel produit afin d'y rechercher des vulnérabilités par tous les moyens à sa disposition.

H2 Poste d'administration

Le poste d'administration du sas ou de la station blanche est sécurisé et maintenu à jour de toutes les vulnérabilités connues concernant le système d'exploitation et les applications utilisées. La station d'administration est installée dans un local à accès contrôlé/protégé.

3.2 Hypothèses sur le produit

Les hypothèses sur le produit sont les suivantes :

H3 Dimensionnement

Le produit est dimensionné pour répondre aux contraintes de l'environnement dans lequel il est déployé (capacité de traitement des fichiers, bande passante éventuelle, etc.).

H4 Utilisateurs

Les utilisateurs du produit sont informés de la manière de l'utiliser et disposent d'une documentation associée.

H5 Administrateurs

Les administrateurs du produit sont compétents, formés et non hostiles.

H6 Consultation des journaux par les administrateurs

Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par le produit.

H7 Intégrité du produit

Le produit est à jour de l'ensemble des correctifs de sécurité en vigueur et des dernières versions des bases antivirales. La configuration usine est également intègre.

H8 Réseau opérationnel

Le réseau de destination (ou réseau opérationnel) n'est pas considéré comme un réseau maîtrisé.

4
Biens sensibles à protéger

Information

Le texte en rouge correspond au(x) bien(s) à prendre en compte de façon facultative.

4.1 Biens sensibles du produit

Les biens sensibles sont les suivants :

B1	Logiciels du produit

- Les logiciels du produit (système d'exploitation, application, base de signatures virales, etc.) sont considérés comme des biens sensibles. Ils doivent être protégés en disponibilité, intégrité et authenticité.

B2	Base des utilisateurs

- La base des utilisateurs et administrateurs du produit, leurs informations d'authentification auprès du produit et leurs droits d'accès sont à protéger en disponibilité, confidentialité et intégrité.

B3	Configuration

- La configuration du produit est à protéger en disponibilité et en intégrité.

B4	Eléments cryptographiques

- Le produit traite et stocke des éléments cryptographiques (mots de passe, clés de chiffrement/déchiffrement, clés de signature, vérification de signatures, etc.) pour assurer ses fonctions de sécurité. Ce bien est à protéger en disponibilité, confidentialité et intégrité.

B5	Politique de gestion des droits

- Cette politique peut être contenue en local sur le produit ou être obtenue à partir d'un annuaire distant. Ce bien est à protéger en disponibilité et intégrité.

B6	Journaux d'évènements

- Les évènements de sécurité sont journalisés localement et de façon déportée. Ce bien est à protéger en disponibilité et intégrité. Les journaux doivent être également authentifiés lorsqu'ils sont déportés.

B7	Journaux de transfert de fichier(s)

- Les informations liées au transfert de fichier(s) sont journalisées localement et de façon déportée. Ce bien est à protéger en disponibilité et intégrité. Les journaux doivent être également authentifiés lorsqu'ils sont déportés.

B8	Contrôleur(s) USB du produit

- Le produit doit être équipé d'une protection contre la destruction par surtension positive ou négative du contrôleur USB. Le contrôleur est à protéger en disponibilité et intégrité.

4.2 Biens sensibles de l'environnement

B9	Les flux du réseau d'administration

- Ce bien est à protéger en confidentialité, intégrité et authenticité.

B10	Le SI opérationnel

- Ce bien est à protéger en intégrité.

B11	Données analysées

- Le fichier à analyser doit être protégé en intégrité.

B12	Média d'import

- Le média utilisé pour l'import des données doit être protégé en intégrité.

B13	Résultat de l'analyse

- Les données issues de l'analyse du fichier par le produit doivent être protégées en confidentialité.

Biens sensibles		Disponibilité	Intégrité	Confidentialité	Authenticité
B1	Logiciels du produit	✗	✗		✗
B2	Base des utilisateurs	✗	✗	✗	
B3	Configuration	✗	✗		
B4	Eléments cryptographiques	✗	✗	✗	
B5	Politique de gestion des droits	✗	✗		
B6	Journaux d'évènements	✗	✗		
B7	Journaux de transfert de fichier(s)	✗	✗		
B8	Contrôleur(s) USB du produit	✗	✗		
B9	Les flux du réseau d'administration		✗	✗	✗
B10	Le SI opérationnel		✗		
B11	Données du fichier(s) à analyser		✗		
B12	Média d'import		✗		
B13	Résultat de l'analyse			✗	

TABLE 1 – Biens sensibles du produit

5
Menaces

5.1 Profils des attaquants

Les attaquants à considérer sont :

- **Utilisateur légitime**
  Utilisateurs du produit ayant accès à ce dernier et insérant un média compromis ou réalisant une erreur de manipulation ;
- **Utilisateur non autorisé**
  Toute personne pouvant accéder physiquement au produit en exploitation ;
- **Attaquant avec des droits d'administration**
  L'attaquant a réussi à compromettre le compte d'un administrateur. Ce compte peut avoir n'importe quel rôle à l'exception du super-administrateur.

5.2 Descriptif des menaces

Information

Le texte en rouge correspond au(x) menace(s) à prendre en compte de façon facultative.

