Stormshield Network Security

Pare-feu Industriel SNi40

Suite logicielle version 2.3.4

Cible de Sécurité CSPN

Document version : 1.3

Référence : SN_ASE_cible_CSPN

Date: 29/06/2016

HISTORIQUE DES MODIFICATIONS

Version	Date	Modifications
1.3	29/06/2016	Mise à jour de la version de la TOE en 2.3.4
1.2	15/12/2015	Quelques précisions sur la configuration évaluée.
1.1	09/12/2015	Précisions sur le périmètre fonctionnel et la configuration évaluée. Précisions sur la fonction d'analyse de conformité protocolaire.
1.0	30/10/2015	Première version soumise à l'ANSSI
0.0	30/09/2015	Premier draft

TABLE DES MATIERES

TERMINOLOGIE ET SIGLES UTILISES

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Politique de filtrage	Ensemble de règles techniques décrivant quelles entités ont le droit d'établir des flux d'information avec quelles autres entités.
Réseau de confiance	Un réseau est dit de confiance si, du fait qu'il est sous le contrôle de l'exploitant de la TOE, la politique de sécurité interne n'implique pas qu'il faille se protéger des flux qui en proviennent, mais au contraire implique qu'il faille les protéger des flux qui y parviennent
Réseau non maîtrisé	Un réseau est dit non maîtrisé s'il n'est pas sous le contrôle de l'exploitant de la TOE, ce qui implique qu'il faille se protéger des flux établis avec les équipements de ce réseau (par exemple Internet).
TOE	Target of Evaluation Désigne le composant de l'évaluation.

DOCUMENTS DE REFERENCE

[QUALIF_ELEM]	Référentiel général de sécurité - Processus de qualification d'un produit de sécurité – niveau élémentaire Version 1.0
[PP_PFI]	Profil de protection d'un pare-feu industriel Version 1.0 court-terme - GTCSI 13 juillet 2015
[GUIDE_ANSSI]	La cybersécurité des systèmes industriels Méthode de classification et mesures principales, ANSSI, janvier 2013

1 IDENTIFICATION DU PRODUIT

Editeur	Stormshield
Site de l'éditeur	www.stormshield.eu
Nom commercial du produit	Stormshield Network Security
Version évaluée	Modèle SNi40 – Suite logicielle version 2.3.4
Catégorie de produit	Pare-feu industriel

2 DESCRIPTION

2.1 Présentation générale des produits Stormshield Network Security

Les firewall-VPN de la gamme Stormshield Network Security sont des boîtiers appliances permettant de sécuriser l'interconnexion entre un ou plusieurs réseaux de confiance et un réseau non maîtrisé, sans dégrader le niveau de sécurité du ou des réseaux de confiance.

Les fonctionnalités principales des appliances Stormshield consistent en deux grands groupes :

- la fonctionnalité firewall regroupant : filtrage, détection d'attaques, gestion de la bande passante, gestion de la politique de sécurité, audit, imputabilité, authentification forte des administrateurs,
- la fonctionnalité VPN (Réseau Privé Virtuel : chiffrement et authentification) implémentant le protocole ESP en mode tunnel du standard IPSec, et sécurisant la transmission des données confidentielles entre sites distants, partenaires ou commerciaux nomades.

L'ASQ (Active Security Qualification) est une technologie de Prévention d'Intrusion en Temps Réel, intégrée dans toutes les appliances Stormshield. Basée sur une analyse multi-couches, l'ASQ détecte et empêche les attaques les plus élaborées sans diminuer les performances de l'appliance et réduit considérablement le nombre de faux positifs. Cette technologie est soutenue par des fonctionnalités d'alarme entièrement configurables.

2.2 Descriptif général de la TOE

Le produit évalué est un pare-feu industriel. Il est destiné à fonctionner dans des environnements physiques hostiles où des pare-feu classiques pourraient ne pas fonctionner du fait de la chaleur, de l'humidité ou de la poussière par exemple.

D'un point de vue fonctionnel, ce pare-feu permet d'assurer l'interconnexion entre un réseau industriel que l'on cherche à protéger et un autre réseau qui présente certaines des caractéristiques suivantes :

- une moins bonne maitrise et niveau de confiance moindre ;
- des applications spécifiques n'ayant aucune interaction avec le réseau industriel ;
- un autre réseau industriel avec des fonctionnalités différentes ;
- des domaines de responsabilité différents.

