Profil de protection d'un pare-feu industriel

Version 1.0 moyen-terme

GTCSI

13 juillet 2015

Avant-propos

Dans toute la suite de ce document, l'acronyme ToE (*Target of Evaluation*) désigne le composant qui est l'objet de l'évaluation.

Les passages en rouge sont ceux qui différent de la version de la cible à court terme.

1 Descriptif du produit

1.1 Descriptif général du produit

La ToE considérée 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 un 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 routeur IP, proxy TCP ou encore pont Ethernet (mode stealth) pour des protocoles industriels non-IP. Il réalise un contrôle des flux, un filtrage et une réécriture des protocoles, du niveau 2 jusqu'au niveau applicatif selon les protocoles connus et inspectés.

1.2 Descriptif des fonctions du produit

La ToE comprend les fonctions suivantes :

— **Filtrage réseau :** La ToE dispose de fonctions de filtrage dynamique aux niveaux 3 et 4 (*stateful firewall*). Elle dispose également de fonctions de filtrage au niveau 2 lorsque l'équipement est en mode transparent (*stealth*).
— **Analyse protocolaire :** La ToE vérifie que les paquets reçus sont bien conformes aux normes spécifiant les protocoles mis en œuvre. Cette fonctionnalité n'est pas nécessairement présente sur tous les équipements et il convient de vérifier que l'équipement choisi supporte bien les protocoles désirés.
— **Fonctions d'administration :** La ToE dispose de fonctions permettant de configurer ou, dans certains cas, de programmer l'ensemble des autres fonctionnalités. Différentes interfaces d'administration sont envisageables :
  — des clients lourds (appelés également, en fonction du contexte, consoles d'administration, de programmation ou de configuration),
  — des clients légers comme des clients web,
  — des supports amovibles (cartes SD, clés USB).

— **Journalisation locale d'évènements :** La ToE permet de définir une politique de journalisation locale d'évènements notamment de sécurité et d'administration.
— **Journalisation distante d'évènements :** La ToE permet de définir une politique de journalisation distante d'évènements notamment de sécurité et d'administration.

1.3 Descriptif de l'utilisation du produit

En application des recommandations du guide [1] de l'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.

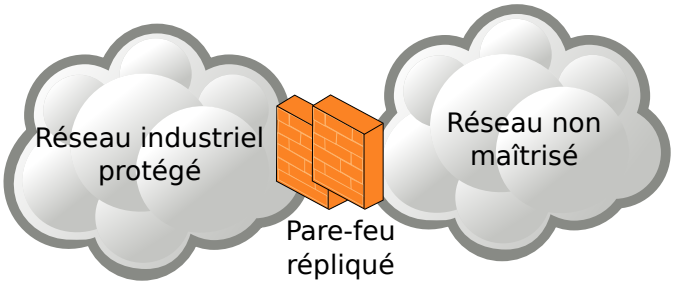

FIGURE 1 – Exemple d'utilisation d'un pare-feu industriel

1.4 Descriptif des différents utilisateurs

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.

1.5 Hypothèses sur l'environnement

Les hypothèses suivantes sont formulées sur l'environnement et les conditions d'utilisation de la ToE :
— **Consultation des journaux :** Il est considéré que les administrateurs consultent régulièrement les journaux locaux ou déportés générés par l'équipement.
— **Super-administrateurs :** Les super-administrateurs de la ToE sont compétents, formés et non hostiles.
— **Local :** La ToE n'est pas nécessairement dans un local sécurisé et l'attaquant peut avoir accès à tous les ports de la ToE. De façon similaire, l'attaquant peut arriver à faire brancher un dispositif piégé (par exemple une clé USB ou une carte SD) sur n'importe quel port physique de la ToE. En revanche, il ne peut pas la démonter ou effectuer d'attaque physique dessus.

1. *La cybersécurité des systèmes industriels : Méthode de classification et mesures principales*, ANSSI, janvier 2014.

On peut également noter que des équipements identiques à la ToE étant disponibles dans le commerce, l'attaquant peut acheter un tel équipement afin d'y rechercher des vulnérabilités par tous les moyens à sa disposition.