Les menaces à considérer sont les suivantes :

M1 Compromission
Un attaquant, via l'une des interfaces réseau ou média du produit, prend connaissance ou altère des biens sensibles en confidentialité ou en intégrité (logiciel ou matériel, destruction d'un contrôleur USB, carte SD, etc. ou compromission du SI opérationnel, etc.) ;

M2 Contournement
Un attaquant, via l'une des interfaces réseau ou média du produit, parvient à transférer des données de manière illégitime, en contournant la politique de sécurité du produit (filtrage, analyse anti-virale, etc.) ;

M3 Usurpation d'identité
Un attaquant, via l'une des interfaces réseau du produit, usurpe l'identité d'un utilisateur ou d'un administrateur du produit ;

M4 Indisponibilité

Un attaquant, via l'une des interfaces réseau ou média du produit, rend indisponible tout ou partie des fonctions des sécurité du produit de manière temporaire ou définitive (vulnérabilités connues ou non) ;

M5 Corruption d'une mise à jour

Un attaquant parvient à corrompre une mise à jour dans le but d'altérer le fonctionnement du produit (injection de code malveillant dans le firmware, corruption des bases virales, etc.) ;

M6 Corruption des journaux d'évènements

L'attaquant parvient à supprimer ou modifier une entrée dans les journaux d'évènements locaux sans y avoir été autorisé. L'attaquant parvient à modifier ou supprimer une entrée de journal distant émise par le produit sans que le destinataire ne puisse s'en rendre compte. L'attaquant parvient à modifier ou supprimer une émission de journalisation distante sans que le destinataire ne puisse s'en rendre compte ;

M7 Corruption des journaux de transfert de fichier(s)

L'attaquant parvient à supprimer ou modifier une entrée dans les journaux locaux de transfert de fichier(s) sans y avoir été autorisé. L'attaquant parvient à modifier une entrée de journal distant émise par le produit sans que le destinataire ne puisse s'en rendre compte.

6
Fonctions du produit

6.1 Fonctions de sécurité du produit

Information

Le texte en rouge correspond au(x) exigence(s) à prendre en compte de façon facultative.

FS1 Obligatoire	***Transfert sécurisé de fichier(s)*** : le produit doit permettre le transfert de fichier(s) depuis un média amovible tout en garantissant l'innocuité du support et des fichiers (le produit doit être conçu de telle sorte que son intégrité et son fonctionnement ne puissent pas être altérés par un média amovible ou un fichier). L'analyse d'un fichier ne doit pas dégrader la disponibilité du produit.

Exigences :

- Le produit effectue un transfert de fichier(s) avec ou sans modification (statification) selon le type de fichier, le format de fichier et l'analyse antivirale ;
- En cas de modification, cette dernière doit échouer si le format de fichier n'est pas reconnu. Si aucune modification n'est réalisée par l'analyse, l'utilisateur doit pouvoir s'assurer que ce fichier est intègre ;
- En cas d'échec de l'analyse des fichiers ou de nocuité avérée d'un fichier, l'utilisateur et les opérateurs du produit doivent être notifiés et aucun des fichiers présents ne doit être transféré ;
- Le transfert ne doit pas être effectué en mode privilégié depuis le système d'exploitation. Les privilèges des applications et processus doivent être réduits au minimum requis ;
- La vérification du type de fichier ne doit pas être contournable par ;
- Le produit doit permettre l'analyse de fichier protégé par un mot de passe (si le mot de passe n'est pas saisi le transfert ne sera pas exécuté) ;
- La saisie du mot de passe, s'il existe, et l'ouverture du document doivent être réalisées dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, l'environnement doit être dédié et sécurisé conformément au guide de sécurisation d'une configuration GNU/Linux [1] (des mesures similaires doivent être mises en œuvre en cas d'utilisation d'un autre système d'exploitation) ;
- Les fichiers doivent être analysés de manière récursive (à l'intérieur du fichier) dans un court délai (inférieur à 10 minutes pour l'analyse du média) quel que soit le résultat de l'analyse (échec

ou réussi). Lorsque ce délai est échu, une action est réalisée. Cette action peut être configurée par l'administrateur (refus de transfert, demande de validation du transfert par l'utilisateur, etc.).

FS2 Facultatif	***Transfert par statification*** : le produit doit permettre le transfert de certains fichiers selon la méthode de statification.

Exigences :

- Le transfert par statification ne doit pas s'appliquer sur les fichiers binaires. Ce transfert doit s'appliquer par exemple sur des fichiers images, des fichiers bureautiques (pour suppression des macros par exemple), etc. ;
- Chaque transformation de fichier doit être exécutée dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, par exemple, un « conteneur » ou une machine virtuelle, il est nécessaire d'appliquer le principe de moindres privilèges conformément au guide de sécurisation d'une configuration GNU/Linux [1] ;

FS3 Obligatoire	***Affichage de la liste de fichier(s)*** : le produit doit permettre de lister le contenu du média d'entrée ainsi que celui de sortie pour la sélection des fichiers à transférer et leurs vérifications.

Exigences :

- Tous les fichiers contenus dans le média d'entrée doivent être présentés à l'écran (ainsi que leurs métadonnées), y compris les fichiers cachés ;
- Seuls les fichiers sélectionnés doivent être copiés pour l'import. Il est possible d'utiliser une liste blanche des formats de fichiers tolérés incluant les formats de fichiers « Métier » ;
- Le filtrage des fichiers à analyser doit être basé sur une analyse du contenu et pas uniquement sur l'extension ;
- Le produit doit permettre de placer en quarantaine (depuis l'interface du produit) un fichier jugé à risque par l'utilisateur.

FS4 Facultatif	***Journalisation sécurisée des transferts de fichiers*** : le produit doit sauvegarder les informations concernant le transfert de fichier (nom et type de médias d'entrée et de sortie, nom et type de fichier, résultat du transfert, résultat de l'analyse anti-virale, dates, etc.). La station doit assurer l'imputabilité des transferts entrants et/ou sortants.

