PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2011/14

Fonctionnalités de pare-feu de StoneGate Firewall/VPN 5.2.4 build 8069

Paris, le 19 décembre 2011

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

Patrick Pailloux
[ORIGINAL SIGNÉ]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2011/14**
Nom du produit **StoneGate Firewall/VPN**
Référence/version du produit **5.2.4 build 8069**
Catégorie de produit **Firewall**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur(s) **STONESOFT France** **38, Rue de Villiers** **92300 Levallois** **France**
Commanditaire **STONESOFT France** **38, Rue de Villiers** **92300 Levallois** **France**
Centre d'évaluation **Silicomp-AQL** **4, rue de la Châtaigneraie CS 51766** **35517 Cesson-Sévigné CEDEX** **Tél : 299125000, mél : cesti@aql.fr**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

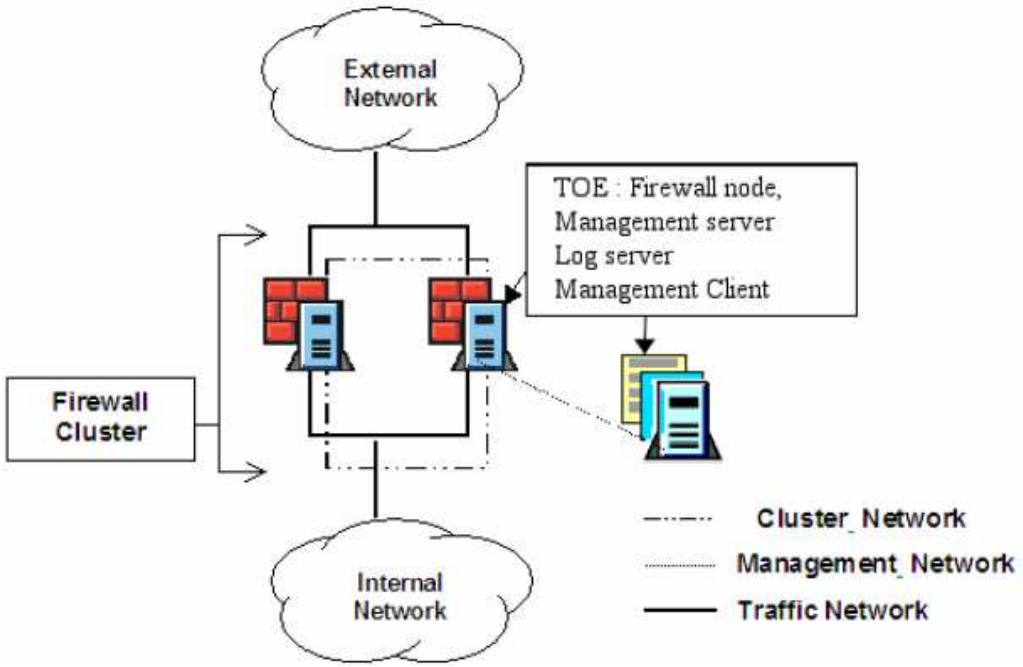
1.1. Présentation du produit

Le produit évalué est « StoneGate Firewall/VPN**,** 5.2.4 build 8069 **»,** développé par STONESOFT France. Il assure des fonctionnalités de pare-feu et de VPN. Seules les fonctionnalités de pare-feu ont été évaluées.

Il s'agit d'une *appliance* à haute disponibilité, dont les services pare-feu incluent le filtrage dynamique des paquets et un contrôle du flux d'informations au niveau applicatif.

Un système d'administration est disponible et apporte une interface sécurisée pour la gestion des règles du pare-feu et des journaux d'évènements. Ce système est installé sur un serveur externe à l'*appliance*.

StoneGate Firewall/VPN peut fonctionner comme un pare-feu autonome ou au sein d'un *cluster* de 2 à 16 nœuds. Le *cluster* de pare-feu est nécessaire pour assurer une haute disponibilité des services de sécurité



1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☒ **3 – firewall**
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☐ 99- Autres

1.2.2. Identification du produit

La version du pare-feu installée sur le réseau est identifiable via le récapitulatif du statut des pare-feu depuis l'interface d'administration (« *Management Client* »).

L'intégrité du *package* d'installation peut être vérifiée à l'aide des checksums fournit par le développeur sur son site internet (https://my.stonesoft.com/download).

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- le contrôle du flux d'informations ;
- la translation d'adresses réseau (NAT) ;
- la journalisation et l'audit ;
- l'administration de la sécurité.