— **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 les traitements qu'elle doit effectuer.
— **Serveurs d'authentification :** Le cas échéant, les serveurs d'authentification utilisés pour authentifier les utilisateurs sont considérés comme sains et configurés correctement.
— **Services non évalués désactivés par défaut :** L'ensemble des services présents dans la ToE mais hors de la cible de sécurité sont désactivés dans la configuration par défaut (parfois appelée configuration usine).
— **Documentation de securité :** La ToE est fournie avec une documentation détaillée sur l'utilisation sécurisée de l'équipement. En particulier, l'ensemble des secrets de connexion présents par défaut est listé pour permettre leur personnalisation.
L'ensemble des préconisations issues de cette documentation ont été appliquées en vue de l'évaluation.

2 Description des biens sensibles à protéger

2.1 Biens sensibles de l'environnement

Les biens sensibles de l'environnement sont les suivants :
— **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	X		X	
Intégrité protocolaire	X		X	
X : obligatoire (X) : optionnel				

2.2 Biens sensibles de la ToE

Les biens sensibles de la ToE sont les suivants :
— **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 peut s'appuyer sur une base de données locale ou sur un connecteur avec un annuaire distant. Dans les deux cas, la ToE doit protéger l'intégrité et l'authenticité du mécanisme [2].
— **Secrets de connexion des utilisateurs :** Il peut s'agir de mots de passe, de certificats, etc. Ils peuvent être contenus dans la ToE ou être échangés avec un serveur distant. Dans tous les cas, la ToE doit garantir l'intégrité et la confidentialité de ces identifiants.

2. Tous les mécanismes d'authentification présents dans la ToE ne doivent pas nécessairement être présents dans la cible de sécurité. Néanmoins, il doit y en avoir au moins un et ceux qui ne sont pas inclus doivent être désactivés par défaut.

— **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.
— **Fonction de journalisation locale :** La ToE dispose d'une fonction de journalisation locale qui, une fois configurée, doit rester opérationnelle.
— **Fonction de journalisation distante :** La ToE dispose d'une fonction de journalisation distante qui, une fois configurée, doit rester opérationnelle.
— **Journaux d'évènements locaux :** Les journaux locaux générés par la ToE doivent être intègres.
— **Journaux d'évènements déportés :** Les journaux déportés émis par la ToE doivent être intègres et authentifiés. Un mécanisme doit également permettre au destinataire de détecter l'absence d'un message au sein d'une sequence de messages correctement reçus.

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

Bien	Disponibilité	Confidentialité	Intégrité	Authenticité
Firmware			X	X
Configuration		X	X	
Mécanisme d'authentification des utilisateurs			X	X
Secrets de connexion des utilisateurs		X	X	
Politique de gestion des droits			X	
Fonction de journalisation locale	X			
Fonction de journalisation distante	X			
Journaux d'évènements locaux			X	X
Journaux d'évènements déportés			X	X
X : obligatoire (X) : optionnel				

3 Description des menaces

3.1 Description des agents menaçants

Les agents menaçants suivants ont été 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.
— **Attaquant avec les droits d'administration :** L'attaquant a réussi à compromettre le compte d'un administrateur. Ce compte peut avoir n'importe quel rôle à l'exception du super-administrateur.

3.2 Menaces retenues

Les menaces suivantes ont été 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.
— **Corruption des journaux d'évènements locaux :** L'attaque parvient à supprimer ou modifier une entrée dans les journaux d'évènements locaux sans y avoir été autorisé par la politique de droits de la ToE.
— **Corruption des journaux d'évènements déportés :** L'attaquant parvient à modifier une entrée de journal distant émise par la ToE sans que le destinataire ne puisse s'en rendre compte. L'attaquant parvient à supprimer une émission de journalisation distante sans que le destinataire ne puisse s'en rendre compte.

