Stonesoft Corporation

StoneGate Firewall/VPN

Version 5.2.4 Build 8069

CIBLE DE SÉCURITÉ

VERSION 1.2

Stonesoft Corporation
Itälahdenkatu 22 A, FIN-0210 Helsinki, Finlande

SOMMAIRE

FIGURES

1 INTRODUCTION A LA CIBLE DE SECURITE

1.1 IDENTIFICATION DE LA CIBLE DE SECURITE

Identification de la cible d'évaluation : Stonesoft StoneGate Firewall/VPN version 5.2.4 Build 8069

Titre de la cible de sécurité : Stonesoft StoneGate Firewall/VPN version 5.2.4 Build 8069

Version de la cible de sécurité : 1.2

Mots-clés : pare-feu, filtre de trafic

1.2 APERÇU DE LA CIBLE DE SECURITE

Stonesoft StoneGate Firewall/VPN est une solution de pare-feu et de réseau privé virtuel (VPN) à haute disponibilité destinée à sécuriser les canaux de communication de données et permettre une connectivité continue des réseaux.

StoneGate Firewall/VPN s'appuie sur la technologie Multi-Layer Inspection, qui associe inspection dynamique des paquets et inspection au niveau application afin de contrôler la connectivité et le flux d'informations entre réseaux internes et externes. Cette solution permet également de maintenir privées les adresses IP des hôtes internes aux yeux des utilisateurs externes. Reposant sur la norme IPsec, les services de sécurité VPN offrent aux utilisateurs plusieurs possibilités de chiffrement. Lorsque StoneGate Firewall/VPN fait partie d'un cluster, il apporte une haute disponibilité aux services de sécurité de ces pare-feu pour les utilisateurs et les serveurs protégés par le cluster de pare-feu lorsqu'un nœud du cluster ou une connexion réseau vers un nœud est défaillante.

Le produit StoneGate Firewall/VPN fonctionne sur un système d'exploitation Linux renforcé, avec lequel il est livré. Il fonctionne sur plate-forme Intel mono- ou multi-processeur. Un système d'administration distribuée comprenant un serveur d'administration, un serveur de journalisation et une interface graphique pour la gestion et le fonctionnement du pare-feu est proposé en option.

Les fonctions de sécurité entrant dans le cadre de la cible de sécurité sont les suivantes :

- Contrôle du flux d'informations au niveau connexion des paquets IP, avec filtrage des paquets de la couche réseau à la couche application et redirection des connexions pour le trafic FTP, HTTP et SMTP ;
- Confidentialité des adresses IP des hôtes sur le réseau interne, assurée via NAT statique ;
- Génération d'audits ;
- Fonctions d'administration et de protection des services de sécurité

1.3 TERMINOLOGIE

Agent de protocole
Module qui assiste le moteur de pare-feu dans la gestion d'un protocole particulier. Les agents de protocole assurent que les connexions liées à un service sont correctement groupées et évaluées par le moteur de pare-feu, tout en assistant le moteur dans ses tâches de filtrage du contenu ou de traduction des adresses réseau.

Certificat électronique
Carte d'identité électronique d'un utilisateur ou d'un dispositif. Distribués ou accordés par des autorités de certification, les certificats numériques permettent à des utilisateurs ou à des dispositifs de s'authentifier, en assurant que l'utilisateur ou le dispositif est bien celui qu'il prétend être. Les détenteurs de certificats numériques disposent d'une paire de clés publique et privée, avec lesquelles ils peuvent s'authentifier, signer des messages (pour authentifier l'expéditeur) et déchiffrer les messages entrants (garantissant que seul le détenteur du certificat peut décoder le message chiffré).

Chemin
Ensemble de routeurs ou de passerelles par lesquel(le)s passe un paquet pour atteindre sa destination. Sur les réseaux TCP/IP, les différents paquets d'une même connexion peuvent passer par des chemins différents pour atteindre l'hôte de destination.

Cluster de pare-feu
Groupe de pare-feu qui, grâce à la technologie de clustering, effectue le travail habituellement réalisé par un pare-feu unique.

Filtrage des paquets
Méthode de contrôle d'accès à un réseau ou à un ensemble de réseaux par l'examen des informations d'adresses source et de destination des paquets et par l'autorisation de passage ou le blocage de ces paquets selon des règles définies.

Haute disponibilité
Mise en œuvre des technologies de clustering, de secours automatique ou de redondance générale sur un système en vue d'accroître la disponibilité d'une application, d'un service ou d'un réseau au-delà de ce qu'un système individuel est capable de fournir. L'élimination de tous les points de défaillance uniques permet d'obtenir une disponibilité accrue, la technologie de clustering apportant un niveau de disponibilité maximal.

IPsec (IP Security)
Ensemble de protocoles prenant en charge l'échange sécurisé des paquets. Utilisé pour la mise en œuvre des VPN, il fournit des modes de chiffrement de transport et de tunnel. La norme IPsec est définie dans le document RFC 2401.

Moteur de pare-feu
Applications ou processus qui fonctionnent sur un pare-feu procédant à l'examen et au contrôle d'accès des données.

Multi-Layer Inspection (inspection multi-couche)
Technologie hybride de pare-feu qui inclut les meilleurs éléments des pare-feu de niveau application et réseau, complétée par une technologie supplémentaire permettant la gestion sécurisée de nombreux types de connexion.

NAT (Network Address Translation, traduction d'adresses réseau)
Mécanisme d'attribution aux réseaux locaux d'un jeu d'adresses IP pour le trafic interne et d'un autre pour le trafic externe. À l'origine, NAT a été décrit dans la RFC 1631 comme un moyen de

résoudre la pénurie croissante d'adresses IP (espace d'adressage). Il a par ailleurs un rôle de sécurité : il masque les adresses IP internes.