Ce pare-feu peut-être positionné et agir en tant que pont Ethernet ou routeur IP pour les protocoles IP. Il réalise un contrôle des flux, un filtrage et une réécriture des protocoles, du niveau 3 jusqu'au niveau applicatif selon les protocoles connus et inspectés.

L'évaluation porte sur le périmètre fonctionnel suivant :

- le filtrage dynamique des flux IP aux niveaux 3 et 4,
- l'analyse et le contrôle des protocoles industriels implémentés,
- la gestion et l'authentification locale des administrateurs,
- la journalisation des événements.

La configuration évaluée précise est fournie en section 2.8.

2.3 Fonctions de sécurité

Filtrage réseau

La ToE dispose de fonctions de filtrage dynamique aux niveaux 3 et 4 (*stateful firewall*).

Analyse protocolaire

La ToE vérifie que les paquets reçus sont bien conformes aux normes spécifiant les protocoles mis en œuvre.

L'évaluation porte principalement sur les protocoles industriels Modbus, S7 et UMAS.

Fonction d'administration

L'outil d'administration Stormshield Web Manager permet, via une interface graphique intuitive et conviviale, l'installation et de la configuration des appliances Stormshield, et offre des fonctionnalités de monitoring et de reporting simplifiées.

Afin d'assurer une authentification forte des administrateurs, l'appliance Stormshield intègre une base d'utilisateurs et offre des services d'authentification auprès de celle-ci.

Journalisation locale d'évènements

La ToE permet de définir une politique de journalisation locale des évènements de sécurité ou d'administration.

Journalisation distante d'évènements

La ToE permet de définir une politique de journalisation distante pour des évènements de sécurité, d'administration ou autres.

Les événements sont envoyés en UDP vers un serveur Syslog central ou via des traps SNMP.

2.4 Utilisation du produit

En application des recommandations du [GUIDE_ANSSI], le pare-feu industriel peut être utilisé pour isoler des réseaux de criticités différentes (classe 1 et classe 2).

Il peut également être utilisé pour protéger un réseau industriel connecté à un système d'information de gestion.

Enfin, il peut être utilisé pour cloisonner différentes parties d'un système industriel.

Lorsque la disponibilité est critique, deux pare-feu peuvent être montés en redondance pour augmenter la résilience de l'interconnexion. Un schéma de l'utilisation d'un pare-feu est donné sur la Figure 1.

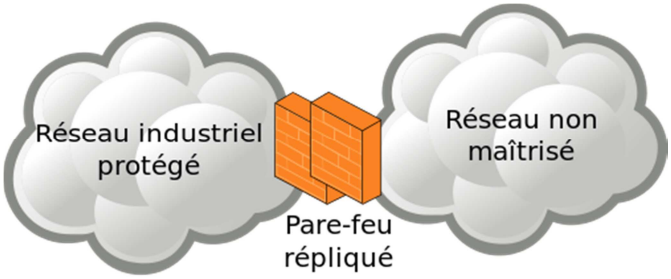

Figure 1: Exemple d'utilisation de la TOE

2.5 Utilisateurs typiques

La liste des types d'utilisateurs susceptibles d'interagir avec la ToE est la suivante :

Administrateur	Utilisateur ayant les droits de modifier une partie de la configuration de la ToE. Il ne peut cependant pas modifier les comptes des administrateurs.
Auditeur	Utilisateur ayant le droit de consulter tout ou partie des journaux d'évènements produits par la ToE.
Super-administrateur	Utilisateur ayant tous les droits sur la ToE, pouvant en particulier créer, modifier ou supprimer les comptes des administrateurs.
Équipement terminal	Équipement terminal connecté directement ou indirectement à la ToE.

Note : Un utilisateur n'est pas forcément une personne physique et peut être un équipement ou un programme tiers. Par ailleurs, une même personne physique peut être titulaire de plusieurs comptes avec des profils d'utilisateur différents.

2.6 Hypothèses sur l'environnement

Consultation des journaux

Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par l'équipement.

Administrateurs

Les administrateurs de la ToE sont compétents, formés et non hostiles.

Super-administrateurs

Les super-administrateurs de la ToE sont compétents, formés et non hostiles.

