



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-CC-2016/56

Fonction de filtrage de la suite logicielle STORMSHIELD Firewall

version 2.2.6

Paris, le 26 août 2016

*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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2016/56

Nom du produit

**Fonction de filtrage de la Suite logicielle STORMSHIELD
Firewall**

Référence/version du produit

Version 2.2.6

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

**EAL 4 augmenté
ALC_FLR.3**

Développeur(s)

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

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

Accords de reconnaissance applicables



**Le produit est reconnu au niveau EAL4 et
ALC_FLR.3.**

SOG-IS



**Le produit est reconnu au niveau EAL4 et
ALC_FLR.3.**

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 | 6 |
| 1.1. PRESENTATION DU PRODUIT | 6 |
| 1.2. DESCRIPTION DU PRODUIT | 7 |
| 1.2.1. <i>Introduction</i> | 7 |
| 1.2.2. <i>Identification du produit</i> | 7 |
| 1.2.3. <i>Services de sécurité</i> | 7 |
| 1.2.4. <i>Architecture</i> | 7 |
| 1.2.5. <i>Cycle de vie</i> | 9 |
| 1.2.6. <i>Configuration évaluée</i> | 10 |
| 2. L’EVALUATION | 11 |
| 2.1. REFERENTIELS D’EVALUATION | 11 |
| 2.2. TRAVAUX D’EVALUATION | 11 |
| 2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI | 11 |
| 2.4. ANALYSE DU GENERATEUR D’ALEAS..... | 11 |
| 3. LA CERTIFICATION | 12 |
| 3.1. CONCLUSION | 12 |
| 3.2. RESTRICTIONS D’USAGE..... | 12 |
| 3.3. RECONNAISSANCE DU CERTIFICAT | 13 |
| 3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> | 13 |
| 3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> | 13 |
| ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT [CCV3.1R4]..... | 14 |
| ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE | 14 |
| ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION | 16 |

1. Le produit

1.1. Présentation du produit

Le produit évalué est la « Fonction de filtrage de la Suite Logicielle STORMSHIELD Firewall, version 2.2.6 » développée par *STORMSHIELD* et embarquée sur l'un des boîtiers suivants : SN200, SN300, U30S, U70S, SN500, SN510, SN700, SN710, SN900, SN910, U150S, U250S, U500S, SN2000, SN3000, SN6000.

Il s'agit d'une brique logique intégrée à la suite logicielle « STORMSHIELD-Firewall » embarquée dans les boîtiers « pare-feu – VPN » de la société *STORMSHIELD*.

Le boîtier « pare-feu – VPN » offre des fonctionnalités de type pare-feu regroupant filtrage, détection d'attaques, gestion de la bande passante, gestion de la politique de sécurité, audit, imputabilité et authentification forte des administrateurs. Il offre également des fonctionnalités VPN (*Virtual Private Network* – Réseau Privé Virtuel : chiffrement et authentification) implémentant le protocole ESP (*Encapsulating Security Payload*) du standard IPsec en mode tunnel, sécurisant ainsi la transmission de données entre des sites distants

De façon plus spécifique le rôle de la fonction de filtrage, consiste à filtrer les flux, entre différentes zones de confiance ; typiquement un réseau non maîtrisé et un réseau de confiance comme schématisé dans la figure 1.