Nœud de pare-feu
Dispositif unique, souvent un routeur ou un PC spécialisé, qui exécute un logiciel de pare-feu et remplit les fonctions de pare-feu dans le cadre d'un cluster de pare-feu.

Paquet
Unité de données envoyée sur un réseau.

Pare-feu
Barrière ou point de passage obligé entre deux réseaux ou plus, le pare-feu examine, contrôle et/ou bloque le flux de données entre ces réseaux. Souvent considérés comme un moyen de défense entre un réseau d'entreprise et Internet, les pare-feu peuvent également protéger les réseaux internes les uns des autres.

Passerelle de sécurité (SGW)
Dispositif sécurisé distant compatible IPsec et capable d'établir un VPN avec la cible d'évaluation (TOE).

Politique de sécurité d'un pare-feu
Base de règles qui définit les politiques mises en œuvre par le pare-feu pour sécuriser le réseau et les ressources des ordinateurs.

Protocole
Format convenu pour transmettre des données entre deux dispositifs ou plus. Les protocoles déterminent généralement comment vérifier l'absence d'erreurs, comment l'expéditeur annonce que l'envoi des données est terminé, comment le récepteur accuse réception des données et comment les données seront compressées, le cas échéant.

Réseau privé virtuel (VPN)
Ensemble de dispositifs connectés à un ou plusieurs réseaux publics et dont les communications sont chiffrées. Concrètement, ces dispositifs créent un tunnel sur le(s) réseau(x) public(s) pour y faire circuler l'information comme si elles étaient reliées par des lignes privées.

Suivi des connexions
Jeu de données relatif à une connexion. Il permet de relier les paquets entrants aux connexions existantes. Le suivi des connexions comprend également les informations pour gérer des fonctions comme le NAT, le routage avec répartition de charge et les agents de protocole. Ce jeu de données peut également contenir des informations comptables.

Système de pare-feu
Ensemble des applications utilisées pour mettre en œuvre les politiques de sécurité et surveiller le trafic réseau sur un ou plusieurs sites. Un système de pare-feu se compose de moteurs de pare-feu, de serveurs d'administration, de serveurs de journalisation et d'interfaces graphiques.

Technologie de clustering
Ensemble de méthodes et d'algorithmes employés pour mettre en œuvre des solutions extrêmement évolutives dans lesquelles la charge de travail est répartie entre plusieurs machines. Avantages de cette technologie : amélioration des performances, disponibilité et fiabilité.

2 DESCRIPTION DE LA CIBLE D'ÉVALUATION

2.1 TYPE DE PRODUIT

Le pare-feu StoneGate est un produit de pare-feu et VPN à haute disponibilité destiné à sécuriser les communications de données et à permettre une connectivité continue des réseaux. Les services de pare-feu incluent le filtrage dynamique des paquets et un contrôle du flux d'informations au niveau application. Le pare-feu StoneGate s'adresse aux entreprises ayant besoin d'un accès aux services contrôlé, protégé et audité, à l'intérieur comme à l'extérieur du réseau de l'entreprise, par le chiffrement, l'autorisation ou le refus d'accès et/ou la redirection du flux de données à travers le pare-feu.

StoneGate Firewall/VPN est le composant (ou nœud) pare-feu du produit StoneGate. Il intègre un moteur de pare-feu, un système d'exploitation et une plate-forme de référentiel de données, des modules de chiffrement et les logiciels de son système d'administration. Le moteur de pare-feu entre dans le périmètre de la cible d'évaluation, contrairement au module de chiffrement SafeNet QuickSec, et aux plates-formes d'exploitation. Le système d'administration (StoneGate Management Center) fait également partie de la TOE. Pour assister les opérations du moteur de pare-feu, le système d'administration fourni séparément comprend un serveur d'administration qui apporte une interface sécurisée pour les fonctions d'administrateur, un serveur de journalisation pour stocker et gérer les enregistrements des journaux (c'est-à-dire les filtrer, les trier et les archiver), ainsi qu'une interface utilisateur graphique permettant un accès convivial pour les administrateurs. Son architecture distribuée le rend souple et évolutif en lui permettant de s'exécuter sur une ou plusieurs plates-formes matérielles, sous Windows 2003, Windows XP, Red Hat Enterprise Linux (4.0 ou 5.0) ou Fedora Core (6 ou 7). Les communications entre le serveur d'administration (Management Server) ou le serveur de journalisation (Log Server), d'une part, et le pare-feu d'autre part, sont protégées par un canal de confiance fournissant des services de confidentialité, d'intégrité, et d'authentification mutuelle des extrémités.

Le moteur de pare-feu utilise un système d'exploitation Linux renforcé, basé sur Debian GNU/Linux, dont tous les packages non essentiels ont été retirés.

StoneGate Firewall/VPN peut fonctionner comme un pare-feu autonome ou au sein d'un cluster de 2 à 16 nœuds de pare-feu. Le cluster de pare-feu est nécessaire pour assurer une haute disponibilité des services de sécurité. Chaque nœud comporte des connexions réseau internes et externes auxquelles il fournit ses services de sécurité, et peut éventuellement disposer de réseaux d'administration distincts destinés à la connectivité vers le système d'administration et les autres nœuds d'un cluster, c'est-à-dire vers le réseau d'administration et vers le réseau du cluster, respectivement. Voir Figure 2.1 ci-dessous.