Local

La ToE doit se trouver dans un local sécurisé dont l'accès est restreint à des personnes autorisées considérées comme non hostiles. En particulier, l'attaquant n'aura pas accès aux ports physiques de la ToE.

En revanche, des équipements identiques à la ToE étant disponibles dans le commerce, l'attaquant peut acheter un tel équipement en vue d'y rechercher des vulnérabilités par tous les moyens à sa disposition pour attaquer la ToE.

Politique de filtrage

La politique de filtrage configurée dans la ToE est considérée comme adaptée au cas d'usage.

Dimensionnement

Il est supposé que la ToE est dimensionnée correctement pour le traitement qu'elle doit effectuer.

Activation des journaux

Les fonctions de journalisation locale et distante sont supposées fonctionnelles. Les journaux locaux sont supposés intègres et authentiques.

Services non-évalués désactivés par défaut

La plupart des services présents dans la ToE mais hors de la cible de sécurité sont désactivés dans la configuration par défaut (parfois appelée configuration usine).

Il faut en plus désactiver les services hors cible suivants :

- Le Serveur DHCP IPv4.
- Les analyses IPS des protocoles non évalués.

La liste précise des services non évalués est fournie en section 2.8 ci-dessous.

Documentation de sécurité

La ToE est fournie avec une documentation détaillée sur l'utilisation sécurisée de l'équipement. En particulier, le mot de passe administrateur par défaut est identifié pour permettre leur personnalisation.

L'ensemble des préconisations issues de cette documentation ont été appliquées en vue de l'évaluation.

2.7 Plateforme d'évaluation

La plateforme d'évaluation comprend :

- Un pare-feu Stormshield modèle SNi40
- Une poste d'administration sous Windows 7.
  Le navigateur utilisé est Microsoft Internet Explorer version 9.

2.8 Configuration et mode d'utilisation soumis à l'évaluation

La configuration et le mode d'utilisation soumis à l'évaluation sont les suivants :

- La console locale n'est pas utilisée en exploitation. Seul le super-administrateur peut s'y connecter, et, par hypothèse, ce genre d'intervention ne se fait que lorsqu'une sortie du cadre de l'exploitation – pour procéder à une maintenance ou à une ré-installation – est décidée.
- Les stations sur lesquelles s'exécute la console d'administration à distance sont sécurisées, dédiées à cette utilisation, et à jour de tous les correctifs concernant leur système d'exploitation et les logiciels applicatifs qui les équipent.
- Tous les administrateurs sont soumis à une étape identification / authentification offerte par la TOE, et pouvant utiliser : une authentification identifiant / mot de passe dans un canal TLS ou une authentification mutuelle par certificat X.509 dans un canal TLS.
- Le mode de distribution des certificats et des CRL est manuel (importation).
- Les fonctions VPN de l'appliance Stormshield sont hors périmètre de l'évaluation.

- En cas d'émission des événements d'audit via syslog, le serveur qui les réceptionne ne fait pas partie de l'évaluation.
- En cas d'émission d'alertes via SNMP, seule la version v3 est activée.
- Le mode d'utilisation soumis à l'évaluation exclut le fait que la TOE s'appuie sur d'autres services tels que PKI, serveur DNS, DHCP, proxies. Les modules fournis en option pour la prise en charge de ces services sont désactivés par défaut et doivent le rester[1]. Il s'agit précisément :
    - des modules permettant la prise en charge des serveurs externes (ex : Kerberos, RADIUS...),
    - du module de routage dynamique,
    - de l'infrastructure à clés publiques (PKI) interne,
    - du module VPN SSL (Portail et Tunnel) ,
    - du cache DNS,
    - du moteur antivirus (ClamAV ou Kaspersky),
    - du module Active Update,
    - des serveurs SSH, DHCP, MPD et SNMPD,
    - du client DHCP et du démon NTP,
    - du relai DHCP,
    - du proxy Cache HTTP,
- Le serveur DHCP IPv4 doit être arrêté après l'initialisation de l'appliance.
- Bien que supportée, la fonctionnalité de routage IPv6 est désactivée par défaut et doit le rester dans le cadre de l'évaluation.
- Les administrateurs sont gérés par une base LDAP interne au logiciel Stormshield Firewall et qui fait partie de la TOE. Le mode d'utilisation soumis à l'évaluation exclut le fait que des clients LDAP externes à l'appliance Stormshield puissent se connecter à cette base.
- Les journaux d'audit doivent être configurés de manière à être stockés localement ou émis par Syslog.
- La technologie ASQ met en œuvre des analyses contextuelles au niveau applicatif, dans le but de vérifier la conformité aux RFC et de contrer les attaques au niveau applicatif. Les fonctions d'analyse applicative qui font l'objet de l'évaluation sont celles associées aux protocoles suivants :
    - au niveau transport : TCP, UDP,
    - au niveau applicatif : FTP, HTTP, SMTP, DNS, Modbus, S7, UMAS.