4 Objectifs de sécurité

Les objectifs de sécurité retenus sont les suivants :
— **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. On peut distinguer deux types de filtrages :

Filtrage non contextuel : L'action de filtrage est effectuée uniquement en fonction du contenu du paquet. Ce filtrage peut être fait au niveau 2 (Ethernet) et au niveau 3 (IP) au niveau 4 (TCP ou UDP...) et sur certains protocoles de niveau applicatif. Cette fonction de sécurité est valable pour une ToE en redondance ou non.

Filtrage contextuel : Après une action de filtrage non-contextuel, l'équipement peut établir 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...) et au niveau applicatif (HTTP, FTP, SMTP, Profinet, Modbus, EtherNet/IP). Il convient à chaque utilisateur de vérifier que le filtrage des protocoles de son choix fait partie de la cible de sécurité de l'équipement choisi.
- **Connexion sécurisée avec le serveur d'authentification :** La ToE permet une connexion sécurisée avec le serveur d'authentification en assurant l'authenticité des deux extrémités, l'intégrité et la confidentialité des échanges, ainsi que le non-rejeu.
- **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. L'intégrité et l'authenticité sont également vérifiées au chargement du firmware lors du démarrage de l'équipement.
- **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.
- **Intégrité des journaux :** Les journaux d'événements générés par la ToE sont intégres et seul le super-adminstrateur peut les modifier.
- **Intégrité des journaux déportés :** La ToE permet de transmettre les journaux déportés à un équipement tiers de manière intègre, authentifiée, et sans rejeu des journaux générés avec détection des événements manquants.

A Couverture des biens par les menaces

	Matrice de flux	Intégrité protocolaire	Firmware	Configuration	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évènements locaux	Journaux d'évènements déportés
Déni de service	D I	D I						D	D		
Contournement de la politique de filtrage	I										
Violation de la conformité protocolaire		I									
Corruption du firmware			I A								
Corruption de la configuration				I							
Compromission de la configuration				C							
Vol d'identifiants						C I					
Contournement de l'authentification					I A						
Contournement de la politique de droits							I				
D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité											

	Matrice de flux	Intégrité protocolaire	Firmware	Configuration	Mécanisme d'authentification des utilisateurs	Secrets de connexion des utilisateurs	Politique de gestion des droits	Fonction de journalisation locale	Fonction de journalisation distante	Journaux d'évènements locaux	Journaux d'évènements déportés
Corruption des journaux d'évènements locaux										I A	
Corruption des journaux d'évènements déportés											I A
D : Disponibilité, I : Intégrité, C : Confidentialité, A : Authenticité											

B Couverture des menaces par les objectifs de sécurité

	Déni de service	Contournement de la politique de filtrage	Violation de la conformité protocolaire	Corruption du firmware	Corruption de la configuration	Compromission de la configuration	Vol d'identifiants	Contournement de l'authentification	Contournement de la politique de droits	Corruption des journaux d'évènements locaux	Corruption des journaux d'évènements déportés
Gestion des entrées malformées	X										
Application de la politique de filtrage		X									
Analyse de conformité protocolaire			X								
Connexion sécurisée avec le serveur d'authentification								X			
Stockage sécurisé des secrets							X				
Authentification sécurisée sur l'interface d'administration					X	X	X	X			
Politique de droits									X		
Signature du firmware				X							

	Déni de service	Contournement de la politique de filtrage	Violation de la conformité protocolaire	Corruption du firmware	Corruption de la configuration	Compromission de la configuration	Vol d'identifiants	Contournement de l'authentification	Contournement de la politique de droits	Corruption des journaux d'évènements locaux	Corruption des journaux d'évènements déportés
Intégrité et confidentialité de la configuration					X	X					
Intégrité des journaux										X	
Intégrité des journaux déportés											X

C Liste des contributeurs

Ce profil de protection a été rédigé dans le cadre des travaux du groupe de travail sur la cybersécurité des systèmes industriels (GTCSI) sous l'égide de l'ANSSI.

Les sociétés et organismes suivants ont apporté leur concours à la rédaction de ce document :

— Amossys
— ARC Informatique
— Belden
— DGA/MI
— Gimelec
— Oppida
— Phoenix Contact
— RATP
— Schneider Electric
— Siemens
— Sogeti
— Stormshield
— Thales