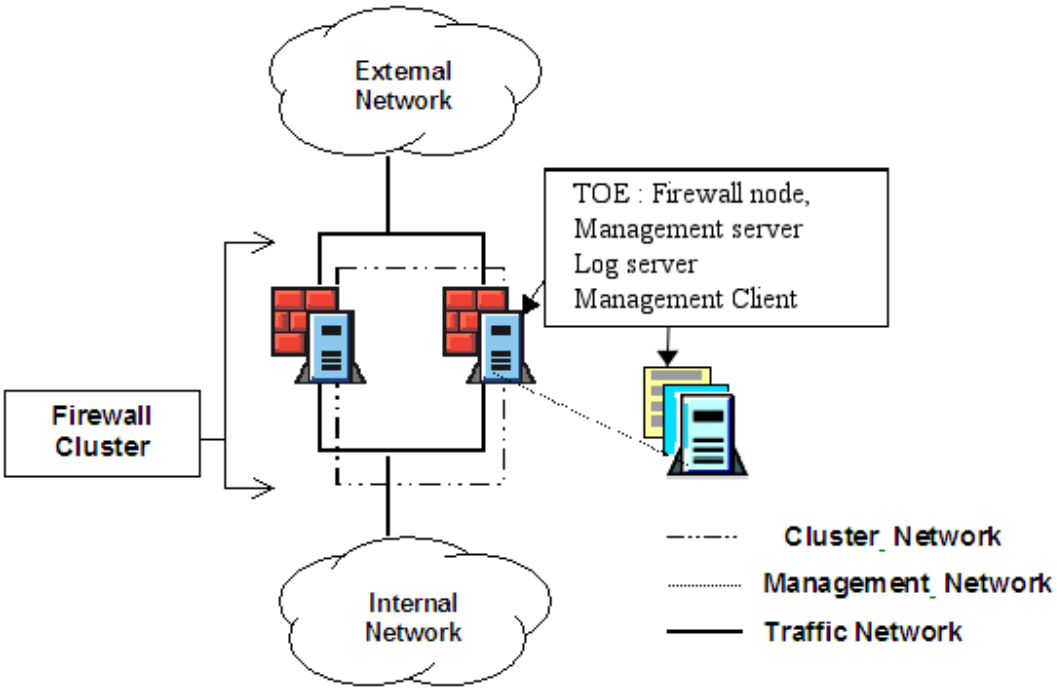

Figure 2.1 Environnement d'exploitation de la cible d'évaluation

Les modèles StoneGate suivants font partie du périmètre d'évaluation :

- FW-310 et FW-315 (desktop)
- FW-105 (desktop)
- FW-1030 (rack)
- FW-1060 (rack ; même matériel que le FW-1030, dont le débit est limité par la licence)
- FW-1301 (rack)
- FW-3200 (rack)
- FW-5200 (rack)

2.2 FONCTIONS DE SÉCURITÉ DE LA CIBLE D'EVALUATION

La cible d'évaluation (TOE) comprend le moteur StoneGate et le SMC. Elle offre les services de sécurité suivants :

Contrôle du flux d'informations sur le trafic qui traverse le pare-feu. Ce dernier contrôle le flux de toutes les informations qui transitent par ses connexions réseau internes et externes pour mettre en œuvre la politique de sécurité du pare-feu à l'aide des éléments suivants :

- Des règles d'accès fondées sur les adresses source et de destination, ainsi que sur le protocole de la couche transport, celui de la couche application, le port source, le port de destination et l'interface sur laquelle le paquet arrive ; le suivi des connexions ; les résultats de l'authentification utilisateur et la durée de validité.
- Des règles de couplage VPN permettant de décider d'accepter ou de rejeter des connexions chiffrées et non chiffrées.

- Des agents de protocole apportant des règles supplémentaires basées sur des mécanismes et des informations au niveau application pour la redirection des connexions. Alors que le moteur de pare-feu prend en charge de nombreux agents de protocole, l'évaluation se limite quant à elle aux agents des protocoles FTP, HTTP et SMTP.

Description détaillée :

Le pare feu/VPN StoneGate fournit un mécanisme de contrôle du flux d'informations grâce à une base de règles qui renferme plusieurs politiques de sécurité, à savoir, les politiques de sécurité du firewall. Le TSF applique toute politique de sécurité du firewall au trafic qui transite via ses interfaces réseau internes et externes.
Le trafic est TCP, UDP et ICMP sur IP. la fonctionnalité de contrôle du flux d'information permet uniquement de passer en fonction de ce qu'autorisent les politiques de sécurité du firewall et mène à bien la défragmentation des paquets afin d'appliquer la politique à l'ensemble des paquets IP. Les administrateurs autorisés qui utilisent le serveur d'administration définissent les politiques de sécurité du firewall.

Le contrôle du flux d'information applique le suivi des connexions pour gérer les décisions de contrôle du flux d'information sur les connexions plutôt que les paquets, permettant ainsi d'améliorer les performances et de supporter les fonctionnalités firewall qui nécessitent des informations sur les paquets au dessus du niveau IP. Le système de suivi des connexions stockent les informations concernant chaque connexion afin de permettre aux paquets liés à une connexion établie de transiter.

Le suivi des connexions fonctionne de concert avec les agents de protocole pour gérer les décisions liées au contrôle du flux d'information en fonction des caractéristiques des informations des différentes couches réseau à travers la couche applicative afin de décider si un paquet doit être autorisé ou non. Les agents de protocole suivants et leurs fonctions de sécurité font partie du champ de l'évaluation : FTP, HTTP, et redirection SMTP.
Le contrôle du flux d'information suit un algorithme spécifique afin de traverser la base de règles, de trouver une correspondance et de filtrer le trafic entre les réseaux externes et internes. Tout trafic n'étant pas explicitement accepté dans les politiques de sécurité sera rejeté par le firewall. La structure de la base de règles et les capacités des agents de protocole associés permet à la fonctionnalité de prendre les décisions de contrôle des flux d'informations sur la base de l'action définie dans chaque règle ('allow' / 'reject') et de la redirection éventuelle vers un proxy FTP, HTTP ou SMTP.