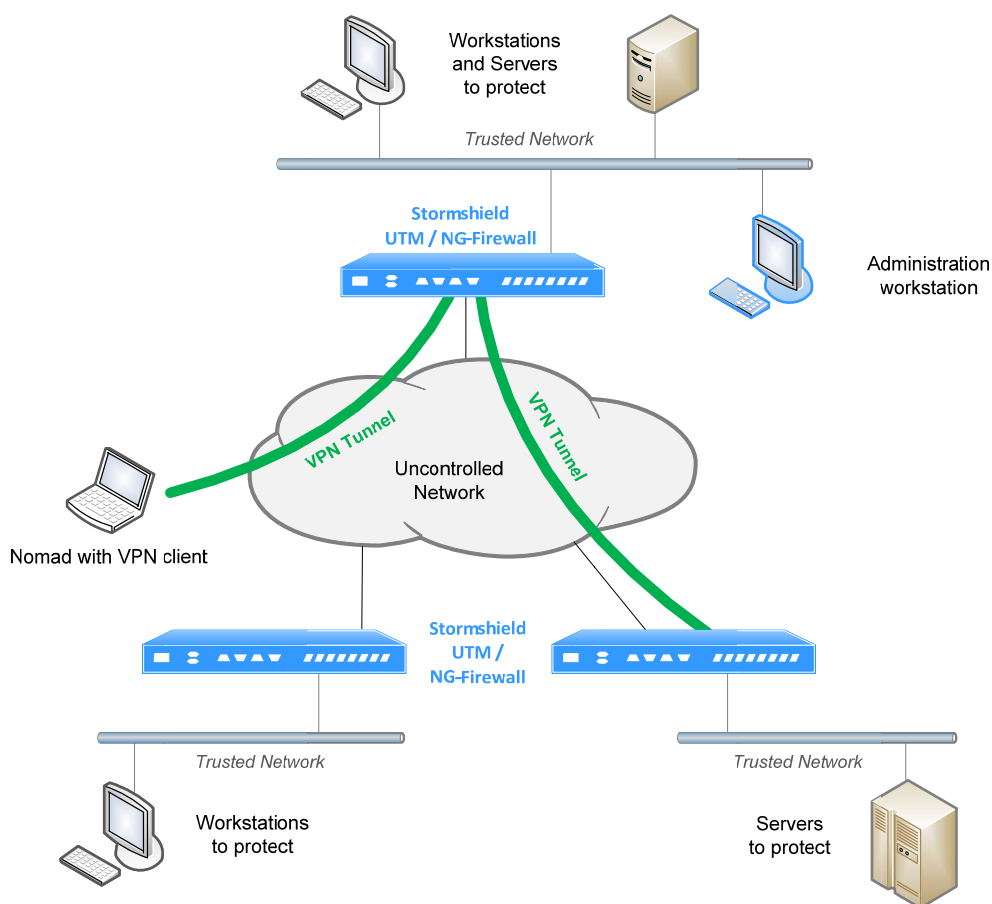


Figure 1 - Cas d'utilisation classique du produit

1.2. Description du produit

1.2.1. Introduction

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

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par :

- l'interface « Web Manager » : une fois connecté, la version de la TOE est indiquée en haut de la fenêtre d'administration ;
- la connexion directe en SSH sur la TOE : une fois connecté, la version est inscrite dans la bannière d'accueil.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- le filtrage des flux entre les équipements ;
- la journalisation, l'audit et la remontée d'alarmes.

1.2.4. Architecture

La TOE est « la fonction de filtrage », qui est elle-même une brique du composant *Active Security Qualification* (ASQ). Ce dernier est l'un des différents composants de la suite logicielle « STORMSHIELD Firewall ». Cette suite inclut notamment un système d'exploitation basé sur le noyau « FreeBSD ».

La « Suite logicielle STORMSHIELD Firewall, version 2.2.6 » dans son ensemble a fait l'objet d'une évaluation menée conjointement à la présente et a été certifiée au niveau EAL3 augmenté de ALC_CMC.4, ALC_CMS.4, ALC_FLR.3, AVA_VAN.3 (voir [ANSSI-CC-2016/55]).