Exigences :

- Lorsque la capacité de stockage est atteinte, les opérateurs du produit doivent être notifiés et une rotation du fichier de journalisation doit être effectuée ;
- Les journaux doivent être protégés en intégrité et doivent être accessibles à tout moment par l'administrateur du produit (se référer au guide de mise en oeuvre d'un système de journalisation [2]) ;
- Les fonctions liées à la journalisation doivent être réalisées dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, l'environnement doit être dédié et sécurisé conformément au guide de sécurisation d'une configuration

GNU/Linux [1]. Des mesures similaires doivent être mises en œuvre en cas d'utilisation d'un autre type de cloisonnement d'environnement (machine virtuelle par exemple) ;

- Les journaux générés doivent contenir les informations concernant l'utilisateur authentifié qui a réalisé le transfert.

FS5 Obligatoire	***Analyse de sécurité*** : le produit doit réaliser une analyse antivirale systématique des fichiers à importer.

Exigences :

- L'analyse antivirale doit s'effectuer uniquement lors du transfert d'un fichier ;
- Le(s) antivirus doi(ven)t être exécuté(s) dans un environnement cloisonné matériellement ou logiciellement. En cas d'utilisation d'un cloisonnement logiciel, par exemple par « conteneur » ou machine virtuelle, il est nécessaire d'appliquer le principe de moindres privilèges conformément au guide de sécurisation d'une configuration GNU/Linux [1]. Quel que soit le cloisonnement utilisé, l'environnement doit être réinitialisé entre deux analyses et le système de fichier racine doit être monté en lecture seule ;
- L'analyse antivirale doit supporter plusieurs moteurs d'antivirus différents. Le choix des moteurs peut être laissé à la discrétion du client ;
- L'analyse antivirale des fichiers doit pouvoir utiliser plusieurs sources de signatures. le choix source peut être laissé à la discrétion du client ;
- L'analyse antivirale des fichiers ne doit pas être contournable ;
- L'authenticité et l'intégrité des mises à jour des signatures et du moteur doivent être vérifiées par le produit ;
- La base antivirale et le moteur doivent pouvoir être mis à jour en mode déconnecté.

FS6 Obligatoire	***Chiffrement*** : le produit stocke les secrets de connexion des administrateurs (Pas d'authentification utilisateur sur la station blanche nécessaire. L'authentification sur le PID s'effectue auprès du SI opérationnel pour les utilisateurs.

Exigences :

- Les secrets de connexion doivent respecter les recommandations de l'annexe B1 du RGS V2 [4] ;
- Le produit doit intégrer un chiffrement de surface complet du disque sur lequel le système d'exploitation est installé (les secrets de connexion des utilisateurs doivent être protégés — en confidentialité et intégrité — des autres processus disposant de droits d'exécution en lecture sur le disque).

FS7 Obligatoire	***Identification, authentification et contrôle d'accès*** : le produit identifie et authentifie les administrateurs permettant de contrôler les ressources selon les droits de ces derniers.

Exigences :

- Le produit doit intégrer les recommandations relatives au guide de sécurisation de la configuration d'un système GNU/Linux [1].

  Des mesures similaires doivent être mises en œuvre en cas d'utilisation d'un autre système d'exploitation.

FS8 Obligatoire	***Intégrité des logiciels*** : le produit permet de mettre à jour les logiciels le constituant (système d'exploitation et logiciel(s) spécifique(s)).

Exigences :

- L'authenticité et l'intégrité de la mise à jour des logiciels du produit doivent être vérifiées ;
- Le système ne doit pas pouvoir être mis à jour avec une version antérieure des logiciels qui le composent (système d'exploitation, logiciels métiers, bases antivirales, etc.).
- Les fichiers binaires, les politiques de sécurité et les configurations de la solution logicielle du produit doivent être protégés en intégrité.

FS9 Obligatoire	***Intégrité des journaux d'évènements*** : le produit journalise l'ensemble des opérations effectuées par les utilisateurs et par lui-même (hors transfert de fichier(s)).

Exigences :

- Lorsque la capacité de stockage est atteinte, une rotation des fichiers est effectuée (conformément au guide de mise en œuvre d'un système de journalisation [2]) ;
- Les journaux doivent être protégés en intégrité ;
- Les journaux doivent pouvoir être émis à un collecteur. Les journaux déportés doivent être protégés en intégrité et authenticité ;
- Les fonctions liées à la journalisation doivent être exécutées avec des comptes non privilégiés.

FS10 Obligatoire	***Protection des flux*** : les flux d'administration entrants et sortants du produit doivent être sécurisés.

Exigences :

- Le produit protège en confidentialité, en intégrité et en authenticité, toutes les actions réalisées à distance par les administrateurs ;
- Le produit doit être équipé d'une interface d'administration dédiée conformément au guide [3].

FS11 Obligatoire	***Cloisonnement*** : les fonctions métier (administration, transfert, analyse, etc.) du produit sont cloisonnées afin de limiter la prise de contrôle à distance et le risque de rebond.

Exigences :

- Chaque processus doit être exécuté dans un environnement cloisonné matériellement ou logiciellement, par exemple par « conteneur » ou machine virtuelle.

- L'analyse de fichier doit être réalisée dans l'espace utilisateur du système d'exploitation et doit permettre d'identifier l'utilisateur ayant effectué le transfert (conformément au guide de cloisonnement système [5]).

FS12 Obligatoire	***Dimensionnement*** : le produit doit être correctement dimensionné afin de prendre en compte les contraintes de délai de transfert, de capacité de stockage etc.

Exigences :

- Le produit doit être résilient lorsque la capacité de rétention des journaux de fonctionnement et d'alertes est atteinte ;
- Le produit doit être correctement dimensionné afin de prendre en compte une durée d'analyse du média acceptable par l'utilisateur (inférieur à 10 minutes par exemple).Cette durée peut être configurée par l'administrateur.

FS13 Obligatoire	***Intégrité des médias entrants et sortants*** : le produit doit garantir l'intégrité des médias insérés, qu'ils soient entrants ou sortants.