Chaque règle intègre un critère correspondant et des actions cibles. Si le critère correspondant est vérifié (c'est-à-dire si une comparaison correspond), le contrôle du flux d'information applique alors les actions ciblées. Le contrôle du flux d'information compare les caractéristiques des paquets au niveau MAC, réseau et transport (interface, adresse source et destination, port TCP /UDP source et destination, etc.) avec le critère correspondant à la règle afin de déterminer si la règle doit être appliquée ou non. Si elles sont appliquées les actions ciblées sont mises en place et les fonctionnalités supplémentaires et les règles de contrôles des flux sont appliquées.

La base de règles est lue de haut en bas et lorsqu'une règle correspondante est trouvée la recherche s'interrompt et la TOE lance la règle correspondante. Il existe deux exceptions à cela :

a) saut de règle : ceci permet de lancer la recherche dans une sous base de règles dans le cas où le saut de règle correspond. La recherche continuera dans la sous base de règle jusqu'à ce qu'une règle correspondante soit trouvée ou non. Si la recherche n'aboutit pas, elle reprendra dans la base de règles principale.
b) continuation de la règle : si une correspondance est trouvée, des variables sont mises en place et la recherche continue.

- **Translation d'adresses réseau (NAT)** entre des entités informatiques externes qui font transiter du trafic par la TOE, assurant que l'adresse IP des hôtes sur les réseaux internes est maintenue privée aux yeux des utilisateurs externes.

Description détaillée :

Lorsque le pare-feu est configuré pour du mapping NAT statique, la TOE fournit un mécanisme qui s'assure que les adresses réelles sur les réseaux internes ne soient pas visibles. Le mapping statique est un mapping un-pour-un et permet de déterminer le numéro choisi de l'adresse IP.

Le NAT est activé pour chaque connexion individuelle en fonction de la base de règles. Le pare-feu réécrit les en-têtes des paquets IP. C'est un processus biunivoque qui garde une trace des adresses d'origine et de destination et réalise la traduction inverse des paquets en retour.

La manipulation effectuée par le NAT a lieu après l'acceptation d'une connexion afin que les décisions liées aux connexions soient fondées sur les adresses d'origine. Le routage a lieu après la modification de la connexion. Les règles NAT peuvent être définies séparément des règles d'accès.

- **Journalisation et audit** : La TOE permet de générer des enregistrements d'audit des événements de sécurité relatifs au trafic IP transitant par le pare-feu et des enregistrements d'audit des modifications de la politique de sécurité du pare-feu. La TOE permet également à l'administrateur autorisé de définir les critères de sélection des événements du trafic IP à auditer. La TOE comporte un mécanisme empêchant la perte des données d'audit.

Description détaillée :

Fonctions de journalisation : La TOE fournit un mécanisme d'audit qui ne peut être désactivé. Démarrer et arrêter la fonction d'audit signifie démarrer et arrêter le pare-feu.
Le mécanisme d'audit est l'opération de journalisation qui est déclenchée via l'utilisation de l'option 'logging' d'une règle dans la politique de sécurité du firewall. La TOE applique le mécanisme de correspondance pour filtrer les paquets (contrôle de flux d'information) et pour chaque correspondance, on peut définir une option de journalisation qui génèrera une donnée d'audit.
En plus de l'opération de journalisation, la TOE permet de générer des données d'audit lorsque que la politique de sécurité du firewall (par exemple : les dossiers actifs) change. Lorsque la TOE reçoit une nouvelle politique de sécurité firewall, elle génère une donnée d'audit où sont consignés la date, l'heure et le type de configuration.
Le pare-feu se base sur le système d'exploitation qui lui fournit la date et l'heure pour la génération des données d'audit et pour que le serveur d'administration génère des données d'audit détaillées sur l'utilisation des fonctionnalités d'administration de la sécurité.

Fonctions de protection des données d'audit : La TOE fournit des mécanismes de prévention contre la perte des données d'audit. Les enregistrements d'audit de la TOE sont d'abord stockés dans le cache des buffers au niveau de chaque nœud. La taille du cache dépend de la taille du disque dur. Le protocole propriétaire de synchronisation et de gestion des données à travers les composants distribués avertit le Log Server de toute nouvelle information de log et envoie l'enregistrement de log vers le Log Server.

Les informations de log sont alors stockées par le Log Server dans des fichiers de la base de données et ne sont accessibles qu'à un administrateur autorisé du firewall via le Management Server. Chaque enregistrement d'audit est retiré du cache du buffer après que la TOE ait reçu une confirmation que l'enregistrement a bien été sauvegardé au niveau du serveur de log.

L'administrateur définit la politique de stockage des logs. Ceci permet de spécifier le comportement du TOE lorsqu'un stockage local de log est rempli d'une des façons suivantes :

- Arrêt du trafic (obligatoire dans la configuration évaluée) : la TOE se met automatiquement hors ligne et les connexions transitant via la TOE sont redirigées vers d'autres nœuds dans un cluster (cf. les informations concernant la haute-disponibilité). Une fois que le problème de remplissage du stockage local a été résolu, le nœud se remet automatiquement en ligne.

