

Secrétariat général
de la défense
et de la sécurité nationale

Paris, le 04 OCT. 2016

N°4094/ANSSI/DIR

Agence nationale de la sécurité
des systèmes d'information

QUALIFICATION AU NIVEAU STANDARD

SUITE LOGICIELLE STORMSHIELD FIREWALL VERSION 2.2.6
sur boîtiers SN200, SN300, U30S, U70S, SN500, SN510, SN700, SN710, SN900, SN910, U150S,
U250S, U500S, SN2000, SN3000, SN6000
STORMSHIELD

Références :

- [1] Processus de qualification d'un produit de sécurité - niveau standard -, version 1.2.
- [2] Cible de sécurité du STORMSHIELD Network Security UTM / NG-Firewall Software Suite, version 2.2 – EAL3 Security Target, référence SN_ASE_sectarget_v2, version 2.9a.
- [3] Rapport de certification ANSSI-CC-2016/55 Suite logicielle STORMSHIELD Firewall version 2.2.6.
- [4] Guide STORMSHIELD Network Firewall Manuel d'utilisation et de configuration, version 2, référence snfrgde_FirewallUserGuide-v2, version 2.2.5.

La suite logicielle Firewall SNS en version 2.2.6 offre des fonctionnalités de type VPN permettant de sécuriser la transmission de données entre des sites distants, et de type pare-feu qui regroupent notamment des fonctions de filtrage, gestion de la bande passante, gestion de la politique de sécurité, journalisation, audit, imputabilité et d'autoprotection.

Conformément au processus de qualification en première référence et sur la base :

- de la cible de sécurité en deuxième référence ;
- du rapport de certification, en troisième référence ;

et sous réserve :

- que l'utilisateur du produit s'assure du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [2], et suive les recommandations se trouvant dans le guide [4], notamment :
 - se conformer à la configuration évaluée décrite dans [2] paragraphe 2.3.1 ;
 - conserver désactivés les services listés dans le guide [4] 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 [4] afin d'en définir une qui soit 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 [4] ;

- réaliser les tâches d'administration depuis des postes sécurisés comme précisé dans la cible de sécurité ;
- 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 [2, §5.2.5] et dans le guide [4] ;
- qu'en cas d'utilisation d'interface virtuelle IPSec, il ne soit défini qu'une seule VTI par paire de correspondants ;
- que pour l'implémentation du protocole SRP, une fonction de hachage SHA2 soit utilisée ;
- qu'aucune règle de filtrage ne soit définie si celle-ci porte sur une interface ayant une adresse attribuée par DHCP ou via un mode (si toutefois une telle règle est nécessaire, il faut désactiver l'optimisation inadaptée à ce type d'interface en lançant dans une console les commandes suivantes :
 - `setconf ~/ConfigFiles/Filter/filter Config Optimize 0`
 - `enfilter -u`
- que dans le cas où il faille laisser un service d'administration NSRPC, la politique de filtrage soit 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 autorisées,

j'atteste que la suite logicielle Firewall SNS en version 2.2.6 embarquée sur l'un des boîtiers suivants SN200, SN300, U30S, U70S, SN500, SN510, SN700, SN710, SN900, SN910, U150S, U250S, U500S, SN2000, SN3000, SN6000, atteint le niveau de qualification standard.

De plus, la fonctionnalité VPN de ce produit est agréée pour la protection d'informations marquées *Diffusion Restreinte*, ou classifiées au niveau *Diffusion Restreinte OTAN* ou *Restreint UE / EU Restricted*.

Cette qualification est valable pour une durée de 3 ans. Elle pourra être prolongée par la mise sous surveillance du produit certifié.

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