1.2.4. Configuration évaluée

Le produit a été évalué en configuration « *cluster* » comprenant deux nœuds de pare-feu.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La charge de travail prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques, soit 25 hommes x jours.

En raison de difficultés d'installation et de configuration du produit, la durée réelle de l'évaluation a été supérieure à la charge de travail prévue lors de la demande de certification.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2.1 « Type de produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 3.2.1 « Identification des biens sensibles »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 3.2.2 « Menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 4.1 « Objectifs de sécurité pour la cible d'évaluation »).

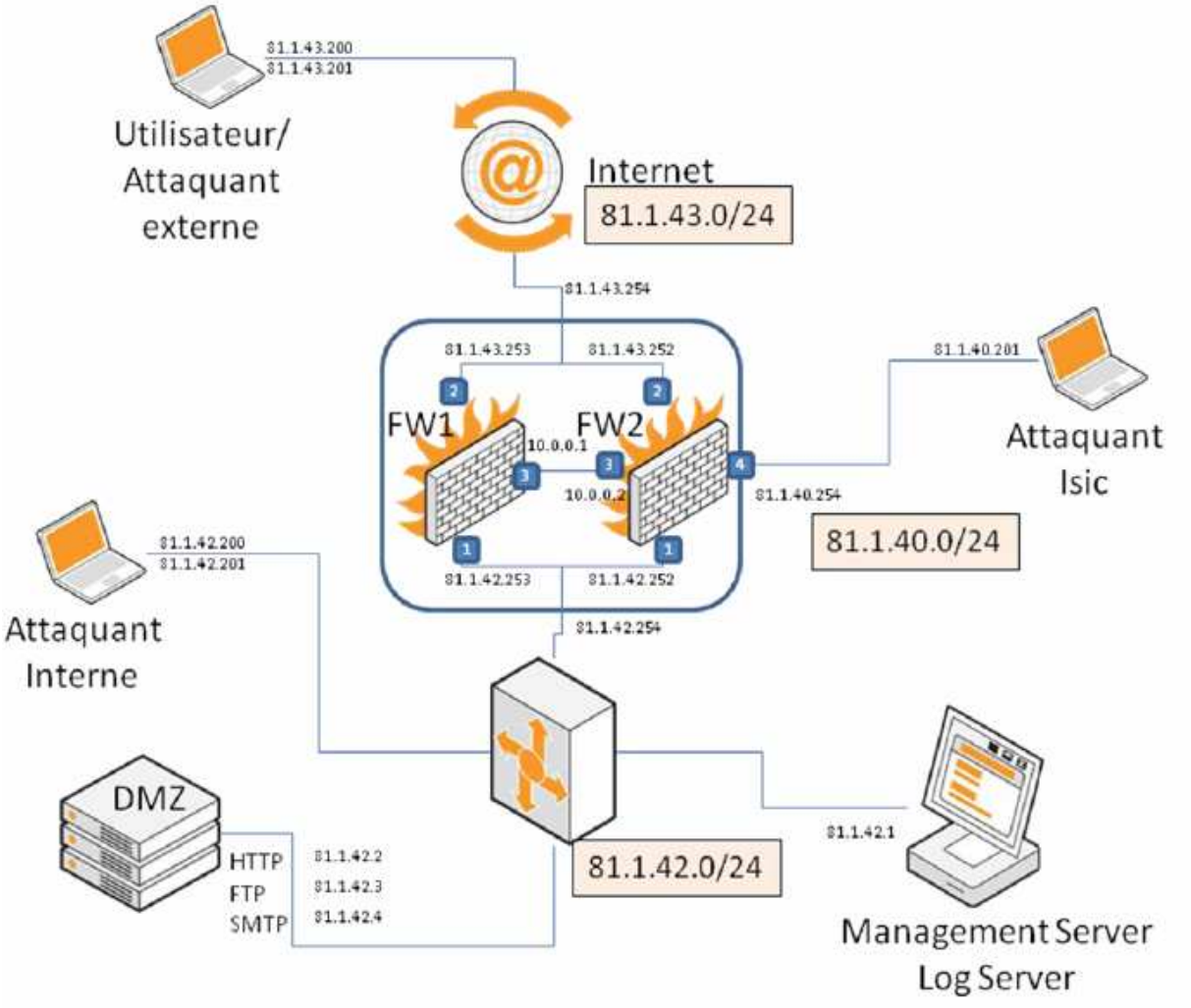
2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2 « Description de la cible d'évaluation »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Le produit a été évalué selon la configuration suivante :