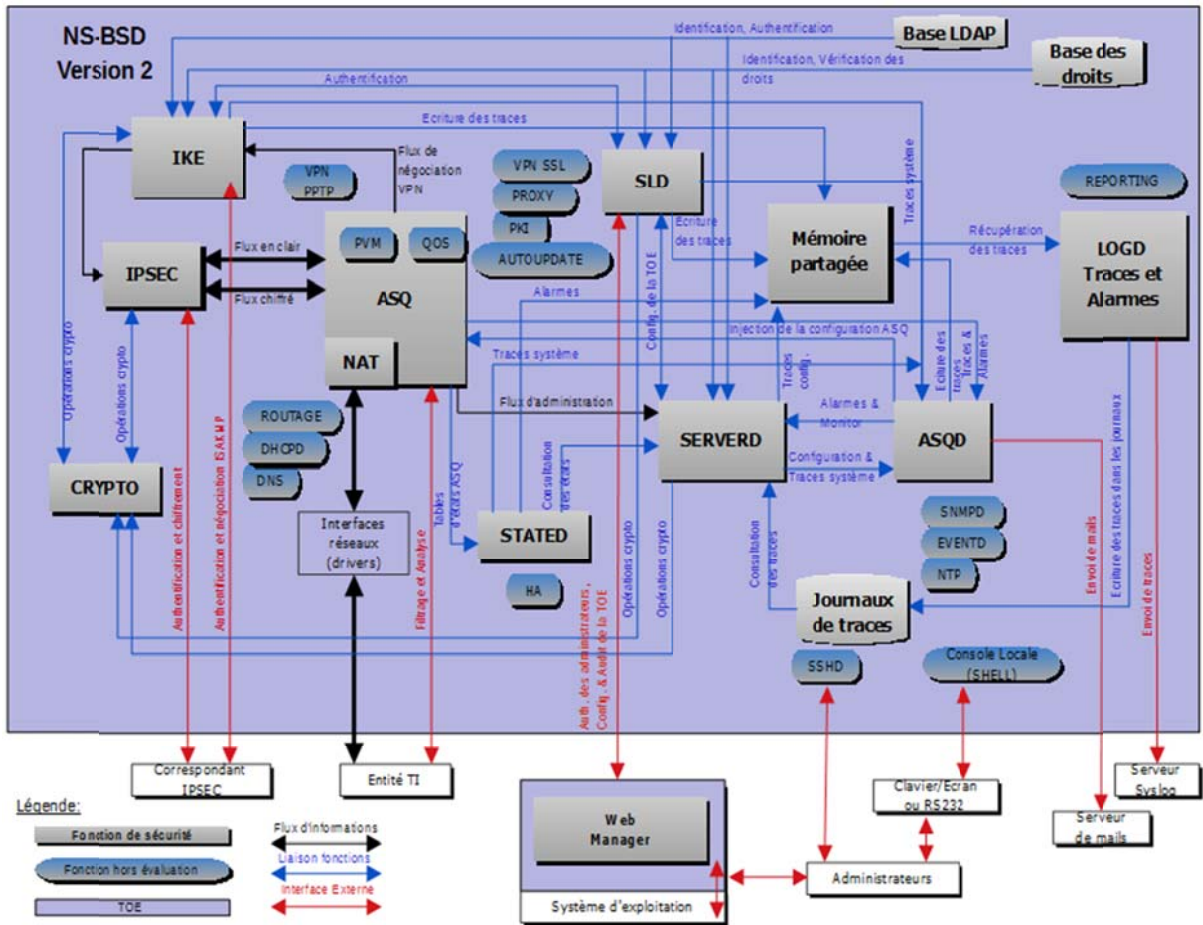
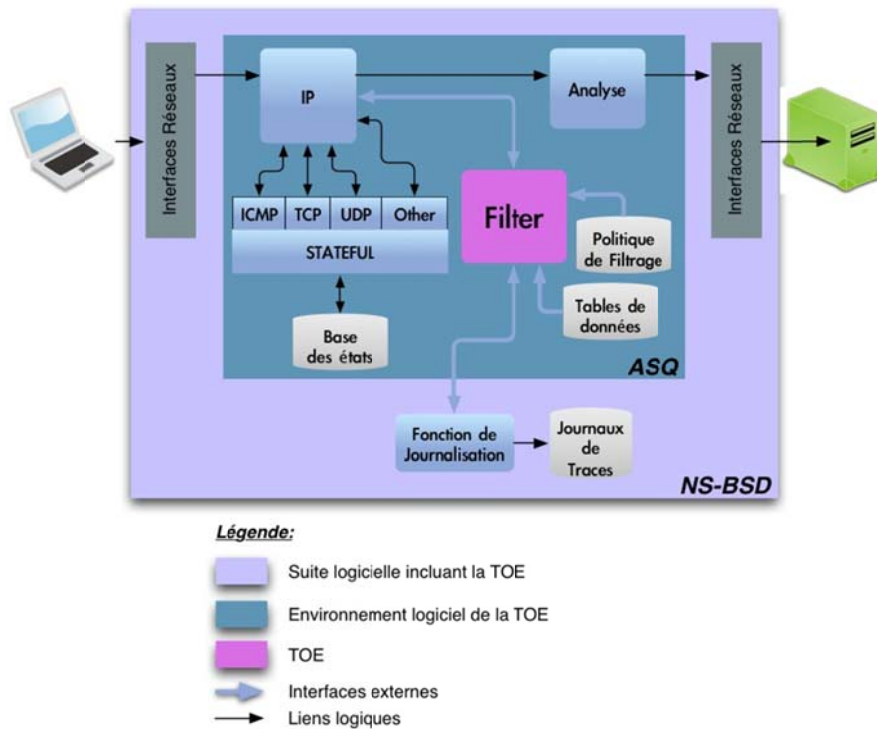