- Ignorer log : (la configuration par défaut a besoin d'être modifiée pour la configuration évaluée) le cluster ignore tout nouvel enregistrement de log sans qu'on puisse le récupérer. Cette politique de stockage de log ne doit être utilisée que si la préservation du trafic est plus importante que celles des logs.

La TOE permet également au Management Server d'affecter des priorités aux données de logs. Ce mécanisme se base sur les niveaux de log suivant :

- Alerte : générées via un statut d'alerte, elles sont toujours stockées
- Essentiel : systématiquement générée même si le moteur firewall n'a plus d'espace disque
- Sauvegardé: stockée dans la base de données de logs si les données de logs 'alerte' et 'essentielles' ont déjà été sauvegardées
- Transitoire: non stockée dans la base de données mais conservée dans le cache des logs du firewall

Avant d'appliquer la politique de stockage des logs choisie, le moteur cesse de produire les logs 'transitoires'. En cas d'insuffisance, il peut abandonner l'ensemble des enregistrements de logs, sauf les 'Essentiels'. En dernier recours, le moteur applique la politique de stockage des logs choisie

Contrôle d'accès aux fonctions d'audit et protection des communications entre le pare-feu et le Log Server.

L'administrateur en charge de l'audit de sécurité utilise le Management Client qui contacter le Log Server. Le Log Server s'appuie sur le Management Server pour déterminer si l'administrateur est bien autorisé à consulter les logs.

Le pare-feu remonte les informations d'audit au Log Server (cf. « Fonctions de protection des données d'audit », ci-dessus). Les communications entre le pare-feu et le Log Server sont protégées par l'établissement d'une session SSL en mode « full hand-shake », dont les caractéristiques sont identiques à celles établies entre le pare-feu et le Management Server (cf. « Administration de la sécurité et protection des fonctions de sécurité » ci-dessous).

- **Administration de la sécurité et protection des fonctions de sécurité :** Les administrateurs accèdent au moteur de pare-feu via le serveur d'administration, lequel fournit l'interface permettant de gérer la politique de sécurité et les attributs d'authentification, les données TSF et les fonctions de sécurité du moteur de pare-feu. Le moteur de pare-feu assure également que les fonctions de sécurité de confiance sont toujours appelées et ne peuvent pas être contournées.

Description détaillée :

L'administration de la sécurité comprend les mécanismes de protection et d'administration de la TOE. L'interface d'administration de la TOE se fait via le Management Client. Cette interface fournit la fonctionnalité nécessaire aux administrateurs pour gérer les données de confiance et les attributs de sécurité pour les fonctionnalités de sécurité. Le Management Server est en charge de l'authentification des administrateurs. Les opérations d'administration sont contrôlées par le Management Server, qui gère une base associant à chaque administrateur son mot de passe et les opérations qu'il a le droit d'effectuer sur chaque pare-feu géré (créer des objets, rafraîchir les politiques, envoyer des commandes, pousser des politiques, consulter les logs).

Du point de vue du pare-feu, seul le Management Server a le droit de modifier les règles de filtrage. À cet effet, le Management Server se connecte au pare-feu en établissant une session SSL en mode « full hand-shake ». Les algorithmes utilisés sont les suivants :

- Authentification mutuelle : RSA 2048 bits
- Chiffrement : Triple DES en mode CBC 168 bits
- Authentification du contenu : HMAC-SHA-1

Le pare-feu met en œuvre un contrôle de cohérence de données de confiance reçues par l'interface du Management Server. Ceci permet d'assurer que seules les valeurs cohérentes sont acceptées.

Le pare-feu applique des valeurs restrictives par défaut aux caractéristiques de sécurité du flux d'informations. Tout trafic qui n'est pas explicitement accepté par la politique de sécurité sera rejeté par le firewall. Un administrateur autorisé doit s'identifier sur le Management Server afin de modifier la configuration qui autorise le flux d'information.

2.3 PERIMETRE DE LA CIBLE D'EVALUATION ET CONFIGURATION EVALUEE

Comme le montre la Figure 2.2 ci-dessous, le périmètre de la TOE est le suivant :

- Application logicielle Firewall/VPN Engine, version 5.2.4 build 8069.

La configuration évaluée de la TOE est la suivante :

- Plate-forme matérielle firewall constituée de deux modèles FW-1301 en mode cluster. Cette plate-forme illustre l'utilisation de la haute disponibilité (qui ne constitue pas une fonction de sécurité) et est suffisamment significative de la gamme identifiée au §2.1. Les différences entre le modèle FW-1301 et les autres modèles listés au §2.1 portent essentiellement sur les performances en termes de débit et sur la taille des disques durs.
- Activation du suivi des connexions ;
- Politique de stockage des journaux paramétrée sur "stop traffic" ;
- Désactivation de l'accès à l'interface en ligne de commande du moteur de pare-feu à partir du système d'exploitation, comme indiqué dans la documentation d'installation ;
- Désactivation des fonctionnalités VPN.
- Pas d'utilisation dans les règles de filtrage de l'option d'authentification des utilisateurs auprès du firewall (nécessite d'utiliser des VPN ou une authentification par telnet).
- StoneGate Management Center et logiciel de support, version 4.2 :
  - Le serveur d'administration,
  - Le serveur de journalisation,
  - L'interface graphique ;
- Activation possible des agents de suivi des connexions FTP, SMTP et HTTP
- Désactivation des agents ou composants IPS associés à tous les autres protocoles : H.323, HTTPS, IMAP4, MS RPC, NetBios Datagram, Oracle SQL Net, POP3, RSH,SIP, SSH, SunRPC, TCP Proxy, TFTP.

