

PREMIER MINISTRE

Secrétariat général  
de la défense  
et de la sécurité nationale

Agence nationale de la sécurité  
des systèmes d'information

Bureau Qualification et Agrément

Paris, le 29 NOV. 2017  
N° 5996/ANSSI/SDE/PSS/BQA

**DECISION DE QUALIFICATION D'UN PRODUIT**  
**AU NIVEAU STANDARD**

**SUITE LOGICIELLE *STORMSHIELD NETWORK SECURITY FIREWALL* version 2.7.2**  
***STORMSHIELD***

Pièces constitutives de la décision de qualification :

**Fiche 1** : Description du produit.

**Fiche 2** : Conditions et limites de la qualification.

**Fiche 3** : Base documentaire de la qualification.

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

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1<sup>er</sup> ;

Vu le décret du 27 mars 2017 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Décide :

Art. 1<sup>er</sup> – La suite logicielle *STORMSHIELD NETWORK SECURITY* en version 2.7.2 fournie par *STORMSHIELD* embarquée sur l'un des boîtiers suivants : SN200, SN300, U30S, U70S, SN500, SN510, SN700, SN710, SN900, SN910, U150S, U250S, U500S, SN2000, SN3000, SN6000 respecte les règles fixées par le décret n° 2015-350 du 27 mars 2015<sup>1</sup> et est qualifiée au niveau standard sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – La fonctionnalité *Virtual Private Network* (VPN) du produit est agréée pour la protection des informations marquées *Diffusion Restreinte* ou classifiées au niveau *Diffusion Restreinte OTAN* ou *Restreint UE/UE Restricted*.

Art. 3 – La présente décision est valable pour une durée de 3 ans.

Art. 4 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

Guillaume POUPARD  
Directeur général de l'agence nationale  
de la sécurité des systèmes d'information

<sup>1</sup> Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Disponible sur <https://www.legifrance.fr>.

## Fiche 1

### Description du produit

#### Désignation et versions

Le produit qualifié est la suite logicielle *STORMSHIELD NETWORK SECURITY FIREWALL*, version 2.7.2 développée par *STORMSHIELD*.

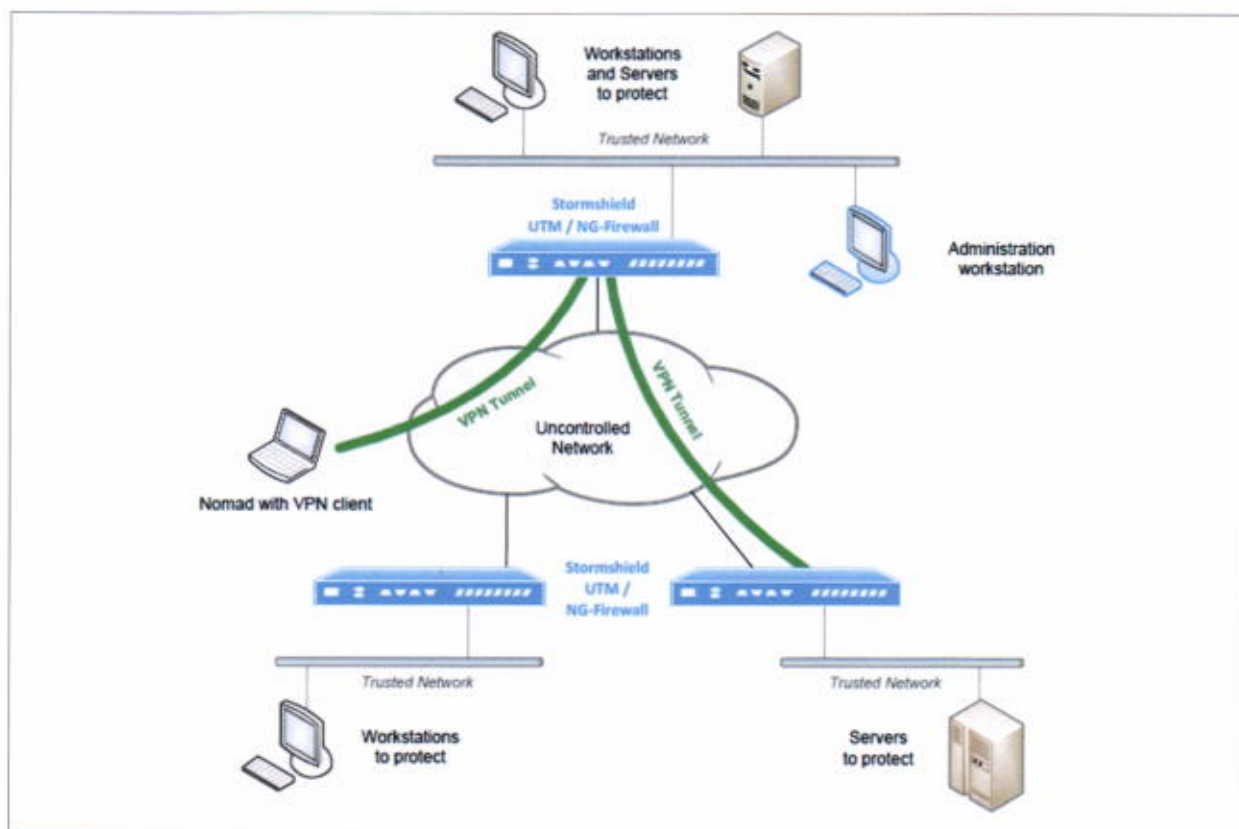


Figure 1. Cas d'usage classique du produit

#### Présentation générale

La suite logicielle *FIREWALL SNS* apporte les fonctions de sécurité pour l'interconnexion entre plusieurs réseaux de confiance à travers un réseau non-contrôlé, sans compromettre ces mêmes réseaux de confiance.

Cette suite logicielle offre les services :

- de filtrage ;
- de *VPN* (avec chiffrement et authentification) implémentant le protocole *ENCAPSULATING SECURITY PAYLOAD (ESP)* du standard *IPSEC* en mode tunnel ;
- de gestion de la bande passante ;
- de gestion de la politique de sécurité ;
- d'audit, d'imputabilité ;
- d'authentification forte des administrateurs.

## Fiche 2

### Conditions et limites de la qualification

#### Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

- C1. L'utilisateur du produit certifié respecte les objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [CDS], et suit les recommandations se trouvant dans le guide [GUIDE], notamment :
- se conformer à la configuration évaluée telle que spécifiée dans [CDS] ;
  - conserver désactivés les services listés dans le guide [GUIDE] à la section « Configurations et mode d'utilisation soumis à l'évaluation » ;
  - modifier la politique de gestion des mots de passe par défaut, comme décrit dans le guide [GUIDE] 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 du guide [GUIDE] ;
  - réaliser les tâches d'administration depuis des postes sécurisés comme précisé dans la cible de sécurité [CDS] ;
  - bloquer l'accès au port 1300 du produit ;
  - employer les algorithmes cryptographiques et les tailles de clés correspondant aux options spécifiées dans la cible de sécurité [CDS, §5.2.5] et dans le guide [GUIDE].
- C2. Les guides d'installation, d'administration et utilisateurs [GUIDE] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie.
- C3. L'utilisateur s'assure de la bonne activation de la protection contre les tunnels *DNS* en lançant dans une console les lignes de commande comme décrit dans le guide [GUIDE].
- C4. En cas d'utilisation d'interface virtuelle *IPSEC*, il n'est défini qu'une seule *VTI* par paire de correspondants.
- C5. Aucune règle de filtrage n'est définie si celle-ci porte sur une interface ayant une adresse attribuée par DHCP ou via un modem. Si toutefois une telle règle est nécessaire, il faut désactiver l'optimisation inadaptée à ce type d'interface en utilisant les commandes suivantes dans la console :
- `setconf ~/ConfigFiles/Filter/filter Config Optimize 0`
  - `enfilter -u`

- C6. Dans le cas où il faudrait laisser un service d'administration NSRPC, la politique de filtrage est configurée afin de n'autoriser l'accès au service NSRPC d'administration du boîtier (port 1300/TCP) qu'aux adresses IP des postes d'administration autorisés.

**Limites**

- L1. Seules les fonctions décrites dans la fiche 1 sont couvertes par la présente décision de qualification.

### Fiche 3

#### Base documentaire de la qualification

##### Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, version 1.0 du 6 janvier 2017. Disponible sur <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a> .
[LPM]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Disponible sur <a href="http://www.legifrance.gouv.fr">http://www.legifrance.gouv.fr</a> .

##### Documents rédigés par le centre d'évaluation

[OUREA]	<i>OUREA-URANUS-TEST REPORT</i> version : 2.0 en date du : 23 mai 2016
[RTE]	Rapport technique d'évaluation, <i>OPPIDA</i> référence : OPPIDA/CESTI/OUREA-URANUS-2017/AVA/1.0 version : 1.0 en date du : 15 juin 2017

##### Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification, référence : ANSSI-CC-2016/55 en date du : 26 août 2016
[QS]	Courrier de Qualification, référence : 4093/ANSSI/SDE du 4 octobre 2016
[DEC_QS]	Décision de Qualification, référence : 4094/ANSSI/SDE du 4 octobre 2016

##### Guides d'utilisation et documentations techniques de l'industriel

[GUIDE]	Guide <i>STORMSHIELD NETWORK FIREWALL</i> , Manuel d'utilisation et de configuration version : 2.2.5
[CDS]	Cible de sécurité, du <i>STORMSHIELD NETWORK SECURITY UTM/NG-FIREWALL SOFTWARE SUITE v.2.2</i> référence : SN_ASE_sectarget_v2 version : 2.9a en date du : 20 juillet 2016
[ANALYSE D'IMPACT]	SN_Nouveautés 2.7.2 vs 2.2.6 version : 1.5 en date du : 13 février 2017