Exigences :

- Des mesures organisationnelles doivent être proposées par le soumissionnaire afin d'éviter la mise en place de médias pouvant présenter un firmware non légitime ;
- Les flux de données échangés entre les médias d'entrée et de sortie et le produit doivent être unidirectionnels (se reporter à l'annexe C du présent document) ;
- L'analyse effective du média par le produit doit être vérifiée avant d'importer des données du PID vers le SI opérationnel.

FS14 Obligatoire	***Intégrité du produit*** : quel que soit le média d'entrée ou de sortie, son insertion ne doit pas porter atteinte à l'intégrité du produit.

Exigences :

- Les ports autres que ceux utilisés par les médias d'entrée et de sortie doivent être physiquement inaccessibles ;
- Dans le cas d'une station blanche, les contrôleurs des interfaces des médias d'entrée et de sortie doivent être composés de firmware distincts et la compromission d'une interface d'entrée ne doit pas compromettre l'interface de sortie (voir l'annexe B) ;
- Dans le cas d'une station blanche, l'utilisation du même média sur le point d'entrée de la station et le point de sortie est à proscrire (voir l'annexe B) ;
- Le produit ne doit pas permettre l'amorçage depuis un support amovible ;
- Aucun des fichiers importés ou présents sur le média d'entrée ne doit pouvoir être exécuté par le produit ;
- L'intégrité et l'authenticité du processus de démarrage du système doivent être vérifiées (Secure Boot) ;

- L'accès aux paramètres de démarrage (BIOS, UEFI, UBOOT, etc.) du produit doit être protégé par authentification ;
- Les médias d'entrée et de sortie doivent être montés par le produit uniquement en tant que « MassStorage » (pas de montage de périphérique HID par exemple) ;
- Le média d'entrée doit être monté uniquement en lecture seule ;
- Un formatage standard doit être réalisé sur le média de sortie lors de la validation du transfert de fichier ;
- Les contrôleurs de média du produit doivent être protégés contre les surtensions (positives ou négatives) ;
- Le produit doit mettre en œuvre des mécanismes de protection physique contre l'effraction afin d'éviter ou de détecter une tentative de piégeage du produit ;
- Effectuer un effacement cryptographique de l'environnement utilisé. En effet, les données utilisées et produites lors du transfert de fichier(s) doivent pouvoir être effacées du produit (en mémoire et sur le disque) afin de réinitialiser l'environnement.

FS15 Obligatoire	***Filtrage dans le cas d'un PID raccordé à un réseau*** : Le produit doit protéger l'accès direct au réseau opérationnel depuis le PID.

Exigences :

- Le filtrage est unidirectionnel et assuré par une fonction de pare-feu ou de diode (se reporter à l'annexe B du présent document) ;
- Le filtrage autorise uniquement les communications sur des ports jugés nécessaires ;
- Pour accéder au réseau opérationnel depuis le PID, un espace de stockage dédié sera mis en place pour effectuer les transferts de fichier depuis le poste de travail de l'utilisateur.

Plusieurs architectures ont été identifiées pour réaliser les fonctions de sécurité du produit. Les deux suivantes sont traitées en exemple dans les annexes du document :

- un sas d'import de données qui permet d'utiliser un seul média amovible et de transférer les données souhaitées sur le réseau opérationnel au travers d'un espace d'échange ;
- une station blanche avec deux médias amovibles : un média amovible externe et un media amovible maîtrisé pour transférer les données depuis la station blanche vers le réseau opérationnel.

Annexe A
Matrices de couverture

A.1 Couverture des biens par les menaces

		B1 Logiciels du produit	B2 Base des utilisateurs	B3 Configuration	B4 Eléments cryptographiques	B5 Politique de gestion des droits	B6 Journaux d'évènements	B7 Journaux de transfert de fichier(s)	B8 Contrôleur(s) USB du produit	B9 Les flux du réseau d'administration	B10 Le SI opérationnel	B11 Fichier(s) à analyser	B12 Média d'import	B13 Résultat de l'analyse
M1	**Compromission**	**IA**	**CI**	**I**	**CI**	**I**	**I**	**(I)**	**I**	**CI**	**I**	**I**	**I**	**I**
M2	**Contournement de la politique de sécurité**	**AI**									**I**			
M3	**Usurpation d'identité**		**CI**							**A**				
M4	**Indisponibilité**	**D**	**D**	**D**	**D**	**D**	**D**	**(D)**	**D**					
M5	**Corruption d'une mise à jour**	**IA**		**I**										
M6	**Corruption des journaux d'évènements**						**DI**							
M7	**Corruption des journaux de transfert**							**(DI)**						

TABLE 2 – Atteintes aux biens sensibles en fonction des menaces

Légende : Disponibilité (D), Intégrité (I), Confidentialité (C), Authenticité (A)

A.2 Couverture des menaces par les fonctions de sécurité

		Compromission M1	Contournement de la politique de sécurité M2	Usurpation d'identité M3	Indisponibilité M4	Corruption d'une mise à jour M5	Corruption des journaux d'évènements M6	Corruption des journaux de transfert M7
FS1	**Transfert sécurisé de fichier(s)**		✗					
FS2	**Transfert par statification**		✗					
FS3	**Affichage de la liste de fichier**		✗					
FS4	**Journalisation sécurisée des transferts de fichier(s)**	(✗)			(✗)			(✗)
FS5	**Analyse de sécurité**	✗	✗					
FS6	**Chiffrement**							
FS7	**Identification, authentification et contrôle d'accès**			✗				
FS8	**Intégrité des logiciels**	✗	✗			✗		
FS9	**Intégrité des journaux d'évènement**	✗			✗	✗	✗	
FS10	**Protection des flux**	✗		✗				
FS11	**Cloisonnement**		✗		✗			
FS12	**Dimensionnement**				✗			
FS13	**Intégrité des médias entrants et sortants**	✗						
FS14	**Intégrité du produit**	✗	✗	✗	✗			
FS15	**Filtrage dans le cas d'un PID raccordé à un réseau**		✗					

TABLE 3 – Couverture des menaces par les fonctions de sécurité

Annexe B
Exemple : Station blanche à deux clés

B.1 Environnement d'utilisation

Les principes généraux sont schématisés figure 2.