L'environnement informatique de la configuration évaluée est le suivant :

- Plate-forme d'exploitation de la TOE :
  - Intel Pentium 4 ou supérieur (ou équivalent) recommandé,
  - 1 Go de RAM recommandé,

- Noyau Linux 2.6.17.13 standard avec quelques modifications mineures, distribution basée sur Debian GNU/Linux 4.0 (Etch),
- Cartes réseau (voir Annexe A) ;

- Architecture et système :
  - Au moins 2 interfaces réseau,
  - 1 interface réseau de cluster,
  - 1 interface réseau d'administration,

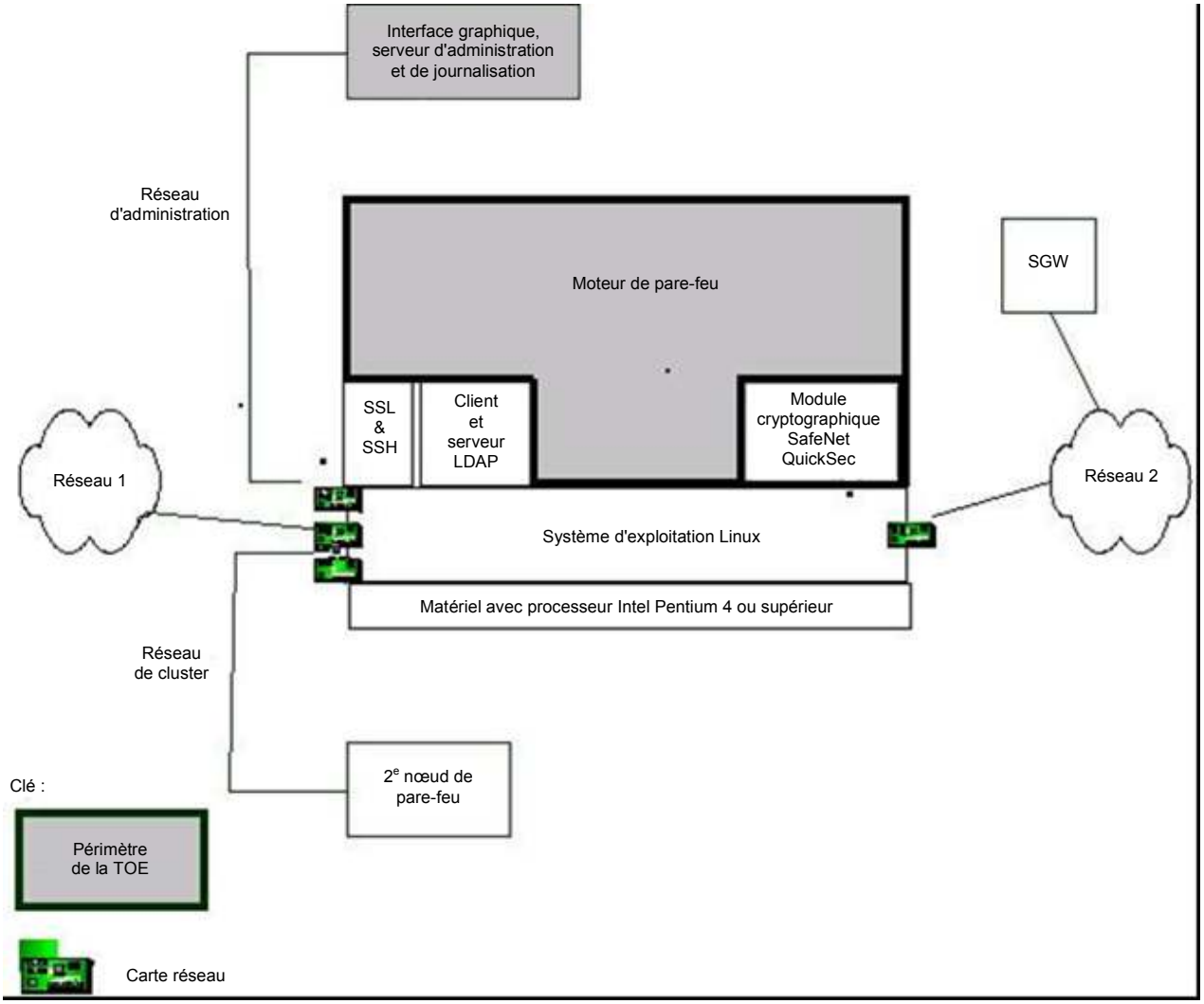

Figure 2.2 Périmètre et environnement informatique de la TOE

3 ENVIRONNEMENT DE SECURITE DE LA TOE

Cette section identifie les éléments suivants :

- Hypothèses d'utilisation sécurisée ;
- Politiques de sécurité organisationnelles ;
- Menaces sur la sécurité.

3.1 HYPOTHÈSES D'UTILISATION SÉCURISÉE

A.ADMINTRUSTED : Attributions de l'administrateur
Les administrateurs autorisés sont formés, qualifiés, non hostiles et respectent toutes les directives.

Note d'application : Si un revendeur à valeur ajoutée installe la TOE, l'utilisateur doit établir que A.ADMINTRUSTED s'applique à ce revendeur. L'utilisateur peut également réinstaller la TOE et vérifier son intégrité à l'aide des sommes de contrôle fournies sur le site Web de Stonesoft, www.stonesoft.com.

A.AUDITMAN : Procédures d'audit de l'environnement
Ces procédures doivent exister pour assurer que les pistes d'audit sont régulièrement analysées et archivées.

