PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Le Directeur général

Paris, le 22 MARS 2024
N° 542 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

STORMSHIELD NETWORK SECURITY UTM / NG-FIREWALL SOFTWARE SUITE

STORMSHIELD

RCS 428 173 975

2-10, Rue Marceau
92130 ISSY-LES-MOULINEAUX
France

Pièces constitutives de la décision de qualification :
Fiche 1 : Description du produit
Fiche 2 : Versions du produit
Fiche 3 : Conditions et limites de la qualification
Fiche 4 : Base documentaire de la qualification

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

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment son article 9 ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu le 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 ;

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 1er ;

Vu le décret du 4 janvier 2023 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. STRUBEL (Vincent) ;

Vu l'Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles ;

Vu l'instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne ;

Vu l'instruction générale interministérielle n° 2100 du 1er décembre 1975 sur l'application en France du système de sécurité de l'organisation du traité de l'atlantique nord ;

Vu le processus de qualification d'un produit ;

Vu le processus d'agrément d'un produit,

Décide que :

Art. 1er – Le produit fourni par la société ***STORMSHIELD*** portant le nom « STORMSHIELD NETWORK SECURITY UTM / NG-FIREWALL SOFTWARE SUITE » et dont les versions sont identifiées en fiche 2 respecte les règles fixées par les décrets n° 2010-112 du 2 février 2010 et n° 2015-350 du 27 mars 2015 est qualifié au niveau standard sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 3.

Art. 2 – Les fonctionnalités pare-feu et réseau privé virtuel du produit dont les versions sont identifiées en fiche 2 sont agréées pour la protection des informations marquées ***Diffusion Restreinte, NATO Restricted*** et classifiées au niveau ***Restreint UE/EU Restricted.***

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

Vincent STRUBEL
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

Fiche 1

Description du produit

Le produit qualifié est la solution matérielle et logicielle STORMSHIELD NETWORK SECURITY UTM / NG-FIREWALL SOFTWARE SUITE en versions spécifiées en fiche 2, fournie par l'entreprise STORMSHIELD.

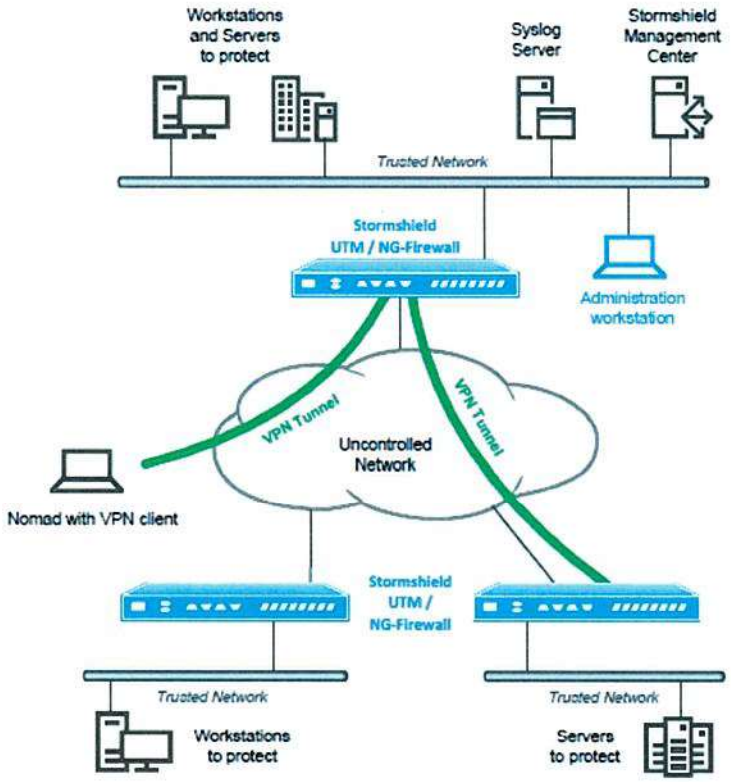

Figure n°1 – Cas d'usage classique du produit

Présentation générale

Le produit permet d'interconnecter un ou plusieurs réseaux de confiance via un réseau non maitrisé sans dégrader le niveau de confiance.

Les principales fonctions offertes sont les suivantes :

- Firewall (*Pare-feu*) : filtrage, détection d'attaques, gestion de la bande passante, gestion des politiques de sécurité, audit, responsabilisation et authentification forte des administrateurs ;
- VPN (*Virtual Private Network*) : chiffrement et authentification mettant en œuvre le protocole Encapsulating Secrity Payload (ESP) du standard IPSec en mode tunnel.