  Les autres protocoles non évalués sont bloqués par défaut et doivent le rester.
- La possibilité offerte par la politique de filtrage d'associer à chaque règle de filtrage une inspection applicative (proxies HTTP, SMTP, POP3, FTP) et une programmation horaire est hors du cadre de cette évaluation et ne devra pas être utilisée.
- La possibilité offerte par la politique de filtrage d'associer l'action « decrypt » (proxy SSL) à une règle de filtrage est hors du cadre de cette évaluation et ne devra pas être utilisée.
- Les fonctionnalités suivantes peuvent être utilisées, mais ne sont pas considérées comme des fonctions de sécurité :
    - la translation d'adresses (network address translation ou NAT) ;
    - le module de management des vulnérabilités ;
    - le module Haute Disponibilité ;

- la fonction de visualisation de rapports embarqués ;

- Les algorithmes cryptographiques mis en œuvre sont ceux de la configuration par défaut :
  - Authentification/Intégrité : SHA2-256 bits
  - Négociation de clé : Groupe Diffie-Hellman 14
  - Chiffrement : AES 256 bits mode CBC
  - PFS (Perfect Forward Secrecy) : activé

3 BIENS SENSIBLES PROTEGES

3.1 Biens sensibles de l'environnement

Matrice de flux

Par son action de filtrage, la ToE permet la communication entre équipements autorisés suivant un cadre défini. Par exemple dans le cadre d'un filtrage au niveau 4, une règle comprend les adresses source et destination, le protocole de transport (TCP, UDP…) et, le cas échéant, les ports source et destination.

Intégrité protocolaire

La ToE s'assure de la conformité protocolaire des échanges sur les flux identifiés dans sa configuration. En plus de cette conformité, la ToE permet éventuellement de limiter les fonctionnalités de certains protocoles.

Les besoins de sécurité pour les biens sensibles de l'environnement sont les suivants :

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Matrice de flux	●		●	
Intégrité protocolaire	●		●	

3.2 Biens sensibles de la TOE

Firmware

Afin d'assurer correctement ses fonctions, le firmware de la ToE doit être intègre et authentique.

Configuration

La configuration de la ToE doit être confidentielle et intègre. L'attaquant ne doit pas pouvoir découvrir cette configuration autrement que par l'observation de l'activité de la ToE.

Mécanisme d'authentification des utilisateurs

Ce mécanisme s'appuie sur une base de données locale.

La ToE doit protéger l'intégrité et l'authenticité de ce mécanisme.

Secrets de connexion des utilisateurs

Il s'agit des mots de passe des administrateurs.

La ToE doit garantir l'intégrité et la confidentialité de ces identifiants.

Politique de gestion des droits

Cette politique peut être contenue en local sur la ToE ou être obtenue à partir d'un annuaire distant. Dans les deux cas, la ToE doit garantir l'intégrité de cette politique de gestion des droits.

Les besoins de sécurité pour les biens sensibles de la ToE sont les suivants :

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Firmware			●	●
Configuration		●	●	
Mécanisme d'authentification des utilisateurs			●	●
Secrets de connexion des utilisateurs		●	●	
Politique de gestion des droits			●	

4 MENACES

4.1 Agents menaçants retenus

Équipement terminal malveillant

Un équipement terminal connecté à la ToE est contrôlé par l'attaquant.

Équipement d'administration malveillant

Un équipement présent sur le réseau d'administration de la ToE est contrôlé par l'attaquant sans que ce dernier ne dispose nécessairement d'identifiants d'authentification valides auprès de la ToE.