A.MEDIAT_SUPPORT : Prise en charge du contrôle du flux d'informations assurée par l'environnement informatique
L'environnement informatique de la TOE doit garantir que le flux d'informations ne peut pas atteindre les réseaux interne et externe sans passer par la TOE, et assurer une protection de l'information résiduelle pour ces paquets. Il doit également permettre un stockage sécurisé de la politique de sécurité du réseau et des données d'authentification des utilisateurs, ainsi qu'un accès à ces données, et s'appuyer sur la source de signaux horaires sécurisée (cf. A.TIME) pour la prise en charge des décisions concernant le contrôle temporel des flux d'informations.

A.OPERATING_ENVIRONMENT : Prise en charge générale de l'environnement informatique
Le nœud sur lequel s'exécute la TOE, ainsi que les serveurs d'administration associés, sont dédiés au système de pare-feu sécurisé. Ils fonctionnent selon leurs spécifications et sont sécurisés physiquement, accessibles physiquement aux seuls administrateurs de confiance.

A.TIME : Source de signaux horaires sécurisée
L'environnement informatique intégrera une source de signaux horaires sécurisée permettant la datation des enregistrements d'audit.

3.2 MENACES SUR LA SÉCURITÉ

3.2.1 Identification des biens sensibles

Les agents menaçants sont soit des personnes non autorisées, soit des entités informatiques externes non autorisées à utiliser la TOE. Les actifs principaux à protéger sont l'information et les ressources informatiques du réseau à protéger. Pour pouvoir appliquer correctement ses fonctions de sécurité, la TOE a également besoin de protéger les actifs secondaires suivants :

- Enregistrements d'audit
- Adresses IP du réseau interne à protéger en confidentialité
- Accès aux fonctions d'administration
- Données de sécurité critiques de la TOE

3.2.2 Menaces

T.AUDIT_UNDETECTED : Événements d'audit non détectés
Un agent menaçant peut tenter de compromettre les ressources sans être détecté. Cette menace se traduit notamment par les actions d'un agent menaçant provoquant la perte d'enregistrements d'audit ou visant à épuiser la capacité de stockage pour empêcher de futurs enregistrements, afin de masquer les actions d'un attaquant.

T.MEDIAT : Contrôle du flux d'informations
Une personne non autorisée peut envoyer des informations interdites via la TOE, donnant lieu à l'exploitation et/ou la compromission des ressources informatiques. Cette menace inclut des tentatives de contournement de la politique de contrôle du flux d'informations par une personne non autorisée envoyant un paquet IP avec une fausse adresse source.

T.SELPRO : Autoprotection
Une personne non autorisée peut accéder aux fonctions d'administration de la TOE et lire, modifier, voire détruire des données de sécurité critiques de la TOE.

4 OBJECTIFS DE SÉCURITÉ

4.1 OBJECTIFS DE SECURITE POUR LA CIBLE D'EVALUATION

O.AUDIT : Détection et enregistrement des événements d'audit et protection de la remontée des journaux d'audit
La TOE doit fournir un moyen de correctement détecter et enregistrer les événements en rapport avec la sécurité dans les enregistrements d'audit et empêcher la perte des données d'audit en établissant des priorités pour les événements en rapport avec la sécurité et en les protégeant lorsque la capacité de stockage s'amenuise. Lors des sessions de remontée des données d'audit entre le pare-feu et le Log Server, la TOE doit garantir l'authentification mutuelle des participants à la session, et protéger les données échangées contre la divulgation, la modification et le rejeu non autorisés. Le Log Server permettra un stockage permanent protégé des pistes d'audit générées par la pare-feu, et s'appuiera sur la source de signaux horaires sécurisée (cf. O.E.TIME) pour la datation des enregistrements d'audit.

O.MEDIAT : Contrôle du flux d'informations
La TOE doit contrôler le flux de toutes les informations transitant entre les utilisateurs et les entités informatiques externes, y compris les passerelles sécurisées, sur les réseaux internes et externes reliés à la TOE, conformément avec sa politique de sécurité.

O.NETADDRHIDE : Masquage des adresses réseau internes
La TOE doit fournir un moyen de masquer les adresses IP des hôtes de son réseau interne.

O.SECFUN : Fonctions d'administration
La TOE doit fournir aux administrateurs un moyen d'administrer les fonctions de sécurité de la TOE via le Management Server. Elle doit obliger les administrateurs à s'authentifier avant qu'ils puissent effectuer toute action d'administration (modifier les règles de filtrage, lire ou purger les journaux d'audit, etc.). Elle doit restreindre les actions effectuables par chaque administrateur à celles qui lui sont autorisées. Lors de la modification des règles de filtrage du pare-feu par le Management Server, la TOE doit garantir l'authentification mutuelle des participants à la session, et protéger les données échangées contre la divulgation, la modification et le rejeu non autorisés.

4.2 OBJECTIFS DE SECURITE POUR L'ENVIRONNEMENT

Les objectifs de sécurité pour l'environnement sont les suivants :

O.E.ADMINTRUSTED : Attributions de l'administrateur
Les administrateurs autorisés sont formés, qualifiés, non hostiles et respectent toutes les directives.

O.E.AUDITMAN : Procédures d'audit de l'environnement
Ces procédures doivent exister pour assurer que les pistes d'audit sont régulièrement analysées et archivées.

O.E.MEDIAT_SUPPORT : Prise en charge du contrôle du flux d'informations assurée par l'environnement informatique
L'environnement informatique de la TOE doit garantir que le flux d'informations ne peut pas atteindre les réseaux interne et externe sans passer par la TOE, et assurer une protection de l'information résiduelle pour ces paquets. Il doit également permettre un stockage sécurisé de la politique de sécurité du réseau et des données d'authentification des utilisateurs, ainsi qu'un accès à ces données, et s'appuyer sur la source de signaux horaires sécurisée (cf. O.E.TIME) pour la prise en charge des décisions concernant le contrôle temporel des flux d'informations.