L'utilisateur insère un média amovible externe sur la station blanche et désigne les éléments à transférer. Si les éléments sont conformes à la politique de sécurité appliquée, ils sont tranférés sur un média amovible maîtrisé.

Ce média amovible est ensuite branché sur le PID. Le PID vérifie : la présence d'un média maîtrisé et le précédent traitement par la station blanche. l'Utilisateur authentifié récupère les éléments. C'est à lui qu'incombe la responsabilité de les insérer sur le réseau opérationnel.

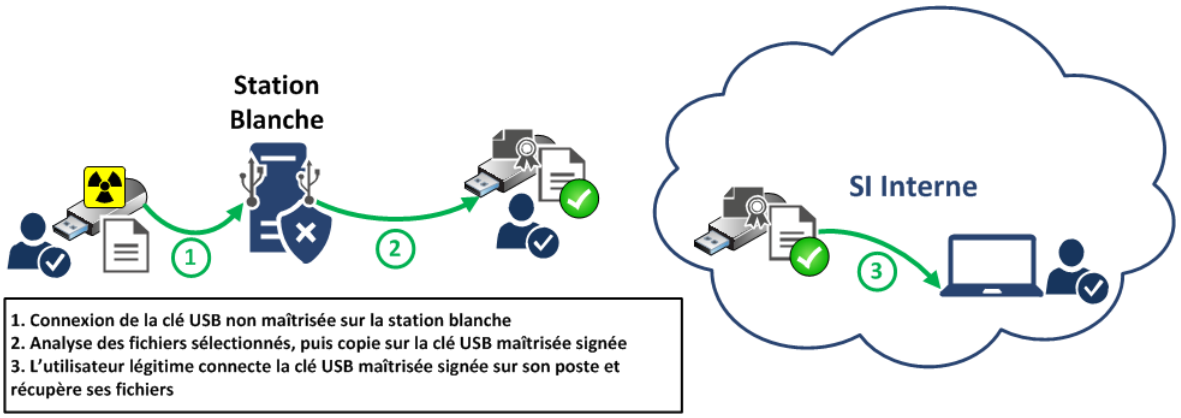

FIGURE 2 – Station blanche : principes généraux

B.2 Périmètre du produit

Le périmètre du produit est décrit à la figure 3. Deux composants majeurs doivent être présents : la station blanche et le PID. L'utilisateur insère le média amovible sur l'interface I3. Les données sont transférées sur un média amovible maîtrisé par l'interface I4. Ce média amovible maîtrisé est ensuite branché sur l'interface I5 pour être récupérées sur le PID. La connexion au serveur d'authentification interne s'effectue par l'interface I6. L'ensemble des composants sont administrés, supervisés et mis à jour au travers de réseaux d'administration [1] (Interfaces I1, I2, I7, I8).

