Secure the world together.

Cible de sécurité

Bwall – Bastion-Wall

Sommaire

Glossaire

Terme	Signification
ANSSI	Agence nationale de la sécurité des systèmes d'information
COM	Communication port
CSPN	Certification de Sécurité de Premier Niveau
IP	Internet Protocol
MAC	Media Access Control
ST	Straight Tip
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToE	Target of Evaluation
UDP	User Datagram Protocol
USB	Universal Serial Bus

1. Préambule

1.1. Objet du document

Ce document représente la cible de sécurité du produit ***Bwall***.
Cette cible de sécurité a été élaborée en vue d'une évaluation Certification Sécurité de Premier Niveau (CSPN).

1.2. Identification et suivi du document

Titre	Cible de sécurité Bwall
Version du document	1.8
Date de dernière révision	04/03/2021
Référence	GEOIDE_cible_Bwall_CSPN
Cible d'évaluation	Produit Bwall
Version de la ToE	GEN1-7.6.14

La cible de sécurité est conforme aux référentiels de l'ANSSI suivants :

- Référentiel Général de Sécurité version 2.0, annexe B1

Suivi des modifications :

Version du document	Date de la révision	Rédacteur	Approbateur
0.1	20/04/2018	Grégory GILLE	
0.2	05/05/2018	Grégory GILLE	
0.3	12/12/2018	Jérémie VERBRUGGHE	
0.4	30/03/2019	Grégory GILLE	
0.5	12/06/2019	Grégory GILLE	
0.6	20/09/2019	Jérémie VERBRUGGHE	
0.7	24/09/2019	Jérémie VERBRUGGHE	
0.8	25/02/2020	Jérémie VERBRUGGHE	
0.9	02/04/2020	Jérémie VERBRUGGHE	
1.0	14/04/2020	Jérémie VERBRUGGHE	Grégory GILLE
1.1	13/07/2020	Jérémie VERBRUGGHE	Grégory GILLE
1.2	21/07/2020	Jérémie VERBRUGGHE	Grégory GILLE
1.3	24/08/2020	Aurélien DARRAGON	Grégory GILLE
1.4	31/08/2020	Jérémie VERBRUGGHE	Grégory GILLE
1.5	12/01/2021	DARRAGON / VERBRUGGHE	Grégory GILLE
1.6	25/02/2021	Jérémie VERBRUGGHE	Grégory GILLE
1.7	01/03/2021	Jérémie VERBRUGGHE	Grégory GILLE
1.8	04/03/2021	Jérémie VERBRUGGHE	Grégory GILLE

2. Identification du produit

Organisation éditrice	GEOIDE Crypto&Com
Lien vers l'organisation	https://public.geoide.fr/
Nom commercial du produit	Bwall
Numéro de la version évaluée	GEN1-7.6.14
Catégorie de produit	Firewall