O.E.OPERATING_ENVIRONMENT : Prise en charge générale de l'environnement informatique
Le nœud sur lequel s'exécute la TOE, ainsi que les serveurs d'administration associés, sont dédiés au système de pare-feu sécurisé. Ils fonctionnent selon leurs spécifications et sont sécurisés physiquement, accessibles physiquement aux seuls administrateurs de confiance.

O.E.TIME : Source de signaux horaires sécurisée
L'environnement informatique intégrera une source de signaux horaires sécurisée permettant la datation des enregistrements d'audit.

4.3 TRAÇABILITE ENTRE LES ELEMENTS

4.3.1 Lien entre les fonctions de sécurité et les objectifs de sécurité

Fonction	Objectifs de sécurité
Contrôle du flux d'informations	O.MEDIAT
Translation d'adresses réseau	O.NETADDRHIDE
Journalisation et audit	O.AUDIT
Administration de la sécurité et protection des fonctions de sécurité	O.SECFUN

4.3.2 Lien entre les objectifs de sécurité et les menaces

Menace	Objectifs de sécurité
T.MEDIAT	O.MEDIAT, O.NETADDRHIDE, O.E.MEDIAT_SUPPORT, O.E.TIME
T.AUDIT_UNDETECTED	O.AUDIT, O.SECFUN, O.E.AUDITMAN, O.E.TIME
T.SELPRO	O.SECFUN

Les objectifs de sécurité sur l'environnement O.E.ADMINTRUSTED et O.E.OPERATING_ENVIRONMENT soutiennent l'ensemble des autres objectifs de sécurité pour contrer les menaces.

4.3.3 Lien entre les fonctions de sécurité et les menaces

Les deux tables ci-dessus montrent, par transitivité, la manière dont les fonctions de sécurité contrent les menaces.

4.3.4 Lien entre les fonctions de sécurité et les modes prévus d'utilisation du produit

Les modes d'utilisation prévus du produit sont décrits par les objectifs de sécurité. La table du §4.3.1 montre la manière dont les fonctions de sécurité sont reliées aux modes d'utilisation du produit. La table du §4.3.2 montre, à travers le soutien qu'apportent les objectifs de sécurité sur l'environnement pour contrer les menaces, les dépendances des fonctions de sécurité envers d'autres fonctions dédiées à la sécurité et d'autres mesures ne relevant pas de la sécurité des TI, supposées fournies par l'environnement.

5 ACRONYMES

3DES	Triple DES (Data Encryption Standard, norme de chiffrement des données)
AES	Advanced Encryption Standard (norme de chiffrement avancé)
CA	Certificate Authorities (autorités de certification)
CBC	Cipher Block Chaining (chaînage de chiffrement de blocs)
CC	Critères communs pour l'évaluation de la sécurité des technologies de l'information
CM	Configuration Management (administration de la configuration)
CVI	Cluster Virtual Interface (interface virtuelle de cluster)
EAL	Evaluation Assurance Level (niveau d'assurance de l'évaluation)
ESP	Encapsulating Security Payload (charge d'encapsulement de la sécurité)
FIPS	Federal Information Processing Standard (norme américaine de traitement de l'information)
FTP	File Transfer Protocol
GUI	Graphical User Interface (interface utilisateur graphique)
GNU	GNU's Not Unix (acronyme récursif)
HMAC	Hash Message Authentication Code (code d'authentification d'une empreinte cryptographique de message)
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation (traduction d'adresses réseau)
NIAP	National Information Assurance Partnership
NIC	Network Interface Card (carte réseau)
NDI	Node Detected Interface
PFS	Perfect Forward Secrecy
PKCS	Public Key Cryptography Standards (normes de cryptographie à clé publique)
RFC	Request For Comments
RSA	Rivest, Shamir et Adleman (algorithme de cryptographie asymétrique)
SF	Security Function (Fonction de sécurité)
SHA	Secure Hashing Algorithm, algorithme de hachage sécurisé

SFP	Security Function Policy
SGW	Security Gateway (Passerelle de sécurité)
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell, protocole de communication sécurisé
SSL	Secure Socket Layer, protocole de chiffrement
ST	Security Target (cible de sécurité)
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation (cible d'évaluation)
TSC	TSF Scope of Control (périmètre de contrôle des fonctions de sécurité de la cible d'évaluation)
TSF	TOE Security Functions (fonctions de sécurité de la cible d'évaluation)
TSP	TOE Security Policy (politique de sécurité de la cible d'évaluation)
UDP	User Datagram Protocol
VAR	Value-Added Reseller (revendeur à valeur ajoutée)
VPN	Virtual Private Network (réseau privé virtuel)
VPNC	VPN Consortium

6 RÉFÉRENCES

Documentation Stonesoft

Guide de l'administrateur :	Version 4.2 du guide d'administrateur StoneGate de Stonesoft
Guide de référence :	Version 4.2 du guide de référence StoneGate de Stonesoft
Guide d'installation :	Version 4.2 du guide d'installation StoneGate de Stonesoft

Normes

Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau. ANSSI. Édition 1, 30 mai 2011. Réf nº 1417/ANSSI/SR.

Internet Engineering Task Force, *File Transfer Protocol,* RFC 959, octobre 1985.

Internet Engineering Task Force, *Simple Mail Transfer Protocol,* RFC 959, août 1982.

Internet Engineering Task Force, *Hypertext Transfer Protocol,* RFC 2616, juin 1999.