Les éléments de la plate-forme de test utilisée sont les suivants :

- Management Server et Log Server : Windows 7 64bits ;
- Serveur HTTP : Linux Ubuntu 11.04 et Apache 2.2.7 ;
- Serveur FTP : Linux Ubuntu 11.04 et VSFTPD version 2.3.2 ;
- Serveur SMTP : Linux Ubuntu 11.04 et Postfix version 2.8.2 ;
- Utilisateur / Attaquant externe :
  - Windows 7 64 bits et
  - Linux Ubuntu 11.04 ;
- Attaquant Isic (tests de dénis de service) : Linux Ubuntu 11.04 ;
- Attaquant interne : Linux Ubuntu 11.04.

2.3.2.2. Particularités de paramétrage de l'environnement

Le produit étant une *appliance*, il ne nécessite aucun paramétrage particulier de l'environnement.

2.3.2.3. Options d'installation retenues pour le produit

La console d'administration StoneGate Management Center a été installée avec l'option « Typical » (Management Server, Log Server et Management Client). Les deux pare-feu StoneGate étaient configurés en *cluster* :

- les interfaces n°1 (cf. figure du chapitre 2.3.2.1) de chaque pare-feu étaient connectées à un *switch* gigabits Ethernet vers le réseau interne ;
- les interfaces n°2 étaient connectées via un autre *switch* gigabits Ethernet au réseau externe ;
- les interfaces n°3 étaient reliées entre elles, constituant le « *Heartbeat* » permettant aux deux pare-feu de dialoguer ensemble.

La politique de filtrage était configurée de manière à ne laisser passer que certaines connexions depuis le réseau externe vers le réseau interne (services HTTP, SMTP et FTP) ainsi que les paquets ICMP. Toutes les connexions vers et depuis la station d'administration étaient autorisées.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

La génération de licence s'effectue sur le site web du développeur en enregistrant le « *proof-of-license* » ou « *proof-of-serial number* » du produit. Un mail contenant les informations de licence des pare-feu, ainsi que les licences elles-mêmes (via un fichier .jar), est envoyé au client. Il suffit alors de les installer par le Management Client.

L'installation se fait en plusieurs étapes :

- installation du Management Server, du Log Server et du Management Client ;
- installation des licences ;
- configuration du réseau à l'aide du Management Client ;
- installation logicielle et configuration des pare-feu;
- transfert des politiques sur les pare-feu.

Aucune non-conformité n'a été observée.

2.3.2.5. Durée de l'installation

En raison du nombre important de fonctionnalités offertes par le produit, son installation et sa configuration sont particulièrement complexes. Il a fallut plusieurs jours à l'évaluateur pour obtenir une configuration parfaitement fonctionnelle du pare-feu.

2.3.2.6. Notes et remarques diverses

L'installation nécessite une connaissance approfondie du domaine des pare-feu pour être menée à bien.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. Bien que très complets, ces documents sont complexes et nécessitent une attention particulière et une lecture approfondie afin d'être utilisés correctement.

2.3.4. Revue du code source (facultative)

Les évaluateurs n'ont pas eu accès au code source du produit.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Contrôle du flux d'informations pour les protocoles HTTP, SMTP et FTP	**Réussite (voir 2.3.7)**
Translation d'adresses réseau (NAT)	**Réussite**
Journalisation et audit	**Réussite**
Administration	**Réussite**

2.3.6. Fonctionnalités non testées

Le moteur de pare-feu prend en charge de nombreux protocoles qui n'étaient pas dans le périmètre de l'évaluation. Seuls les protocoles HTTP, SMTP et FTP ont été testés.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

L'utilité des agents protocolaires dédiés à l'analyse des protocoles HTTP et SMTP ne s'est pas révélée probante. En effet, bien que leurs comportements soient conformes à ce qui est décrit dans la cible de sécurité [CDS], ils sont peu ou pas configurables et permettent uniquement de renvoyer les paquets vers un serveur IDS externe.