2.1. Identification physique

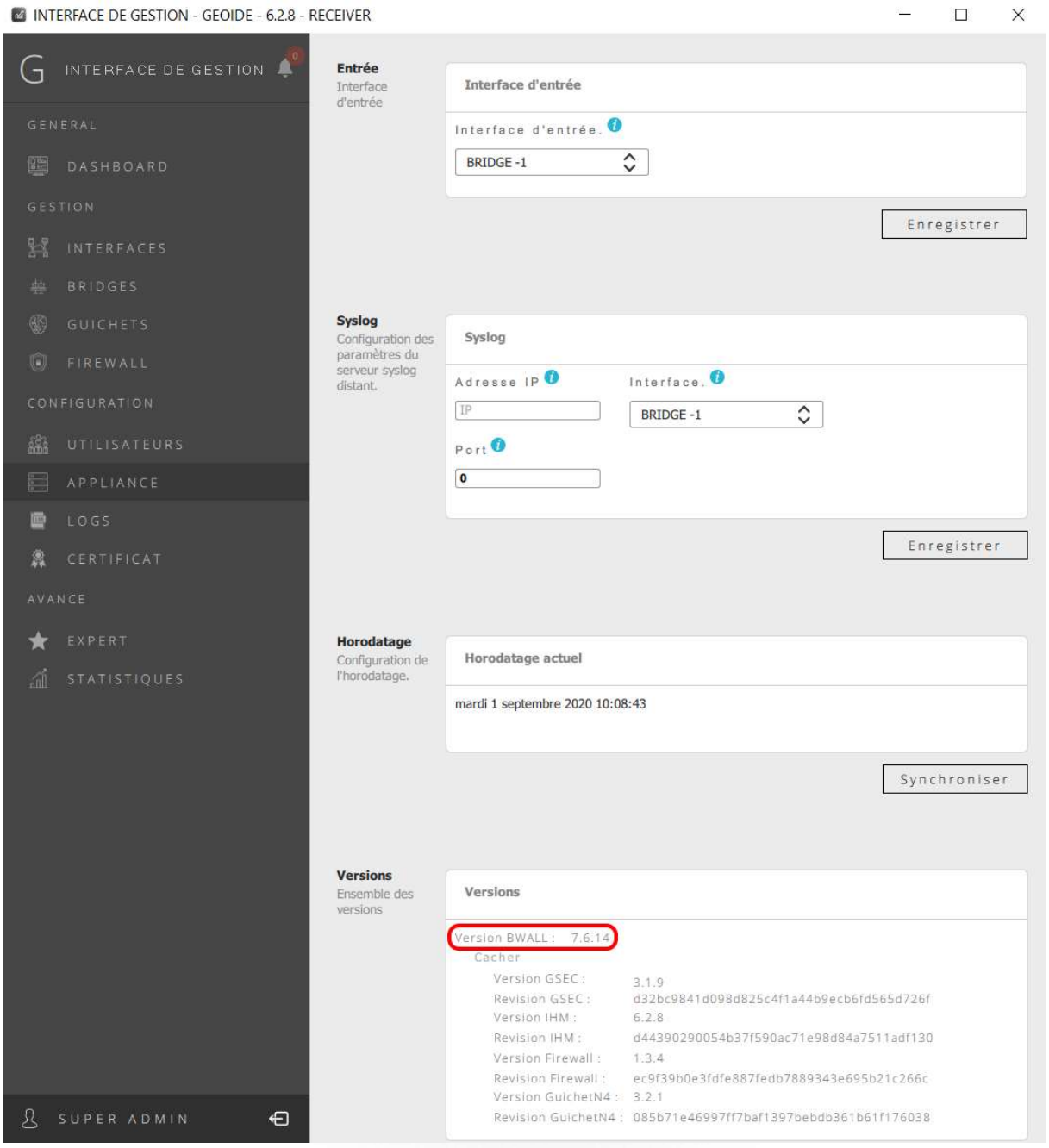
L'aspect physique du produit Bwall est le suivant :

- Face avant :

- Face arrière :

2.2. Identification logicielle

La partie logicielle du produit Bwall est identifiée par un numéro de version, visualisable via l'outil d'administration et de configuration (aussi appelé « interface de gestion »). Le libellé correspondant est « Version BWALL ».



La version évaluée est la version **7.6.14**.

3. Description du produit et ses options

3.1. Description générale du produit Bwall

Le produit évalué (ToE), nommé « Bwall », est une appliance fournie par la société GEOIDE Crypto&Com dont le fonctionnement est similaire à un pare-feu. Il agit en tant que routeur IP avec la fonction filtre. Il ne laisse transiter que les trames réseau dont l'adresse source et l'adresse destination sont autorisées à communiquer entre-elles. Il constitue un élément de type réseau.

Il ne fonctionne qu'en mode « liste blanche ».
Les règles autorisant le trafic doivent être configurées de manière exhaustive.
Une règle d'autorisation est un ensemble formé d'un émetteur et d'un destinataire, chacun pouvant être défini par :

- un numéro d'interface (celle de la ToE, sur laquelle est relié l'émetteur ou le destinataire),
- une adresse MAC,
- une adresse IP,
- un port,
- le protocole autorisé : TCP ou UDP.

Une trame ne correspondant pas à l'une des règles est automatiquement non transmise.

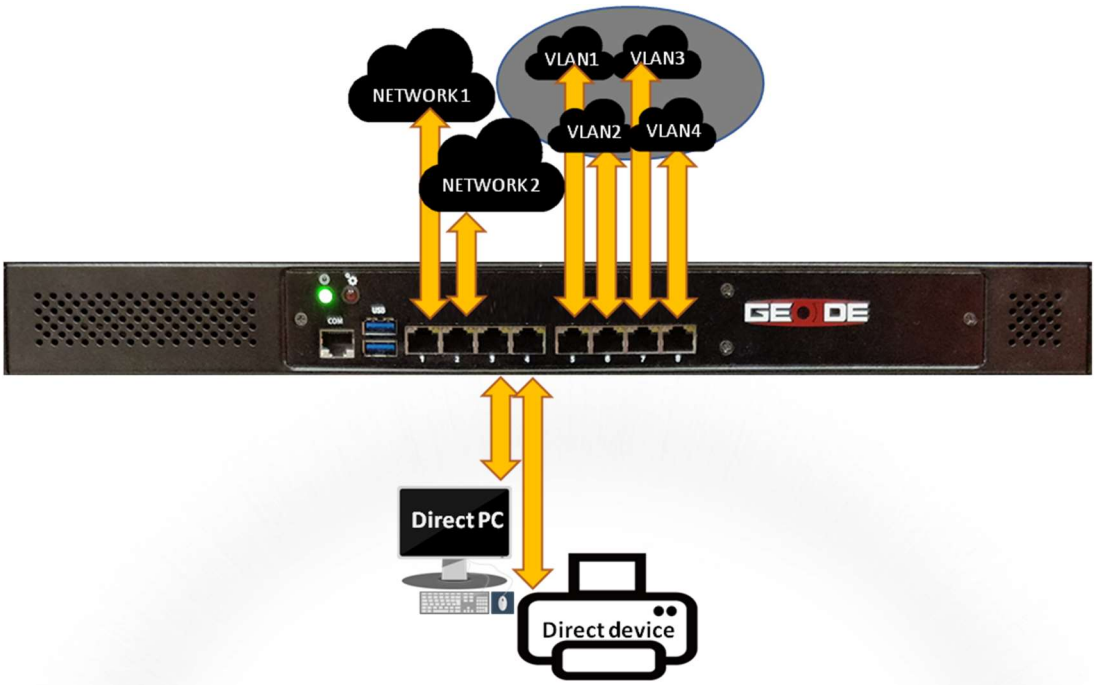
Il possède une spécificité qui consiste à créer des cloisonnements entre les systèmes connectés (bastion).

La configuration du produit est réalisée uniquement via le port série (port « COM »). L'outil logiciel d'administration et de configuration est fourni, mais la station sur laquelle il est exécuté ne l'est pas.

L'appliance Bwall est confectionnée en usine par GEOIDE Crypto&Com et livrée au client « prête à l'emploi ».

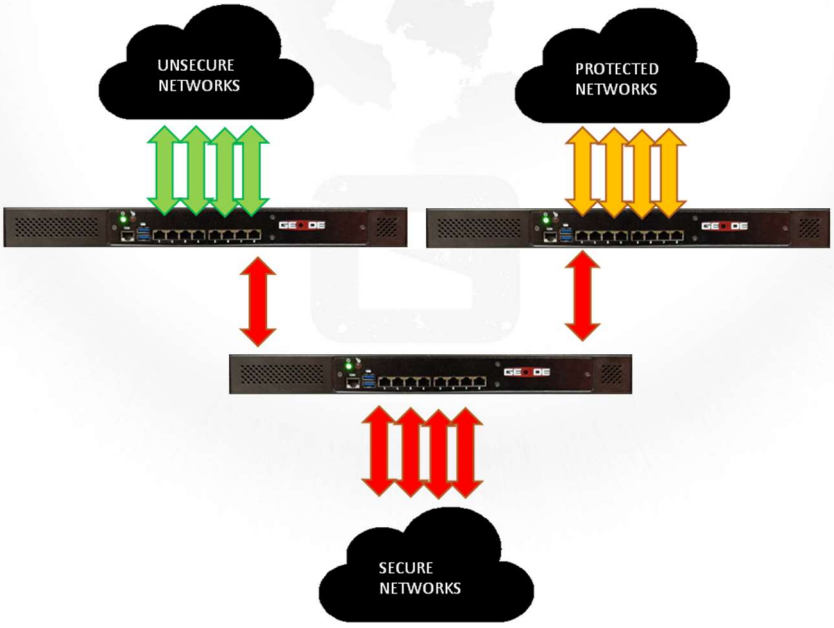
L'appliance Bwall se place en coupure des réseaux à cloisonner et garantit l'identification des flux entre ces réseaux.

Exemple d'architecture réseau type :



Les appliances Bwall sont scalables de manière à produire des architectures reliant plus de 8 réseaux ou à cloisonner les réseaux par niveau de protection ou classification.

Exemple d'architecture cloisonnée par niveau de protection :



3.2. Options disponibles non incluses dans l'évaluation

3.2.1. Option GuichetN4

L'option GuichetN4 est un logiciel additionnel installé dans l'appliance Bwall qui sert à créer un guichet unique qui concentre les connexions clientes à destination de serveurs distants en traversant une diode réseau. La diode utilisée peut être l'option Diode GEOIDE ou une autre diode du marché.

GuichetN4 simplifie les configurations réseaux et les tables de routages en concentrant tous les sous-réseaux sur une seule liaison de sortie.

Il possède un paramètre supplémentaire permettant de limiter les messages non conformes aux protocoles attendus.

La fonction « module » permet de filtrer des protocoles connus ou simuler des comportements de systèmes hôtes.

3.2.2. Option Diode

L'option Diode est une option physique ajoutée dans l'appliance Bwall qui permet de garantir un lien unidirectionnel vers ou depuis un système distant.

L'option diode ajoute donc une entrée ou une sortie sur une connexion fibre optique (ST).

4. Argumentaire du produit

4.1. Limite de l'évaluation

L'évaluation porte sur le périmètre fonctionnel suivant :

- la configuration des interfaces réseau et règles d'autorisation,
- le filtrage des flux réseau aux niveaux 2, 3 et 4,
- la journalisation des événements,
- la vérification d'intégrité des mises à jour.

L'évaluation fait l'hypothèse que les fonctions d'administration sont protégées par l'environnement du produit (locaux sécurisés, personnel de confiance). Pour cette raison, les menaces sur les fonctions d'administration ne sont pas prises en compte.

4.2. Manière d'utiliser le produit

Le produit, une fois démarré, reste actif en permanence.
Les administrateurs ont en charge sa configuration en fonction des besoins.

4.3. Environnement prévu pour son utilisation

Bwall est conçu pour être placé entre plusieurs réseaux et avoir un niveau de contrôle élevé sur les flux en transit grâce à l'identification des émetteurs et destinataires.

4.4. Hypothèses sur l'environnement

4.4.1. Environnement logique

H.STATION_CONFIGURATION

La station, sur laquelle s'exécute l'outil d'administration et de configuration, doit être maîtrisée et dédiée à l'administration et à la configuration de l'appliance Bwall. Elle doit être capable de communiquer avec l'appliance en s'y branchant sur le port série. Son système d'exploitation doit être Windows 10.

H.STATION_CONSULTATION

La station, sur laquelle s'exécute l'outil de consultation des journaux locaux, doit être capable de communiquer avec l'appliance en s'y branchant sur une interface réseau spécifiée lors de la configuration du produit. Son système d'exploitation doit être Windows 10.

4.4.2. Environnement physique

H.LOCAL_SÉCURISÉ

L'appliance Bwall doit se trouver dans des locaux sécurisés dont l'accès est nominativement contrôlé et restreint au super-administrateur, aux administrateurs et aux auditeurs. En particulier, l'attaquant n'aura pas physiquement accès à la ToE.

H.RÉSEAU_ADMIN_DÉDIÉ

L'action d'administration et de configuration de l'appliance est effectuée à partir d'un réseau séparé et dédié. L'outil d'administration et de configuration de la ToE s'exécute sur une station à relier à la ToE par le port série. Cette station est décrite plus loin dans ce document.

H.SOURCE_HORAIRE

L'environnement informatique intègre une source de signaux horaires sécurisée permettant la datation des enregistrements d'audit.
Dans le cadre de l'évaluation, la source horaire est fournie par la station d'administration et de configuration.

4.4.3. Utilisateurs

H.PERSONNEL

- Super-administrateur :
  Le super-administrateur est une personne considérée comme non hostile. Il est compétent, formé pour exécuter les opérations dont il a la responsabilité et suit les manuels et procédures d'administration et de configuration.
- Administrateur :
  Les administrateurs sont des personnes considérées comme non hostiles. Ils sont compétents, formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures de configuration.
- Auditeur :
  Les auditeurs sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité.

4.4.4. Maîtrise de la configuration

H.MAÎTRISE_CONFIGURATION

Le super-administrateur a installé lui-même la mise à jour de la ToE qu'il a pu récupérer par un moyen proposé par GEOIDE Crypto&Com.

4.4.5. Consultation des journaux

H.CONSULTATION_JOURNAUX

Il est supposé qu'un auditeur consulte régulièrement les journaux générés par l'équipement.

4.4.6. Activation des journaux

H.JOURNAUX

L'administrateur configure la ToE en suivant les guides fournis, bien que par défaut, la configuration soit la suivante :

- la fonction de journalisation distante vers un serveur Syslog est non active.
- la fonction de journalisation locale est active.

4.4.7. Installation réseau et dimensionnement

H.COUPURE

Les appliances sont installées conformément à la politique d'interconnexion des réseaux en vigueur et sont les seuls points de passage entre les différents réseaux sur lesquels il faut appliquer la politique de filtrage. De même, le nombre d'appliances déployées est lié au dimensionnement du système et des flux à surveiller. L'évaluation porte sur le déploiement d'un seul équipement (aucune redondance n'est testée).

4.4.8. Politique de filtrage

H.POLITIQUE_FILTRAGE

La politique de filtrage configurée dans la ToE est considérée comme adaptée au cas d'usage.

4.4.9. Documentation de sécurité

H.APPLICATION_PRÉCONISATIONS

Les utilisateurs se conforment à la documentation fournie avec la ToE et appliquent toutes les préconisations sur l'utilisation sécurisée de cette dernière.

4.4.10. Mise à jour

H.GÉNÉRATION_CLÉS

La génération de la paire de clés requise pour la signature de la mise à jour logicielle est effectuée sur un serveur dédié aux officiers de sécurité de GEOIDE et sous le contrôle de l'un d'entre eux. La paire de clés utilisée est définie sur la courbe elliptique P-384 et a pour taille 384 bits. La courbe P-384 est conforme aux recommandations RGS.

4.5. Dépendances matérielles et logicielles

La station, sur laquelle s'exécute l'outil d'administration et de configuration, n'est pas fournie. Pour information, l'outil d'administration et de configuration est fourni sous forme de binaire. Il est compilé pour cibler le système d'exploitation Windows 10.
De même, la station, sur laquelle s'exécute l'outil de consultation des journaux locaux, n'est pas fournie. L'outil de consultation des journaux locaux est fourni sous forme de binaire. Il est compilé pour cibler le système d'exploitation Windows 10.

Les deux stations citées précédemment, sont sécurisées, dédiées à l'utilisation spécifique à laquelle elles sont destinées, déconnectées du réseau, et à jour de tous les correctifs concernant leur système d'exploitation et les logiciels applicatifs qui les équipent. Leur accès est restreint au super-administrateur, aux administrateurs et aux auditeurs de la ToE.

4.6. Utilisateurs typiques

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

- Super-administrateur :
  Utilisateur ayant tous les droits sur la ToE, pouvant en particulier :
  - créer, modifier ou supprimer les comptes des administrateurs et des auditeurs, via le port série de l'appliance.
  - procéder aux opérations de configuration (lecture et écriture) de la ToE, via le port série de l'appliance.
  - accéder aux journaux locaux (lecture et suppression) de la ToE, via le port RJ45 spécifié de l'appliance.
- Administrateur :
  Utilisateur ayant le droit de :
  - procéder aux opérations de configuration (lecture et écriture) de la ToE, via le port série de l'appliance.
  - accéder aux journaux locaux (lecture et suppression) de la ToE, via le port RJ45 spécifié de l'appliance.
- Auditeur :
  Utilisateur ayant le droit de :
  - consulter la configuration (sans pouvoir la modifier) de la ToE, via le port série de l'appliance.
  - consulter les journaux locaux (lecture seule) de la ToE, via le port RJ45 spécifié de l'appliance.
- Utilisateur standard du réseau :
  Utilisateur contrôlant un équipement faisant transiter des flux au travers de la ToE.

4.7. Périmètre de l'évaluation (caractéristiques de sécurité du produit concernées par l'évaluation)

La partie logicielle de la ToE est divisée en plusieurs éléments :

- le logiciel Bwall, module développé pour noyau UNIX,
- le système d'exploitation durci basé sur FreeBSD (UNIX),
- le serveur de communication gérant l'administration et la configuration de Bwall via le port série,
- tout autre élément logiciel présent dans l'appliance.

Les fonctions incluses dans le périmètre de l'évaluation sont les suivantes :

- **Filtrage réseau :**
  La ToE dispose de fonctions de filtrage aux niveaux 2, 3 et 4. L'IPv4 est supportée tandis que l'IPv6 ne l'est pas.

- **Fonction d'administration et de configuration :**
  L'outil d'administration et de configuration est une interface en mode graphique.
  Il s'agit d'un logiciel faisant usage du port série pour communiquer avec l'appliance.
  L'appliance et cet outil communiquent deux à deux via un protocole GEOIDE.
  Le service de communication gérant l'administration et la configuration de Bwall, présent dans l'appliance, fait partie de la ToE.
  Le logiciel d'administration et de configuration, exécuté sur un équipement externe à l'appliance, fait partie de l'évaluation.

- **Journalisation locale d'événements :**
  Le produit journalise dans son système de fichiers les événements de sécurité ou d'administration.
  Il est possible de configurer la journalisation pour chaque règle d'autorisation de la fonction filtre. Par défaut, c'est la réception de paquets non autorisés qui est journalisée.
  Un administrateur peut configurer le produit de manière à permettre la consultation de ces journaux locaux via un port RJ45 spécifié. Un tel accès aux journaux nécessite l'utilisation de l'outil de consultation des journaux locaux, qui est un logiciel exécuté sur une station externe.
  Le service de communication gérant la consultation des journaux locaux, présent dans l'appliance, fait partie de la ToE.
  Le logiciel de consultation des journaux locaux fait également partie de l'évaluation.