Les fonctions évaluées sont précisément :

- Le filtrage des flux ;
- Le chiffrement (au niveau IP) des communications entre les équipements ;
- La prévention d'intrusion basée sur une analyse de conformité protocolaire ;

- La protection des opérations d'administration de la sécurité (y compris via la console d'administration centralisée SMC) ;
- La journalisation des événements, en local ou à distance (vers un serveur Syslog TLS).
- L'enrôlement de certificat via le protocole EST (Enrollment over Secure Transport, RFC 7030).

Fiche 2

Versions du produit

Version du matériel	Version du logiciel
SN210, SN220, SN310, SN320, SN510, SN520, SN710, SN720, SN910, SN920, SN1100, SNxr1200, SN2000, SN2100, SN3000, SN3100, SN6000, SN6100, SNi20 etSNi40	4.3.x (Avec x ≥ 12)

Fiche 3

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 ainsi s'assurer que :

C1. L'utilisateur du produit qualifié et agréé doit s'assurer du respect des objectifs de sécurité lors du déploiement, de la configuration et de l'utilisation du produit tout au long de son cycle de vie, tels que spécifiés dans la cible de sécurité [**CDS**] et dans les guides fournis [**GUIDES**] ;

C2. Les administrateurs sont informés de la politique de sécurité du système d'information, et doivent contrôler que les règles de filtrage et de chiffrement qui sont implémentées sont conformes avec la politique de sécurité ;

C3. Le produit qualifié est installé dans un environnement sécurisé protégé de tout accès physique non autorisé ;

C4. Le SMC et l'IGC externe de gestion des certificats sont installés dans un environnement sécurisé qui empêche tout accès physique non autorisé ;

C5. L'installation du produit qualifié est en coupure du flux de communication, interdisant toute possibilité de contournement de l'équipement ;

C6. Les terminaux utilisés pour la gestion et l'administration du produit qualifié sont durcis et protégés contre des attaques qui pourraient mener à une fuite d'information liées aux biens sensibles (clés, topologie, configuration ...) ;

C7. L'accès au SMC est restreint conformément aux règles de contrôle d'accès du réseau d'administration de l'organisation utilisatrice ;

C8. Le contrôle d'accès aux bases de données internes du SMC doit limiter leur consultation aux seuls utilisateurs locaux ayant les droits d'accès au système d'exploitation du SMC ;

C9. Le système d'exploitation du SMC doit être maintenu en condition de sécurité par l'application régulière des corrections de sécurité corrigeant ou rendant inexploitables les éventuelles vulnérabilités ;

C10. Les modules que Stormshield fournit en option pour la prise en charge de ses services sont désactivés par défaut et doivent le rester dans le cadre de la mise en œuvre de la configuration qualifiée ;

C11. Les équipements de réseau avec lesquels la TOE établit des tunnels VPN sont soumis à des restrictions concernant l'accès physique et la protection de la configuration équivalentes aux restrictions appliquées à la TOE ;

C12. Les postes de travail exécutant les clients VPN sont soumis à des restrictions concernant l'accès physique et la protection de leur configuration. Ils sont sécurisés et maintenus à jour ;

C13. L'environnement informatique fournit des horodatages fiables par l'intermédiaire du protocole NTP.

Limites

La décision de qualification est valide sous réserve du respect de la limite d'utilisation suivante :

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

Fiche 4

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, référence QUAL-PROD-PROCESS, version en vigueur. Disponible sur https://cyber.gouv.fr/procedures-et-formulaires-pour-la-qualification
[PROCESS_AGREMENT]	Processus d'agrément des produits de sécurité n°001047/SGDSN/DCSSI/SDR du 16 mai 2003.
[RGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Disponible sur https://www.legifrance.gouv.fr
[II 901]	Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles. Disponible sur https://www.legifrance.gouv.fr/.
[IGI 2102]	Instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne

Documents rédigés par le centre d'évaluation

[RTE]	Rapport technique d'évaluation - référence : OPPIDA/CESTI/THEIA/RTE - version : 3.0 - date : 24/11/2023 Rapport d'analyse des mécanismes cryptographiques - référence : OPPIDA/CESTI/THEIA/CRYPTO - version : 2.1 - date : 06/09/2023

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

[CERTIF]	Rapport de certification - référence : ANSSI-CC-2023/62 - date : 08/12/2023
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - référence : ANSSI-PG-083 - version : 2.04 - date : 01/01/2020

Guides d'utilisation et documentations techniques de l'industriel

[CDS]	STORMSHIELD NETWORK SECURITY UTM/NG-FIREWALL SOFTWARE SUITE VERSION 4, EAL4+ SECURITY TARGET - référence : SN_ASE_sectarget_v4 - version : 4.8 - date : 07/08/2023
[GUIDES]	Voir 1.5.1 TOE Guides de la cible de sécurité [CDS]