2.3.8. Avis d'expert sur le produit

La configuration des pare-feu demande de solides connaissances de l'administration réseau et des protocoles réseau. Les tests montrent que dans la plupart des aspects, le produit se comporte correctement. Les agents protocolaires sont utilisés pour filtrer les requêtes de certains services et pour éliminer celles dont le comportement parait suspect ou dont le contenu ne suit pas la norme associée. En réalité, hormis l'agent FTP qui réalise correctement l'inspection des paquets FTP, les autres agents protocolaires sont de simples agents de redirection vers des serveurs IDS. Aucune analyse des protocoles n'est réalisée.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Mise en œuvre des règles de sécurité telles que configurées dans l'application
Blocage des attaques suite à leur détection
Journalisation des évènements et des actions

2.3.9.2. Avis d'expert sur la résistance des mécanismes

L'évaluation a montré que si la configuration « par défaut » du produit est activée, ces mécanismes de sécurité n'offrent pas une résistance suffisante. Par conséquent, il est essentiel d'appliquer les recommandations indiquées dans le §2.3.12.2 ainsi que celles contenues dans [GUIDES].

Il a notamment été montré que le produit ne fournissait pas directement de moteur de détection d'intrusion. Il permet cependant de rediriger certains protocoles vers un système de détection d'intrusion externe (cf. §2.3.12.2).

Le produit est résistant à une attaque de type « déni de service ». Toutefois, dans certains cas, la visualisation des journaux d'évènements et d'actions peut être ralentie.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Une fois le produit configuré conformément au §2.3.12.2 et aux [GUIDES], aucune vulnérabilité n'a pu être exploitée dans l'environnement décrit dans la cible de sécurité [CDS].

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Dans leur configuration par défaut, les services de sécurité offerts par le produit StoneGate Firewall/VPN peuvent être remis en cause. Il est donc important de respecter les recommandations indiquées dans le §2.3.12.2 et dans [GUIDES].

2.3.12.2. Recommandations pour une utilisation sûre du produit

<u>Configuration du pare-feu</u>

Le pare-feu doit être configuré en respectant les guides d'utilisations [GUIDES]. Plus particulièrement, l'utilisateur devra veiller à ce que :

- les règles d'analyse du protocole TCP soit passées en mode « strict » ;
- la case « *Keep Previous Configuration Definitions* » soit décochée lors d'un changement de configuration.

<u>Gestion du client d'administration</u>

Afin de contrôler la complexité des mots de passe, il est nécessaire d'activer l'option « *Enforce Password Settings* » dans l'utilitaire « System Tools » du client d'administration.

Comme indiqué dans la cible de sécurité [CDS], les administrateurs autorisés à utiliser le client d'administration doivent être formés, qualifiés et de confiance. Ils doivent également être les seuls à avoir un accès physique au poste sur lequel est installé le client d'administration.

Le client d'administration doit être installé sur un PC hébergeant un système d'exploitation correctement administré et à jour des correctifs de sécurité. Il doit être au minimum protégé

par un produit anti-virus (avec bases d'information à jour et proposant des fonctions de détection des infections informatiques furtives - anti-*spyware*, anti-*rootkit*, etc.).

Analyse des protocoles filtrés
Pour permettre une analyse en profondeur des protocoles, il est nécessaire d'installer un serveur IDS et d'activer la fonction IPS (« *Deep Inspection* ») dans l'interface d'administration du produit afin de rediriger les paquets vers le serveur.

2.3.12.3. Avis d'expert sur la facilité d'emploi

De par sa nature, Stonegate Firewall/VPN est destiné à être utilisé par un administrateur possédant des connaissances pointues dans la gestion des pare-feu.
L'approche choisie par le développeur pour la configuration du produit est assez complexe et nécessite un temps d'adaptation non négligeable. Les nombreuses possibilités offertes par le produit justifient le volume important de la documentation [GUIDES], mais nécessitent d'être étudiées avec minutie.
Les principales fonctions du produit sont facilement accessibles via le « Management Client », ce dernier fonctionnant d'une manière similaire à un navigateur / explorateur de documents.

2.3.12.4. Notes et remarques diverses

Les aspects jugés comme étant les plus consommateurs de temps sont la configuration, la gestion du *cluster* et la configuration du NAT.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « StoneGate Firewall**,** 5.2.4 build 8069 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*StoneGate Firewall/VPN - Cible de sécurité ;* Date : *06/09/2011*
[RTE]	*Rapport Technique d'Évaluation CSPN ;* Référence : *TON001-RTE-1.20* ; Date : *06/12/2011*
[GUIDES]	Guide d'installation : *StoneGate Firewall Installation Guide ;* Référence : *SGFIG_20101231* ; Date : *31/12//2010* Guide d'utilisation : *StoneGate Firewall/VPN Reference Guide ;* Référence : *SGFIG_20101015* ; Date : *15/10/2010* Guide d'administration : *StoneGate Administrator's Guide ;* Référence : *SGAG_20101027* ; Date : *27/10/2010*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr