PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2021/09

BWALL

BWALL version GEN1-7.6.14

Paris, le 16 avril 2021

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD

[ORIGINAL SIGNE]

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2021/09**
Nom du produit **BWALL**
Référence/version du produit **BWALL version GEN1-7.6.14**
Catégorie de produit **Pare-feu**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **GEOIDE CRYPTO&COM (SASU)** 18 rue Alain Savary 25000 Besançon, France
Développeur **GEOIDE CRYPTO&COM (SASU)** 18 rue Alain Savary 25000 Besançon, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Filtrage des flux réseau Journalisation locale Contrôle d'accès aux journaux locaux Flux sécurisé d'accès aux journaux locaux
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. §3.2)

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :
L'agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
Les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est «BWALL version GEN1-7.6.14 » développé par GEOIDE CRYPTO&COM (SASU).

Ce produit est une appliance 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.

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☒	**3**	**pare-feu**
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	Autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	BWALL
Numéro de la version évaluée	BWALL version GEN1-7.6.14

La version certifiée du produit peut être identifiée dans l'outil d'administration et de configuration (aussi appelé « interface de gestion »). Le libellé correspondant est « Version BWALL », dans l'onglet « appliance ».

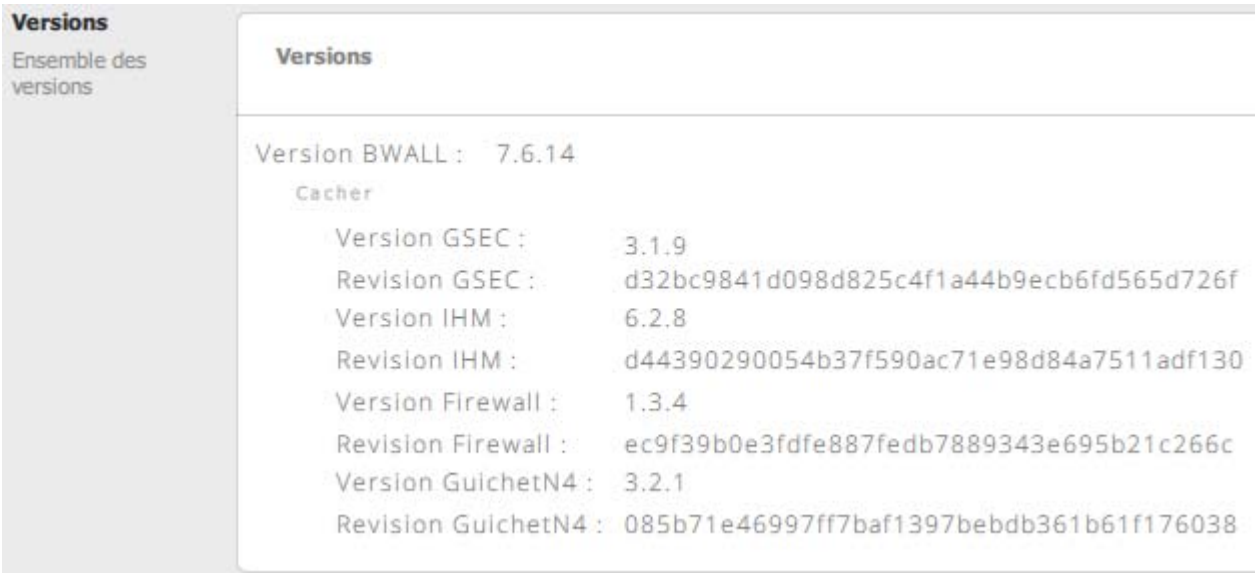

Figure 1 : affichage de la version certifiée du produit

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le filtrage des flux réseau ;
- la journalisation locale ;
- le contrôle d'accès aux journaux locaux ;
- les flux sécurisés d'accès aux journaux locaux.

1.2.4 *Configuration évaluée*

L'appliance BWALL est produite en usine par le développeur et livrée au client « prête à l'emploi ». La configuration évaluée correspond à cette configuration de production.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en ANNEXE B.

2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1 *Installation du produit*

2.3.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.3.1.2 Description de l'installation et des non-conformités éventuelles

L'évaluateur a récupéré une applicance dans une version logicielle inférieure à le version à évaluer. Il a donc dû effectuer une mise à jour logicielle en suivant les [GUIDES].

2.3.1.3 Durée de l'installation

L'installation a duré moins d'une demi-journée.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.3.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

Il est à noter cependant que l'évaluation ne donne aucune garantie sur l'authentification et le contrôle d'accès des super-administrateurs et administrateurs : l'utilisateur a donc la responsabilité de limiter à des personnels de confiance l'accès physique au produit, et plus généralement au réseau de configuration/administration. Ce point constitue une restriction d'usage détaillée au chapitre 3.2.

2.3.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.3.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.3.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.3.7 *Analyse de la facilité d'emploi*

2.3.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.3.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de vulnérabilité exploitable dans le contexte défini par la cible de sécurité [CDS].

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. Cette analyse n'a pas identifié de vulnérabilité exploitable dans le contexte défini par la cible de sécurité [CDS].

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « BWALL, version GEN1-7.6.14 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et mettre en œuvre les recommandations et restrictions suivantes :

1. L'évaluation ne porte pas sur l'authentification et le contrôle d'accès des super-administrateurs et administrateurs. Le certificat n'est donc valide que si l'utilisateur s'assure qu'aucun attaquant potentiel ne peut accéder physiquement au produit, à son port série ou plus largement au réseau d'administration/configuration (incluant le poste d'administration/configuration lui-même).
   L'utilisateur a donc la responsabilité de :
   - protéger l'accès aux locaux hébergeant le produit et le réseau de configuration/administration ;
   - garantir que les personnes accédant à ces locaux sont de confiance.

   Ce point est d'application impérative et constitue une restriction d'usage du certificat CSPN.
2. Plus largement, les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité Bwall Référence : GEOIDE_cible_Bwall_CSPN ; Version : 1.8 ; Date : 4 mars 2021.
[RTE]	Rapport Technique d'Évaluation CSPN F2020 – BWALL GEOIDE Référence : OPPIDA/CESTI/F2020/RTE ; Version : 1.1 ; Date : 22 mars 2021.
[GUIDES]	Manuel utilisateur BWALL : 2.2 - 13/08/2020 Version : 2.2 ; Date : 13 août 2020. Manuel utilisateur BWLOG : 1.1 - 12/08/2020 Version : 1.1 ; Date : 12 août 2020.

ANNEXE B. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.