Figure 2 – Architecture logique de la TOE

Le schéma Figure 3 place la TOE dans son environnement et les différentes interconnexions.



Le composant ASQ est en charge de l'application de la politique de filtrage des flux d'information et de leur analyse.



1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- **Développement** : développement du produit ;
- **Déploiement** : mise à disposition du produit aux clients ;
- **Installation** : installation du produit conformément aux recommandations fournies par *STORMSHIELD* dans les guides (voir [GUIDES]) ;
- **Exploitation** : suivi du produit au jour le jour lorsqu'il est en production avec remontée éventuelle de bugs ;
- **Rebus** : destruction d'un produit obsolète ou défaillant.

Seules les phases de développement et de déploiement (réalisées par *STORMSHIELD*) ont été évaluées.

Les phases d'installation, d'exploitation et de rebus sont réalisées par le client. Les guides associés sont référencés en annexe 2

Le produit a été développé sur les sites suivants :

STORMSHIELD

Parc Horizon – Bâtiment 6
Avenue de l'horizon
59650 Villeneuve d'Ascq
France

STORMSHIELD

22 rue du Gouverneur Général Eboué
Immeuble Axiom Bât. D – 2ème étage
92130 Issy-les-Moulineaux
France

L'évaluateur a considéré comme administrateurs du produit les personnes réalisant les opérations d'administration de la sécurité et responsables de leur exécution conformément aux guides [GUIDES], et comme utilisateurs du produit les personnes utilisant des ressources informatiques des réseaux de confiance protégés par le produit.

La définition des profils administrateurs est du ressort d'un administrateur spécial, le « super-administrateur », qui intervient exclusivement lors des phases d'installation et de maintenance et est le seul habilité à se connecter, via la console locale, sur les boîtiers. Il doit être le seul responsable de l'accès dans les locaux où sont stockés les boîtiers.

1.2.6. Configuration évaluée

Le certificat porte sur la configuration décrite dans le chapitre 2.3.1 de la cible de sécurité [ST].

Par ailleurs, la TOE a été configurée en désactivant les services suivants:

- les modules permettant la prise en charge des serveurs externes (ex : *Kerberos*, *RADIUS*, etc) ;
- le module de routage dynamique ;
- l'infrastructure à clés publiques (PKI) interne ;
- le module VPN SSL ;
- le cache DNS ;
- le moteur antivirus (ClamAV ou *KASPERSKY*) ;
- le module Active Update ;
- les services SSH, DHCP, MPD et SNMPD.

Les tests ont été effectués sur les boîtiers U30S, SN200 et SN910. Ces produits ont été jugés représentatifs de la gamme de produits. Ce certificat porte donc sur l'ensemble des boîtiers identifiés au paragraphe 1.1.

Les stations d'administration, A-UTI et B-UTI représentées dans la figure 3 sont des postes sous Windows Professionnel Seven 32 bits avec tous les correctifs publiés par Microsoft.

