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-2016/11

Stormshield

Stormshield Network Security

Pare-feu Industriel SNi40

Suite logicielleVersion 2.3.4

Paris, le 27 juillet 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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-2016/11

Nom du produit

Stormshield Network Security

Référence/version du produit

Pare-feu Industriel SNi40
Suite Logicielle version 2.3.4

Référence de la cible de sécurité

Cible de sécurité

Référence : SN_ASE_cible_CSPN version 1.3 en date du 29 juin 2016.

Catégorie de produit

Pare-feu

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Commanditaire

Stormshield
22 rue du Gouverneur Général Eboué
92130 Issy-les-Moulineaux
France

Centre d'évaluation

Oppida
4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Fonctions de sécurité évaluées

Gestion des entrées malformées
Application de la politique de filtrage
Analyse de conformité protocolaire
Stockage sécurisé des secrets
Authentification sécurisée sur l'interface d'administration
Politique de droits
Signature du firmware
Intégrité et confidentialité de la configuration

Fonctions de sécurité non évaluées

Journalisation

Restrictions d'usage

Oui (cf. §3.2)

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 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 la « Suite logicielle Stormshield Network Security, version 2.3.4 » développée par *STORMSHIELD* et embarquée dans le boîtier pare-feu industriel SNi40.

Ce pare-feu industriel permet de protéger l'interconnexion entre un réseau industriel à protéger vis-à-vis d'un autre réseau. Il est notamment utilisé si ce dernier réseau est d'une moindre maîtrise ou d'un niveau de confiance moindre, s'il dispose d'applications sans interactions avec le réseau industriel, s'il correspond à un autre réseau industriel comportant des fonctionnalités différentes ou s'il correspond à des domaines de responsabilités différentes.

La principale particularité d'un pare-feu industriel, vis-à-vis d'un pare-feu classique est qu'il doit fonctionner dans des conditions ambiantes hostiles. En particulier, il doit pouvoir fonctionner en présence d'humidité ou de poussière, ou à des températures inhabituelles.

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 – matériel et logiciel embarqué
☐ 12 – terminal de réception numérique (Set top box, STB)
☐ 13 – automate programmable industriel

1.2.2. Identification du produit

Nom du produit	Stormshield Network Security Pare-feu Industriel SNi40
Numéro de la version analysée	Suite logicielle 2.3.4

La version certifiée du produit peut être identifiée en haut de l'interface d'administration web, une fois l'utilisateur authentifié.

1.2.3. Configuration évaluée

Le pare-feu est livré sous la forme d'un boîtier, la configuration évaluée est celle par défaut, conformément au paragraphe 2.8 de la [CDS]. Elle correspond au mode *bridge*.
Le serveur DHCP IPV4 doit être arrêté après l'initialisation du boîtier.

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 a été 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, menaces, utilisateurs et fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Plateforme de test

La plateforme de test est constituée des éléments suivants :

- un pare-feu SNi40 configuré en mode *bridge* ;
- un serveur S7Comm ;
- un automate programmable industriel Schneider M340 ;
- un automate programmable industriel Simatic S7 1200 ;
- une machine virtuelle dans le rôle de l'attaquant.

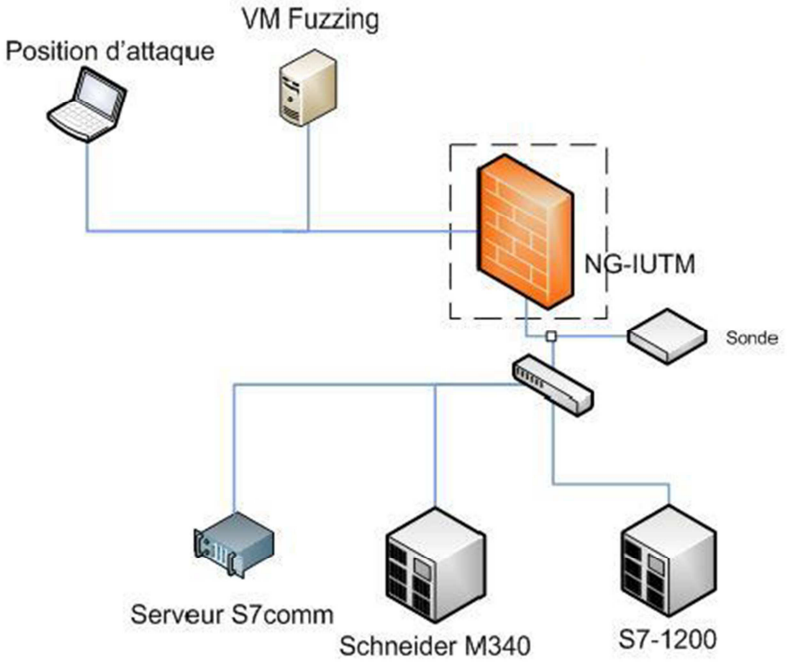

Figure 2 – Plateforme de test.