1. Se référer au guide [3] pour plus d'informations.

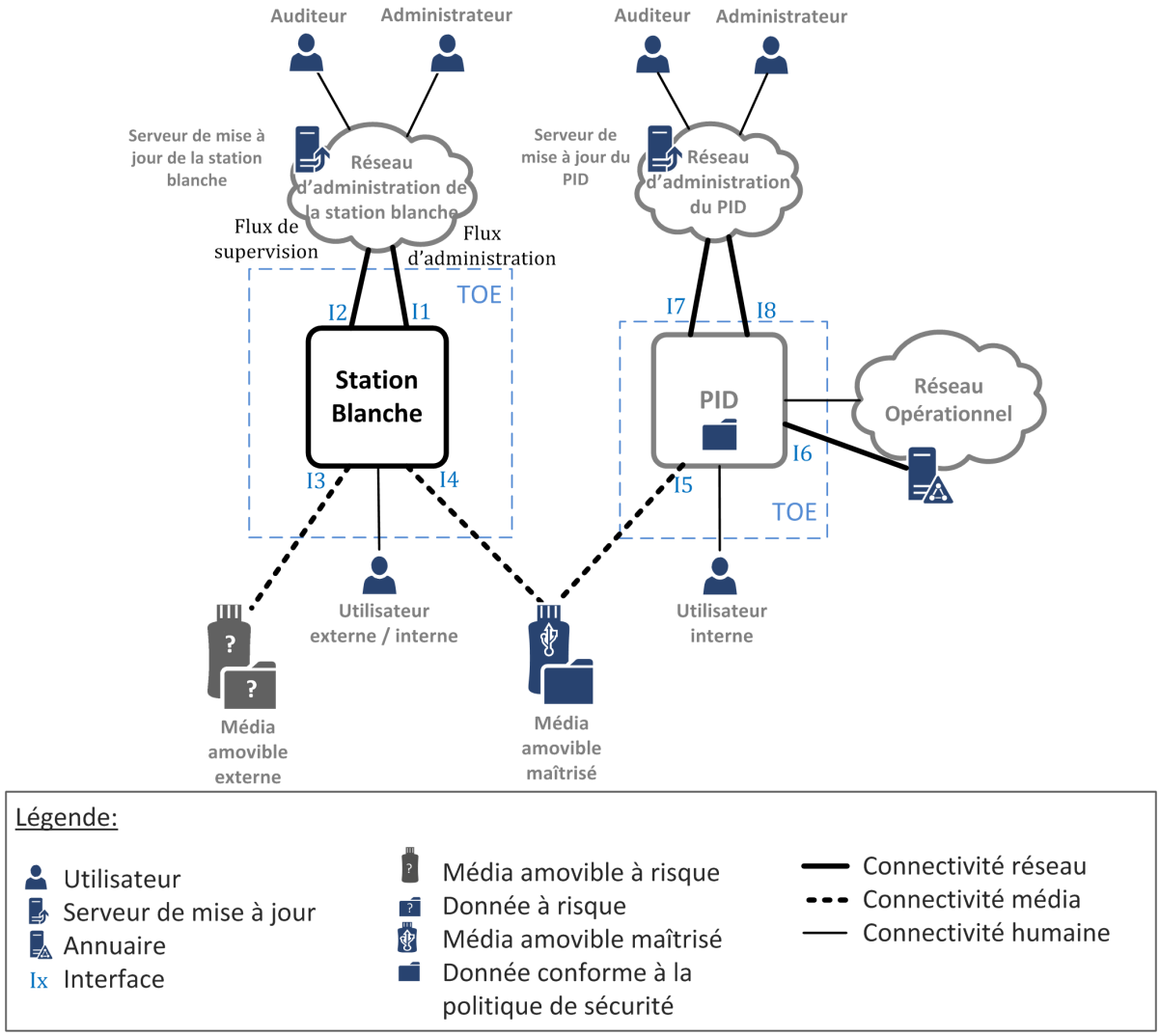

FIGURE 3 – Station blanche : détails et interfaces

B.3 Menaces

B.3.1 Profils des attaquants

Ces attaquants peuvent être positionnés comme représentés sur la figure 4.

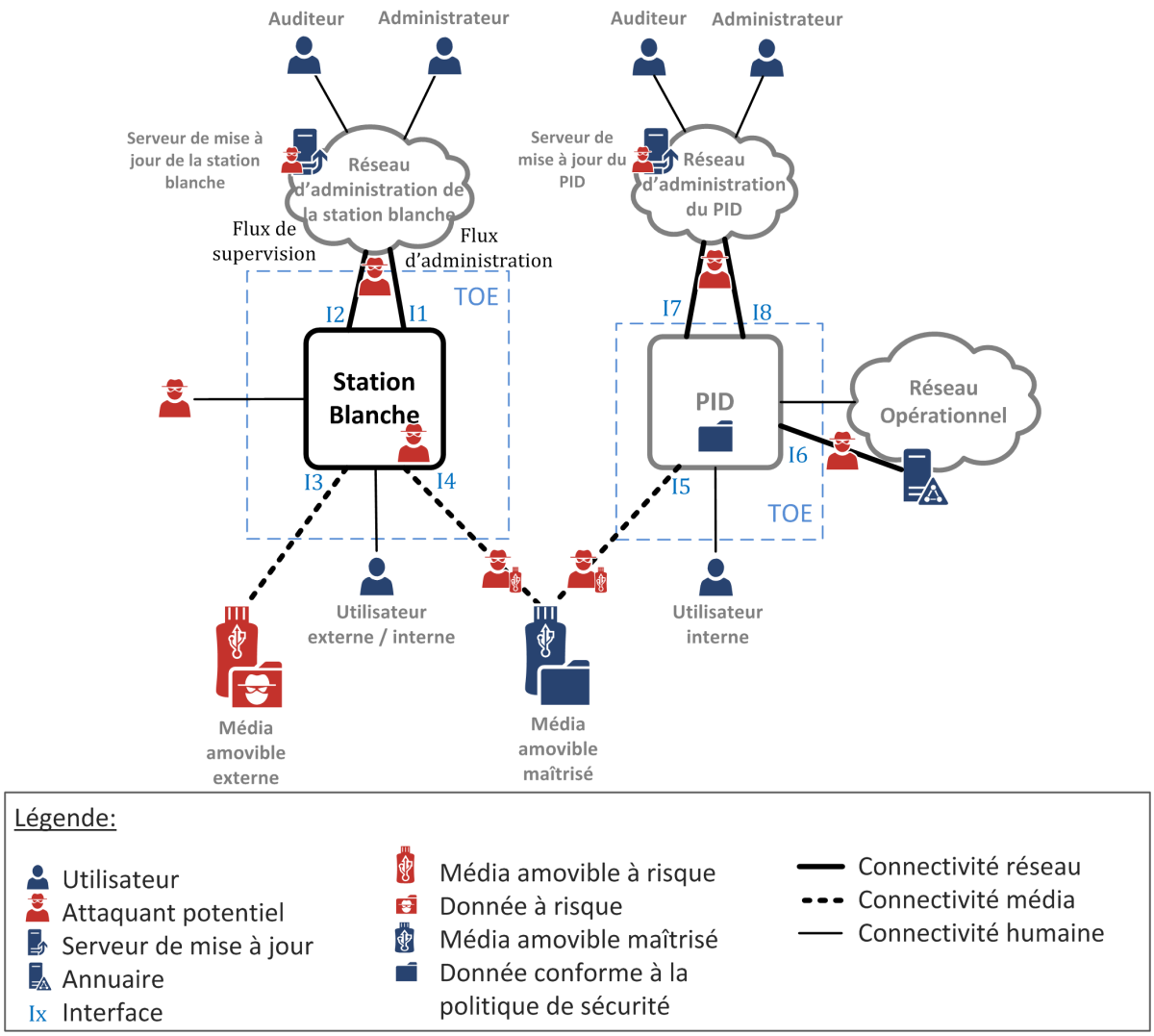

FIGURE 4 – sas : positionnement des attaquants

Annexe C
Exemple : Sas

C.1 Environnement d'utilisation

Les principes généraux sont schématisés figure 5.