Une connexion VPN de type IPsec de site à site est configurée entre les LAN interne 1 et 2. Une connexion avec un poste nomade INT-UTI-1 est aussi configurée avec l'un des deux LAN.

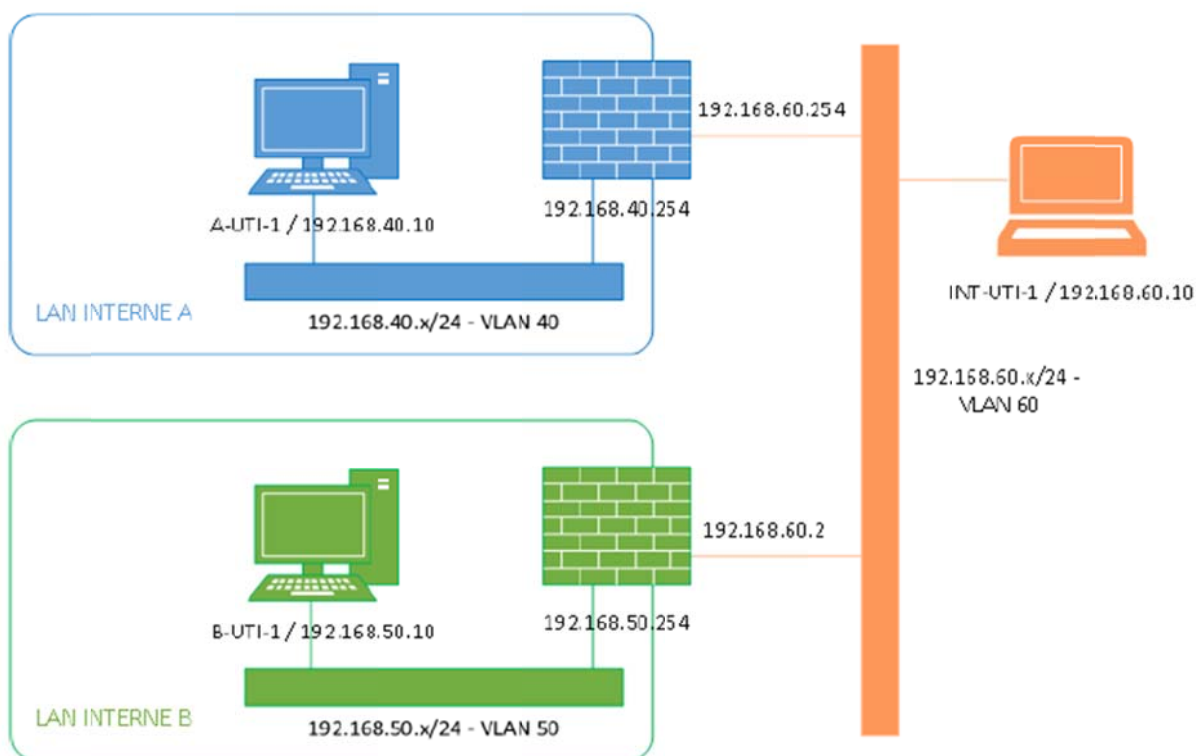


Figure 3 – Plateforme de test

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 25 mai 2016, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « réussite ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La TOE ne comporte pas de mécanismes cryptographiques.

2.4. Analyse du générateur d'aléas

La TOE ne comporte pas de générateur d'aléas.

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. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que la « Fonction de filtrage de la Suite logicielle STORMSHIELD Firewall, version 2.2.6 » embarquée sur l'un des boîtiers listés au paragraphe 1.1, soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté du composant ALC_FLR.3.

3.2. 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 d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- se conformer à la configuration évaluée et respecter les restrictions d'usage mentionnées dans le rapport de certification [ANSSI-CC-2016/55] dans la mesure où cette fonction est intrinsèquement liée à suite logicielle dans son ensemble ;
- conserver désactivés les services listés dans les guides [GUIDES] à la section « Configurations et mode d'utilisation soumis à l'évaluation ».

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires², des certificats Critères Communs.

La reconnaissance dans le cadre de ce projet de réévaluation, bénéficie du programme de transition et s'applique ainsi jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR lorsque les dépendances CC sont satisfaites

Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

² Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

| Classe | Famille | Composants par niveau d'assurance | | | | | | | Niveau d'assurance retenu pour le produit | |
|--|---------|-----------------------------------|-------|-------|-------|-------|-------|-------|---|--|
| | | EAL 1 | EAL 2 | EAL 3 | EAL 4 | EAL 5 | EAL 6 | EAL 7 | EAL 4+ | Intitulé du composant |
| ADV Développement | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security architecture description |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | 4 | Complete functional specification |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 | 1 | Implementation representation of TSF |
| | ADV_INT | | | | | 2 | 3 | 3 | | |
| | ADV_SPM | | | | | | 1 | 1 | | |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 | 3 | Basic modular design |
| AGD Guides d'utilisation | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Operational user guidance |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Preparative procedures |
| ALC Support au cycle de vie | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 | 4 | Production support, acceptance procedures and automation |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | 4 | Problem tracking CM coverage |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Delivery procedures |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | 1 | Identification of security measures |
| | ALC_FLR | | | | | | | | 3 | Systematic flaw remediation |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | 1 | Developer defined life-cycle model |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 | 1 | Well-defined development tools |
| ASE Evaluation de la cible de sécurité | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Conformance claims |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Extended components definition |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ST introduction |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Security objectives |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Derived security requirements |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security problem definition |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TOE summary specification |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | 2 | Analysis of coverage |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 | 1 | Testing: basic design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | 1 | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | Independent testing: sample |
| AVA Estimation des vulnérabilités | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | 3 | Advanced methodical vulnerability analysis |

Annexe 2. Références documentaires du produit évalué

| | |
|--------------------|--|
| [ST] | Cible de sécurité de référence pour l'évaluation : Stormshield Network Security UTM / NG-Firewall Filtering Function, version 2.2 – EAL4 Security Target, référence SN_ASE_sectarget_filter_v2, version 2.5. |
| [RTE] | Rapport technique d'évaluation : <ul style="list-style-type: none">- Evaluation Technical Report URANUS Project, référence OPPIDA/CESTI/URANUS/ETR, version 1.0. |
| [CONF] | Liste de configuration du produit : <ul style="list-style-type: none">- référence : SN_ALC_sources_liste_v2,- liste des fournitures - Fonction de Filtrage & Suite logicielle Stormshield Firewall version 2, référence SN_ADV_FSP_TSFI_SFR_v2, version 2.9. |
| [ANSSI-CC-2016/55] | Rapport de certification du produit : « Suite logicielle STORMSHIELD Firewall, version 2.2.6 » |
| [GUIDES] | Guide d'installation du produit : <ul style="list-style-type: none">- Guide Firewalls Stormshield Network Présentation et Installation Produits Gamme SN, référence snfrgde_installation-produit-GammeSN, version 1.4. Guide d'utilisation et configuration du produit : <ul style="list-style-type: none">- Guide Stormshield Network Firewall Manuel d'utilisation et de configuration, version 2, référence snfrgde_FirewallUserGuide-v2, version 2.2.5. Guide de restauration logicielle par clé USB : <ul style="list-style-type: none">- TECHNICAL NOTE Stormshield Network Firewalls Software Recovery via USB key, ref. smentno_USB_Recovery, version 1.1 Guide de démontage du boîtier pour garantir la confidentialité lors d'une panne ou la mise au rebut : <ul style="list-style-type: none">- TECHNICAL NOTE Stormshield Network Firewalls SECURE RETURN option, ref. smentno_secure-return, version 1.1 |

Annexe 3. Références liées à la certification

| | |
|---|---|
| <p>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.</p> | |
| [CER/P/01] | <p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.</p> |
| [CC] | <p>Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.</p> |
| [CEM] | <p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.</p> |
| [CC RA] | <p>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.</p> |
| [SOG-IS] | <p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.</p> |
| [REF] | <p>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.</p> |