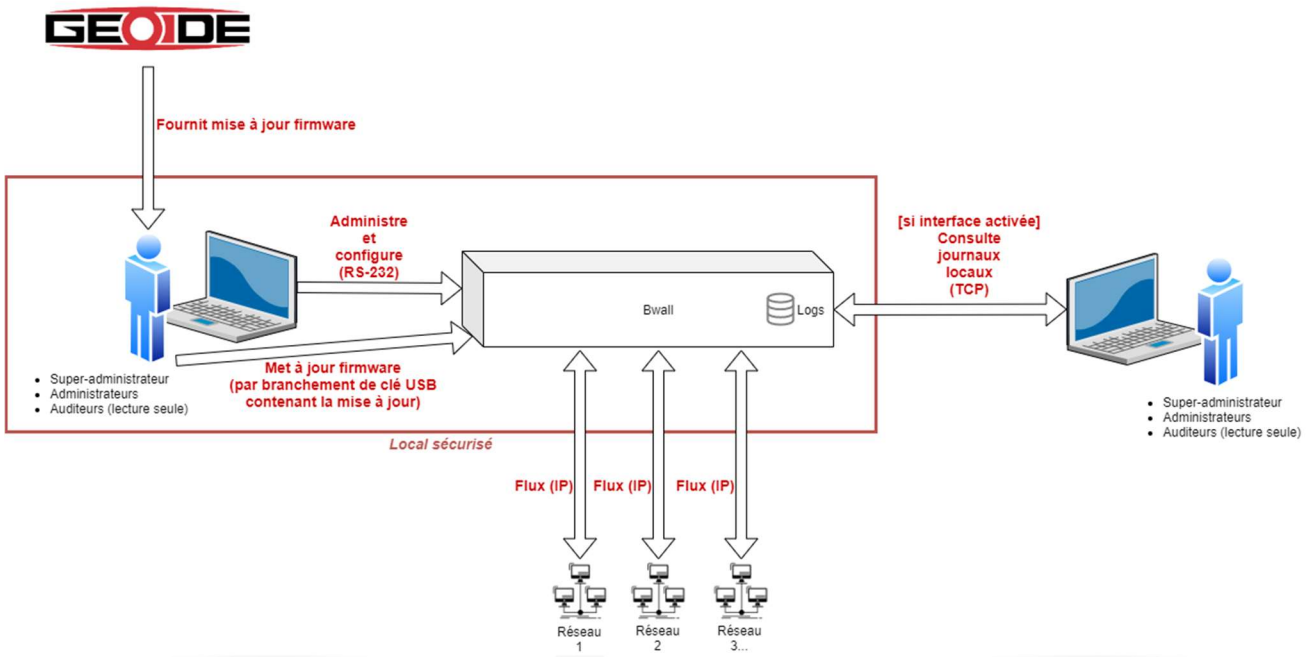
5. Environnement technique dans lequel le produit doit fonctionner

5.1. Plateforme d'évaluation

La plateforme d'évaluation comprend :

- Une appliance Bwall.
- Un poste d'administration sous Windows 10, reliable au port série de l'appliance.
- Un poste de consultation de journaux locaux, sous Windows 10, reliable à un port RJ45 de l'appliance. La consultation des journaux locaux se fait par un canal chiffré TLS 1.3 et l'appliance est authentifiée par certificat.
- Une clé USB de stockage contenant les binaires exécutables des outils :
  - d'administration et de configuration,
  - de consultation des journaux locaux.
- Une clé USB de stockage dédiée au processus de mise à jour.

Illustration du produit et des interactions qui le concernent :



Vue d'ensemble du produit

6. Biens sensibles que le produit doit protéger

6.1. Biens sensibles de la ToE

B.LOGICIEL : Partie logicielle

Afin d'assurer correctement ses fonctions, la partie logicielle de la ToE doit être intègre.

B.SECRETS_CONNEXION : Mots de passe des administrateurs

Il s'agit des mots de passe du super-administrateur, des administrateurs et des auditeurs. La ToE doit garantir la confidentialité, la disponibilité et l'intégrité de ces données.

B.DONNÉES_CONFIGURATION : Données de configuration

Il s'agit de l'ensemble des données de configuration telles que les règles de filtrage et la politique de gestion des droits. La ToE doit garantir la confidentialité, la disponibilité et l'intégrité de ces données.

Remarque sur la confidentialité et l'intégrité des données de configuration :

Les données de configuration stockées dans le produit ne sont pas chiffrées. Leur confidentialité et leur intégrité reposent sur les hypothèses H.LOCAL_SÉCURISÉ et H.PERSONNEL.

B.FLUX_CONSULTATION_JOURNAUX_LOCAUX : Flux de consultation des journaux locaux

Ce sont les flux entre l'appliance et le poste exécutant l'outil de consultation des journaux locaux. Ces journaux sont l'ensemble des traces générées par l'appliance concernant la gestion du produit (authentification des utilisateurs, actions d'administration) ainsi que les traces générées par le filtrage.

Les communications entre le serveur des journaux locaux et l'outil de consultation des journaux locaux sont protégées en confidentialité et en intégrité par la mise en œuvre d'un chiffrement avec des clés de 256 bits en TLS 1.3 (TLS_AES_256_GCM_SHA384). Un certificat est utilisé par l'outil logiciel client pour authentifier le serveur où sont les journaux au sein du produit. Enfin, il est nécessaire de s'authentifier par mot de passe via l'outil logiciel client pour avoir accès aux journaux locaux.

La ToE doit garantir l'authenticité, la confidentialité, la disponibilité et l'intégrité de ces données.

Remarque sur le stockage des journaux générés au sein du produit :

Les journaux générés par le produit ne sont pas chiffrés. Ils sont stockés sur une partition dédiée. Ils ne sont accessibles que par l'outil de consultation des journaux locaux.

B.MISES_À_JOUR : Mises à jour du logiciel

La ToE doit garantir l'authenticité et l'intégrité de ces données.

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

Bien	Authenticité	Confidentialité	Disponibilité	Intégrité
B.LOGICIEL				●
B.SECRETS_CONNEXION		●	●	●
B.DONNÉES_CONFIGURATION		●	●	●
B.FLUX_CONSULTATION_JOURNAUX_LOCAUX	●	●	●	●
B.MISES_À_JOUR	●			●

7. Menaces

7.1. Agents menaçants retenus

Équipement terminal malveillant

Un équipement terminal malveillant ou utilisateur situé hors du local sécurisé, ayant accès :

- au réseau filtré ou
- au réseau de consultation des journaux.

Par hypothèse, le super-administrateur, les administrateurs et les auditeurs ne sont pas considérés comme des attaquants potentiels. Les attaques physiques sur l'appliance ne sont également pas considérées pour l'évaluation CSPN.

7.2. Menaces retenues

M.DÉNI_DE_SERVICE

L'attaquant parvient à effectuer un déni de service sur la ToE en effectuant une action imprévue ou en exploitant une vulnérabilité. Ce déni de service peut concerner toute la ToE ou seulement certaines de ses fonctions.

M.CONTOURNEMENT_PARE_FEU

L'attaquant parvient à violer la politique de filtrage en empêchant un flux légitime de transiter ou en permettant à un flux illégitime de transiter en provenance, à destination ou au travers de la ToE.

M.ALTÉRATION

Un attaquant (utilisateur standard du réseau) altère (modification ou suppression) ou compromet les journaux locaux en intégrité ou les compromet en confidentialité.

M.DIVULGATION

Un attaquant parvient à prendre connaissance des éléments cryptographiques, des journaux locaux produits, des données de configuration ou de la politique de contrôle de flux.

M.UTILISATEUR_ILLICITE

Un attaquant ne disposant pas d'accès à la ToE parvient à accéder aux journaux locaux. Cette menace peut prendre la forme d'une usurpation d'identité suite à des tentatives aléatoires répétées ou par le biais d'analyses de séquences d'authentification interceptées.

M.MITM_CONSULTATION_JOURNAUX_LOCAUX

Un attaquant se place en homme-du-milieu entre l'appliance et la station de consultation des journaux locaux afin de porter atteinte en intégrité et/ou confidentialité aux données transitant sur ce lien.

M.MISE_À_JOUR_MALICIEUSE

Un attaquant parvient à forcer l'application d'une mise à jour malicieuse ou intercepte et modifie à son compte un flux de mise à jour légitime.

M.CORRUPTION_LOGICIEL

L'attaquant parvient à injecter et à faire exécuter un logiciel corrompu sur la ToE. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée.

8. Fonctions de sécurité du produit

F.ANALYSE

La ToE offre des fonctionnalités de filtrage des flux entre des réseaux IP, basées sur des règles permettant de mettre en œuvre la politique de sécurité du système d'information concerné.

Le filtrage pouvant être réalisé par la ToE est de type non contextuel, c'est-à-dire que l'action de filtrage (acceptation, blocage, avec journalisation ou non) est déterminée en fonction du contenu d'un paquet réseau.

Il est tout de même à noter que Bwall est capable d'identifier et de traiter, dans le cadre du protocole TCP, les attaques « SYN flood » visant à atteindre un déni de service.

Les fonctionnalités de filtrage offertes par Bwall, s'appliquent uniquement aux flux portés par le protocole IP et prennent en compte les couches liaison (filtrage d'adresses MAC), réseau (filtrage d'adresses IP) et transport (filtrage de numéros de ports, filtrage sur les protocoles UDP et TCP).

F.JOURNALISATION

Ce service permet de définir les événements à tracer et leur consultation. Les événements disposent d'un indicateur de criticité.

La ToE met la priorité sur sa fonctionnalité principale qui est le filtrage de flux. Dans le cas où les ressources de la ToE ne permettraient pas de gérer la totalité du filtrage et de la journalisation, c'est la disponibilité de la journalisation qui ne serait plus garantie, au profit de la disponibilité du filtrage. Ce mécanisme peut prévenir certaines formes d'attaque par déni de service.

F.CONTRÔLE_ACCÈS_JOURNAUX

Pour accéder aux journaux locaux, le super-administrateur, les administrateurs et les auditeurs se placent sur le réseau de consultation des journaux locaux.

Ils sont soumis à une authentification par mot de passe.

F.FLUX_SÉCURISÉS_JOURNAUX

Les communications concernant la consultation des journaux locaux grâce à une station et un outil logiciel client dédiés, sont protégées en confidentialité et en intégrité par l'utilisation d'un chiffrement avec des clés de 256 bits en TLS 1.3 (TLS_AES_256_GCM_SHA384). L'authentification du serveur par le client est effectuée sur la base de l'installation d'un certificat sur la station exécutant l'outil logiciel client (peer certificate authentication). Le certificat utilisé est généré par l'acquéreur de la ToE, lors de sa première installation et de sa configuration. Ce certificat est auto-signé (par le produit) et récupérable grâce à l'outil d'administration et de configuration. Enfin, il est nécessaire de s'authentifier par mot de passe via l'outil logiciel client de consultation des journaux locaux pour avoir accès aux journaux locaux.

F.MISES_À_JOUR_SECURISÉES

À chaque installation d'un nouveau firmware (partie logicielle), l'intégrité et l'authenticité de celui-ci sont vérifiées.

L'intégrité et l'authenticité sont garanties par un processus de signature du firmware (par le fabricant) et de vérification de cette signature (par le produit).

Le mécanisme employé est le mécanisme de signature asymétrique ECDSA utilisant la courbe P-384. La taille de la clé est de 384 bits.

La vérification de la signature repose sur l'algorithme de hachage SHA256.

9. Matrices de couverture

9.1. Menaces et biens sensibles

La matrice suivante présente la couverture des biens sensibles par les menaces et les lettres y associent les besoins :

- D : Disponibilité
- I : Intégrité
- C : Confidentialité
- A : Authenticité

	B.FILTRAGE	B.LOGICIEL	B.SECRETS_CONNEXION	B.DONNÉES_CONFIGURATION	B.FLUX_CONSULTATION_JOURNAUX_LOCAUX	B.MISES_À_JOUR
M.DÉNI_DE_SERVICE	D			D		D
M.CONTOURNEMENT_PARE_FEU	I					
M.ALTÉRATION			I	I	ICA	
M.DIVULGATION			C	C	C	
M.UTILISATEUR_ILLICITE	D		DIC	DIC	DIC	
M.MITM_CONSULTATION_JOURNAUX_LOCAUX					IC	
M.MISE_À_JOUR_MALICIEUSE						IA
M.CORRUPTION_LOGICIEL		I				

Couverture des biens sensibles par les menaces

9.2. Menaces et fonctions de sécurité

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

	F.ANALYSE	F.JOURNALISATION	F.CONTRÔLE_ACCÈS_JOURNAUX	F.FLUX_SÉCURISÉS_JOURNAUX	F.MISES_À_JOUR_SECURISÉES
M.DÉNI_DE_SERVICE	✓				✓
M.CONTOURNEMENT_PARE_FEU	✓				
M.ALTÉRATION		✓	✓	✓	
M.DIVULGATION				✓	
M.UTILISATEUR_ILLICITE		✓	✓		
M.MITM_CONSULTATION_JOURNAUX_LOCAUX				✓	
M.MISE_À_JOUR_MALICIEUSE					✓
M.CORRUPTION_LOGICIEL					✓

Couverture des menaces par les fonctions de sécurité

FIN DU DOCUMENT