L'utilisateur insère un média amovible externe sur le sas et désigne les éléments à transférer. Si les éléments sont conformes à la politique de sécurité appliquée, ils sont transférés dans un espace d'échange. Depuis le réseau opérationnel, un utilisateur authentifié récupère les éléments transférés sur cet espace d'échange. C'est à lui qu'incombe la responsabilité de les insérer sur le réseau opérationnel.

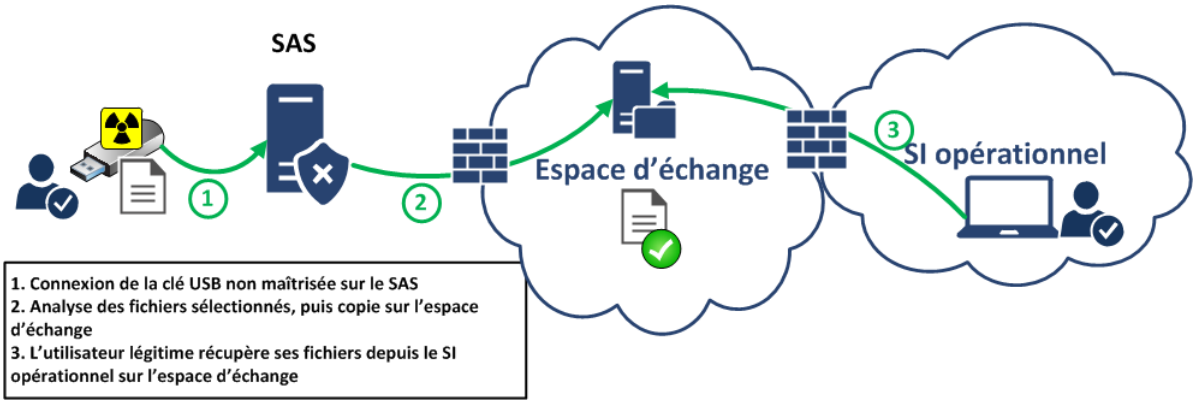

FIGURE 5 – Sas : principes généraux

C.2 Périmètre du produit

Le périmètre du produit est décrit à la figure 6. Deux composants majeurs doivent être présents : le sas d'import et l'espace d'échange (l'ensemble des éléments de la figure ci-dessous constitue une passerelle d'importation de fichier(s)). L'utilisateur insère le média amovible sur l'interface I3. Les données sont transférées sur l'espace d'échange par l'interface I9 et récupérées depuis le réseau opérationnel par l'interface I10. La connexion au serveur d'authentification interne s'effectue par l'interface I6. L'ensemble des composants sont administrés, supervisés et mis à jour en passant au travers de réseaux d'administration [2] (Interfaces I1, I2, I7, I8).