2.3.1.2. Particularités de paramétrage de l'environnement et options d'installation

Le pare-feu a été évalué dans la configuration précisée au paragraphe 1.2.3.

2.3.1.3. Description de l'installation et des non-conformités éventuelles

Sur le boitier SNi40, la journalisation est par défaut désactivée.

2.3.1.4. Durée de l'installation

L'installation de la plateforme de test a nécessité quelques heures.

2.3.1.5. Notes et remarques diverses

Néant.

2.3.2. Analyse de la documentation

La documentation est claire et correctement rédigée.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

2.3.4. Analyse de la conformité des fonctions de sécurité

L'évaluation en boîte noire n'a permis de faire qu'une analyse partielle de la fonction de sécurité « stockage sécurisé des secrets » sans pour autant la mettre en défaut.

La fonction de sécurité « signature du *firmware* » a bien fait l'objet de tests qui ont montrés qu'un *firmware* malformé est rejeté par la cible. Cependant cette évaluation en boîte noire n'a pas permis d'analyser en détail le mécanisme de vérification d'authenticité et de protection de l'intégrité du *firmware*.

Les autres fonctions de sécurité ont été testées et sont 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 testées 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

Il n'a pas été identifié de vulnérabilités connues et exploitables sur ce produit dans sa version évaluée.

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 ou à son implémentation pouvant remettre en cause la sécurité du produit sur le périmètre évalué et ses fonctions de sécurité.

2.3.7. Accès aux développeurs

Le centre d'évaluation n'a pas contacté les développeurs.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

Sans objet.

2.3.8.2. Recommandations pour une utilisation sûre du produit

L'utilisateur du produit devra mettre en œuvre les mesures suivantes :

- modifier la politique de gestion des mots de passe par défaut, comme décrit dans les [GUIDES] afin d'en définir une conforme aux recommandations de l'ANSSI ;
- modifier le mot de passe par défaut du compte administrateur, comme proposé lors de la première connexion par l'assistant de configuration et conformément aux recommandations des [GUIDES] ;
- conserver désactivé le service SSH[1] (comme c'est le cas dans la configuration par défaut) ;
- réaliser les tâches d'administration depuis des postes sécurisés comme précisé dans la cible de sécurité ;
- définir une liste blanche afin de ne donner accès au port 1300 du produit qu'aux postes réalisant une administration avec un client NSRPC[2].

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

Sans objet.

2.3.8.4. Notes et remarques diverses

Sans objet.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

[1] *Secure Shell.*
[2] *Netasq Secure Remote Protocol Client.*

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 la « Suite logicielle Stormshield Network Security, version 2.3.4 » embarquée dans le boîtier pare-feu industriel SNi40 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. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.
L'utilisateur de ce certificat devra s'attacher à employer la configuration énoncée au paragraphe 1.2.3 et suivre les recommandations décrites au paragraphe 2.3.8.2.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité Stormshield Network Security* *Pare-feu Industriel SNi40 Suite logicielle version 2.3.4* Référence : SN_ASE_cible_CSPN ; Version : 1.3 ; Date : *29 juin 2016.*
[RTE]	*Rapport Technique d'Evaluation CSPN PONTOS – SNi40* Référence : OPPIDA/CESTI/PONTOS/RTE/1.1 ; Version : 1.1 ; Date : *13 juillet 2016.*
[GUIDES]	*Guide Stormshield Network Security* *Présentation et installation produits* *Gamme SN* Référence : *snfrgde_installation-produit-GammeSN* ; Version : 1.5 ; Date : *mai 2016.* *SNS – Manuel d'utilisation et de configuration* Référence : *snfrgde_FirewallUserGuide-v2* ; Version : 2.3 ; Date : *mars 2016.* *Identifier les commandes de protocoles industriels traversant le firewall* Référence : *snfrtno_NGIUTM-protocol-discovery* ; Version : 1.0 ; Date : *2016.*

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 (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur http://www.ssi.gouv.fr/
[NOTE-3]	Méthodologie pour l'évaluation logicielle d'automates programmables industriels en vue d'une certification de sécurité de premier niveau ANSSI-CSPN-NOTE-03/1 du 30 juillet 2015. Documents disponibles sur http://www.ssi.gouv.fr/
[REF-CRY]	Référentiel général de sécurité, version 2.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03. Documents disponibles sur http://www.ssi.gouv.fr/
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.