4.2 Menaces retenues

Déni de service

L'attaquant parvient à effectuer un déni de service sur la ToE en effectuant une action imprévue ou en exploitant une vulnérabilité (envoi d'une requête malformée, utilisation d'un fichier de configuration corrompu…). Ce déni de service peut concerner toute la ToE ou seulement certaines de ses fonctions.

Contournement de la politique de filtrage

L'attaquant parvient à violer la politique de filtrage en empêchant un flux légitime de transiter ou en permettant à un flux illégitime de transiter en provenance, à destination ou au travers de la ToE.

Violation de la conformité protocolaire

L'attaquant parvient à faire transiter des échanges non-conformes au protocole spécifié au travers de la ToE. L'attaquant parvient à contourner les limitations protocolaires configurées dans la ToE.

Corruption du firmware

L'attaquant parvient à injecter et faire exécuter un firmware corrompu sur la ToE. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée.

L'attaquant peut également réussir à substituer une mise à jour corrompue à une mise à jour légitime. Un utilisateur pourra alors tenter d'installer cette mise à jour dans la ToE par des moyens légitimes.

Enfin, l'attaquant peut également tenter d'installer une version légitime du firmware sans en avoir le droit.

Corruption de la configuration

L'attaquant parvient à modifier, de façon temporaire ou permanente, la configuration de la ToE.

Compromission de la configuration

L'attaquant parvient à récupérer tout ou partie de la configuration de la ToE de manière illégitime.

Vol d'identifiants

L'attaquant parvient à récupérer les secrets de connexion d'un utilisateur.

Contournement de l'authentification

L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

Contournement de la politique de droits

L'attaquant parvient à obtenir des droits qui ne lui sont pas normalement dévolus.

5 OBJECTIFS DE SÉCURITÉ

Gestion des entrées malformées

La ToE a été développée de manière à gérer correctement les entrées malformées, en particulier en provenance du réseau.

Application de la politique de filtrage

La ToE offre des possibilités de filtrage de flux entre des réseaux, basées sur des règles permettant de mettre en place la politique de sécurité du système d'information concerné.

Le filtrage est contextuel (stateful) **:** Après une action de filtrage effectuée uniquement en fonction du contenu du paquet, l'équipement établit un contexte en fonction du flux et du protocole associé qui permet d'augmenter la pertinence du filtrage par l'équipement.

Le filtrage contextuel ne peut s'effectuer que sur des flux au-dessus d'IP et prend en compte les couches transport (TCP/UDP) et éventuellement certaines couches applicatives (FTP).

Cette fonction de sécurité est également valable pour une ToE en redondance ou non.

Analyse de conformité protocolaire

La ToE vérifie la conformité des paquets reçus envers les normes des protocoles mis en œuvre. Cette analyse qui permet de détecter certaines attaques, est assurée :

- au niveau transport : TCP, UDP,
- au niveau applicatif : FTP, HTTP, SMTP, DNS, Modbus, S7, UMAS.

La ToE offre la possibilité d'autoriser ou non l'utilisation de "code fonction" pour les protocoles Modbus, UMAS et S7. En particulier, cela permet d'interdire :

- les commandes de modification (écriture) adressées aux équipements protégés,
- les commandes de maintenance (arrêt, mise à jour, ...) de ceux-ci.

Stockage sécurisé des secrets

Les secrets de connexion des utilisateurs sont stockés de manière sécurisée sur la ToE et la compromission d'un fichier ne permet pas de les récupérer.

Authentification sécurisée sur l'interface d'administration

Les jetons de session sont protégés contre le vol et contre le rejeu. Les jetons de session ont une durée de vie limitée. L'identité du compte utilisé est vérifiée systématiquement avant toute action privilégiée.

Politique de droits

La politique de gestion des droits est gérée de manière extrêmement stricte. L'implémentation de cette politique permet en particulier de garantir l'authenticité des opérations critiques, c'est-à-dire pouvant porter atteinte aux biens sensibles identifiés.

Signature du firmware

À chaque installation d'un nouveau firmware, l'intégrité et l'authenticité de celui-ci est vérifiée.

Intégrité et confidentialité de la configuration

La politique de gestion des utilisateurs ne permet à une personne non autorisée, ni de consulter, ni de modifier tout ou partie de la configuration de la ToE.