2. Se référer au guide [3] pour plus d'informations.

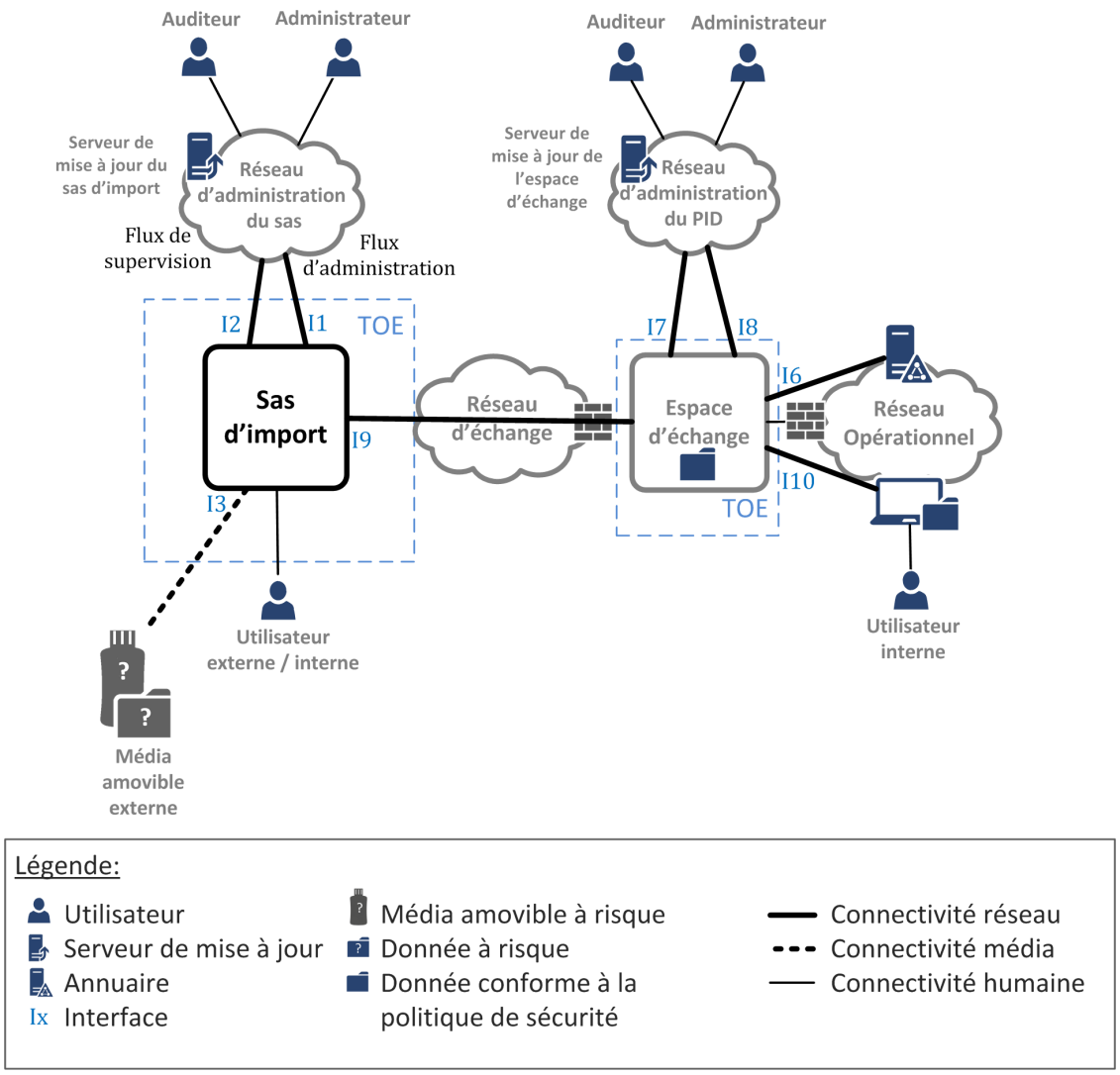

FIGURE 6 – exemple d'une passerelle d'importation de fichier(s) composée d'un sas et d'un espace d'échange

C.3 Menaces

C.3.1 Profils des attaquants

Ces attaquants peuvent être positionnés comme représentés sur la figure 7.

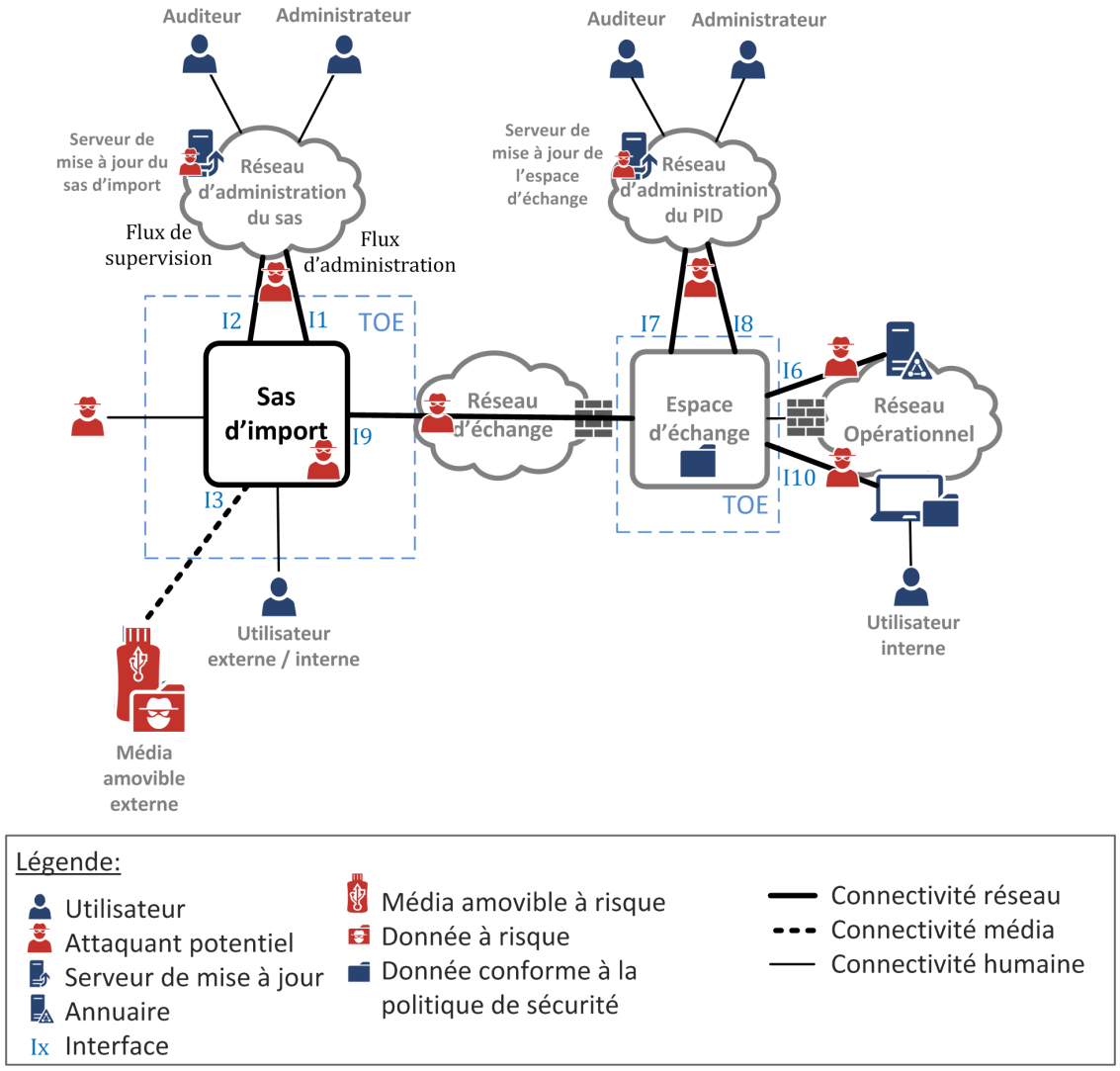

FIGURE 7 – passerelle d'importation de fichier(s) : positionnement des attaquants

Bibliographie

[1] *Recommandations de configuration d'un système GNU/Linux*.
Guide ANSSI-BP-028 v1.2, ANSSI, 2019.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[2] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[3] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[4] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[5] *Recommandations pour la mise en place de cloisonnement système*.
Guide ANSSI-PG-040 v1.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/guide-cloisonnement-systeme.

[6] *Licence ouverte / Open Licence*.
Page Web v2.0, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

ANSSI-PG-076
Version 1.0 - 01/07/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN