Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2019/15

Wallix Bastion
Version 6.0.102.100

Paris, le 25 novembre 2019

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

[Original signé]
Guillaume POUPARD

SÉCURITÉ CERTIFICATION

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-2019/15**
Nom du produit **Wallix Bastion**
Référence/version du produit **Version 6.0.102.100**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Wallix** **118 rue de Tocqueville** **75017 Paris**
Développeur **Wallix** **118 rue de Tocqueville** **75017 Paris**
Centre d'évaluation **Amossys** **11 rue Maurice Fabre, 35000 Rennes, France**
Fonctions de sécurité évaluées **Communications sécurisées** **Authentification et contrôle des accès aux ressources** **Authentification et contrôle d'accès GUI** **Authentification unique** **Traçabilité des connexions aux ressources** **Traçabilité des actions GUI** **Stockage sécurisé** **Durcissement du Bastion**
Fonction de sécurité non évaluée **Changement automatique de mot de passe**
Restriction(s) d'usage **Non**

Préface

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 Premier ministre 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « Wallix Bastion, Version 6.0.102.100 » développé par *WALLIX*.

Ce produit est destiné à être utilisé en tant que passerelle d'administration entre un domaine *Utilisateurs* potentiellement hostile et un domaine protégé *Ressources*, comme illustré par la Figure 1.

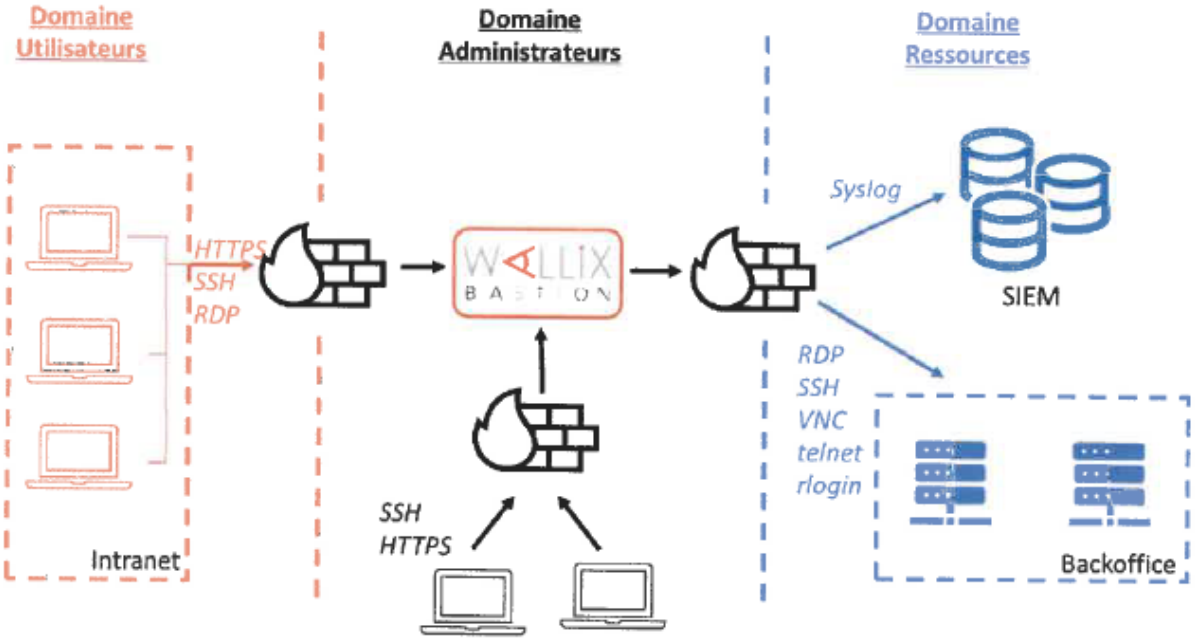

Figure 1 – Schéma d'utilisation du Bastion

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

Nom du produit	Wallix Bastion
Numéro de la version évaluée	Version 6.0.102.100

La version certifiée du produit peut être identifiée de la manière suivante :

- la section 14.4 du guide d'administration du produit [Admin_guide] indique d'utiliser la commande « WABVersion » pour obtenir la version, le numéro et la date de compilation du bastion depuis la console d'administration via SSH :

```
wabadmin@Bastion01-6-0-102-100:~$ WABVersion
WALLIX Bastion 6.0 hotfix 102 (build 100; 2019-03-08)

History of installation operations:
2019-03-11 11:31:59 (+01:00): Installation of WALLIX Bastion 6.0
hotfix 102 (build 100; 2019-03-08)
```

- le numéro de version peut également être récupéré au niveau de l'interface web, sous *System* → *Status* :

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- les communications sécurisées entre le domaine « utilisateurs » et le domaine « ressources »,
- l'authentification et le contrôle des accès aux ressources,
- l'authentification et le contrôle d'accès à l'interface web,

- l'authentification unique des utilisateurs,
- la traçabilité des connexions aux ressources,
- la traçabilité des actions effectuées sur l'interface web,
- le stockage sécurisé,
- le durcissement du Bastion.

1.2.4. Configuration évaluée

La configuration évaluée correspond à une configuration en mode *standalone*, conformément à la description faite au 3.2 de la cible de sécurité (voir [CdS]).

La plateforme de test mise en œuvre est illustrée par la Figure 2.

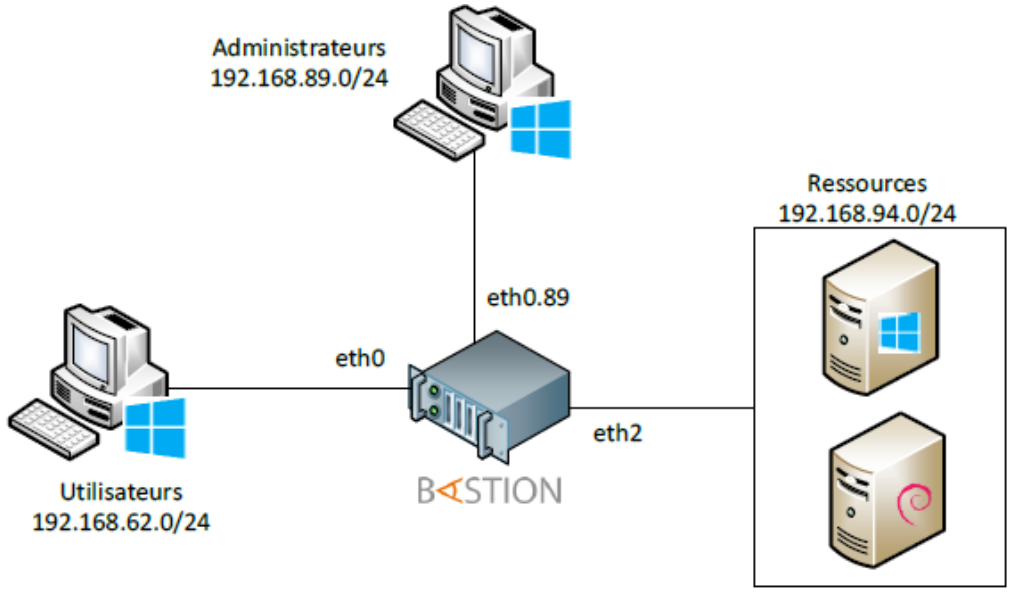

Figure 2 - Plateforme d'évaluation

Cette plateforme est composée des postes suivants :

- domaine utilisateurs :
  - un poste sous Windows 10 ;
- domaine administrateurs :
  - un poste sous Windows 10) ;
- domaine ressources :
  - un poste sous Windows serveur 2016, avec :
    - un Active Directory contenant les comptes utilisateurs ;
    - la fonctionnalité « Bureau à distance » activée pour les connexions RDP.
  - un poste sous Debian Stretch, avec :
    - un serveur OpenSSH version 7.4 ;
    - un serveur rsyslog version 8.24.0.

Les communications entre le domaine utilisateurs et le domaine ressources s'effectuent obligatoirement via le bastion. Un poste sous Kali Linux, positionné sur les différents domaines, a également été utilisé pour les besoins des tests.

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 2.

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

Le bastion a été livré sous forme d'*appliance* pré-installée. Son installation a consisté à relier les réseaux utilisés pour l'évaluation au boîtier et à configurer ce dernier.

2.3.1.3. Durée de l'installation

L'installation et la configuration complète de la plateforme ont duré 2 jours.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

L'évaluateur a eu accès aux documents suivants dans le cadre de cette évaluation :

- un guide d'administration [Admin_guide] ;
- un guide d'installation [Install_guide] ;
- un guide de démarrage rapide [Quickstart_guide] ;
- un guide utilisateur [User_guide] ;
- les *release notes* de la version 6.0.102 ;
- les guide relatifs aux briques logicielles tierces [COTS_guide].

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

L'utilisation du guide d'administration peut toutefois s'avérer complexe. C'est la raison pour laquelle son utilisation est à réserver à des administrateurs ayant des connaissances approfondies en réseau et familiarisés avec ce type de produit.

2.3.3. Revue du code source (facultative)

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

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

2.3.6.1. Liste des vulnérabilités connues

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

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

Il n'a pas été découvert de vulnérabilité propre au produit qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi

2.3.8.1. Cas où la sécurité est remise en cause

Le mécanisme de changement automatique de mot de passe est fonctionnel et permet de renouveler régulièrement les mots de passe des comptes associés aux ressources de manière transparente pour les utilisateurs. Toutefois, la politique définie par défaut n'impose pas de critère suffisamment fort sur les mots de passe générés et doit être configurée par l'administrateur.

2.3.8.2. Avis d'expert sur la facilité d'emploi

Dans l'ensemble, l'utilisation du produit est simple et intuitive. Les instructions contenues dans les guides sont claires et permettent d'appréhender correctement le produit. Cependant,

certaines opérations de configuration peuvent s'avérer complexes pour les utilisateurs non familiarisés avec le produit, comme la mise en place d'une politique d'accès aux ressources via un système d'autorisations, et devraient être réservées à des administrateurs avertis.
La lecture de la documentation est recommandée en amont de l'utilisation de ce produit.

2.3.8.3. 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 non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable

2.5. Analyse du générateur d'aléas

Le produit utilise de l'aléa fourni par le générateur du noyau Linux, et la bibliothèque PyCrypto via le générateur Fortuna. Bien que ces générateurs présentent des non conformités au RGS, l'évaluateur n'a pas identifié de faiblesse exploitable liée à leur utilisation.

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 « Wallix Bastion, Version 6.0.102.100 » 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, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictions suivantes :

- la politique pour la génération des mots de passe doit être configurée par l'administrateur en suivant les bonnes pratiques (voir [Reco-MDP]) ;
- la mise en place d'une politique d'accès aux ressources, via un système d'autorisations, doit être effectuée par des administrateurs avertis en se référant à la documentation applicable (voir [Admin_guide] et [Install_guide]) ;
- lorsqu'une authentification par Active Directory est mise en place, l'administrateur est invité à consulter les journaux régulièrement afin de détecter d'éventuelles attaques par recherche exhaustive sur les comptes RDP ou SSH.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – Bastion 6.0.102* Référence : CSPN-Bastion-6.0 ; Version : 3.2 ; Date : *30 janvier 2019.*
[RTE]	*Rapport Technique d'Evaluation CSPN - Produit Wallix Bastion - version 6.0.102.100* Référence : CSPN-RTE-Wallix_Bastion-1.01 ; Version : 1.01 ; Date : *25 juillet 2019.* *Expertise des mécanismes cryptographiques* *Produit WALLIX Bastion - version 6.0.102.100* Référence : CSPN-CRY-WALLIX_Bastion-1.01 ; Version : 1.01 ; Date : *23 juillet 2019.*
[GUIDES]	
[Admin_guide]	*Guide d'administration du produit WALLIX Bastion version 6.0.102* Référence : Bastion-admin-guide-fr.pdf ;
[Install_guide]	*Guide d'installation du produit WALLIX Bastion version 6.0.100* *Référence : Bastion-quickstart-fr.pdf*
[Quickstart_guide]	*Guide de démarrage rapide du produit WALLIX Bastion version 6.0.102* *Référence : Bastion-quickstart-fr.pdf*
[User_guide]	*Guide de l'utilisateur du produit WALLIX Bastion version 6.0.102* *Référence : Bastion-user-guide-fr.pdf*
[COTS_guide]	*Third-Party Components du produit WALLIX Bastion version 6.0* *Référence : Third_Party_Components.pdf*

Annexe 2. 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-01/2.0 du 6 septembre 2018. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/2.0 du 6 septembre 2018. 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.
[Reco-MDP]	Note technique – Recommandations de sécurité relatives aux mots de passe, référence : DAT-NT-001/ANSSI/SDE/NP, 5 juin 2012), voir www.ssi.gouv.fr.