Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2013/01

IPS Stonegate
Version 5.4.1

Paris, le 19 février 2013

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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-2013/01**
Nom du produit **IPS Stonegate**
Référence/version du produit **5.4.1 build 9659**
Catégorie de produit **Détection d'intrusions**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **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** **France**

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 le logiciel « IPS Stonegate**,** version 5.4.1 **»** développé par Stonesoft. Ce logiciel est embarqué dans la solution matérielle intégrée (de type *appliance*) StoneGate IPS-1205.

Il s'agit d'un système de détection et de prévention d'intrusion réseau (ou NIDPS pour *Network Intrusion Detection and Prevention System*) proposant une analyse de flux réseau, des remontées d'alertes et un blocage des tentatives d'intrusion détectées.

Le système StoneGate est composé de :

- une ou plusieurs *appliance* IPS-1205 ;
- un système d'administration SMC (*StoneGate Management Center*) pour la configuration de l'IPS comprenant les composants suivants :
    - un serveur de gestion (*Management Server*) pour la configuration de l'IPS ;
    - un ou plusieurs serveurs de journalisation (*Log Server*) pour le stockage et la gestion des journaux ;
    - un ou plusieurs clients du serveur de gestion (*Management Client*) qui fournissent une interface graphique de configuration et de suivi de l'IPS.

L'*appliance* peut être installée dans deux configurations :

- en mode IDS (*Intrusion Dectection System*) : le produit est installé pour capturer et analyser des flux sans les filtrer ;
- en mode IPS (*Intrusion Prevention System*) : le produit est installé pour capturer, analyser les flux et filtrer ceux correspondants à d'éventuelles tentatives d'intrusion.

1.2. Description du produit évalué

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

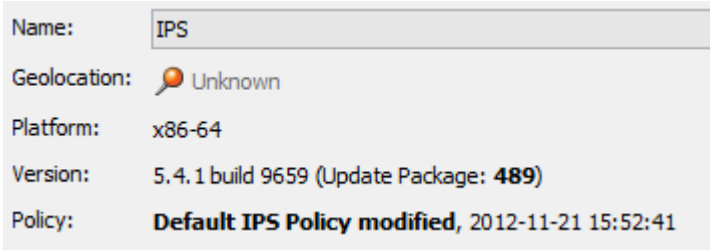
1.2.1. Catégorie du produit

☒ **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

1.1.1. Identification du produit

Organisation éditrice	StoneSoft
Nom commercial du produit	StoneGate IPS Appliance
Numéro de la version évaluée	Appliance IPS-1205 embarquant la suite logicielle de l'IPS StoneGate version 5.4.1

La version de l'appliance est accessible via l'interface principale :



La version du moteur peut aussi être récupérée via la console série en tapant la commande *sg-version* :

```
root@IPS:~# sg-version
Stonesoft Engine version 5.4.1.9659 (x86_64)
```

1.2.2. Services de sécurité

L'IPS StoneGate propose deux principaux services de sécurité :

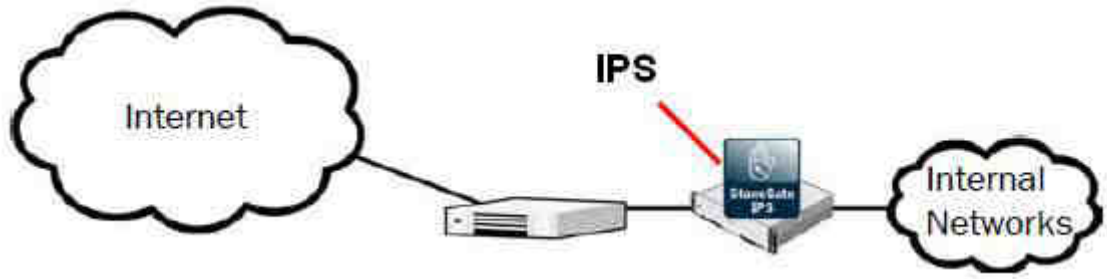
- détection des intrusions ;
- blocage des intrusions.

Pour assurer le bon fonctionnement de ces deux services principaux, le produit dispose également des fonctions de sécurité suivantes :

- mise à jour de la base de signatures d'intrusions ;
- corrélation d'évènements ;
- mise à disposition d'une liste noire d'adresses IP ;
- gestion des alertes et des journaux.

1.2.3. Configuration évaluée

L'IPS StoneGate est évalué en mode coupure.



Installation du produit en mode coupure

La configuration et la politique par défaut[1] ont été retenues pour cette évaluation. Cette configuration correspond à un compromis entre performance et détection des attaques : toutes les règles de filtrage ne sont pas activées. Il est donc important d'adapter la configuration en fonction de l'environnement dans lequel le produit est destiné à être utilisé et en fonction des menaces qu'il est censé couvrir (cf. §2.3.12.2).

[1] La configuration et la politique par défaut sont celles en place directement après l'installation du produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et s'est également basée sur la méthodologie pour l'évaluation des systèmes de détection d'intrusion réseau, en phase expérimentale [CSPN-IDS]. Les références des documents se trouvent en annexe 2.

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

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN-IDS] pour un système de prévention d'intrusions, soit 35 hommes x jours.

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 « Argumentaire du produit»).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 3 « Description des biens sensibles que le produit doit protéger »).

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

Conforme à la cible de sécurité [CDS] (chapitre 4 « Menaces supposées de l'environnement »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 5 « Fonctions de sécurité du produit »).

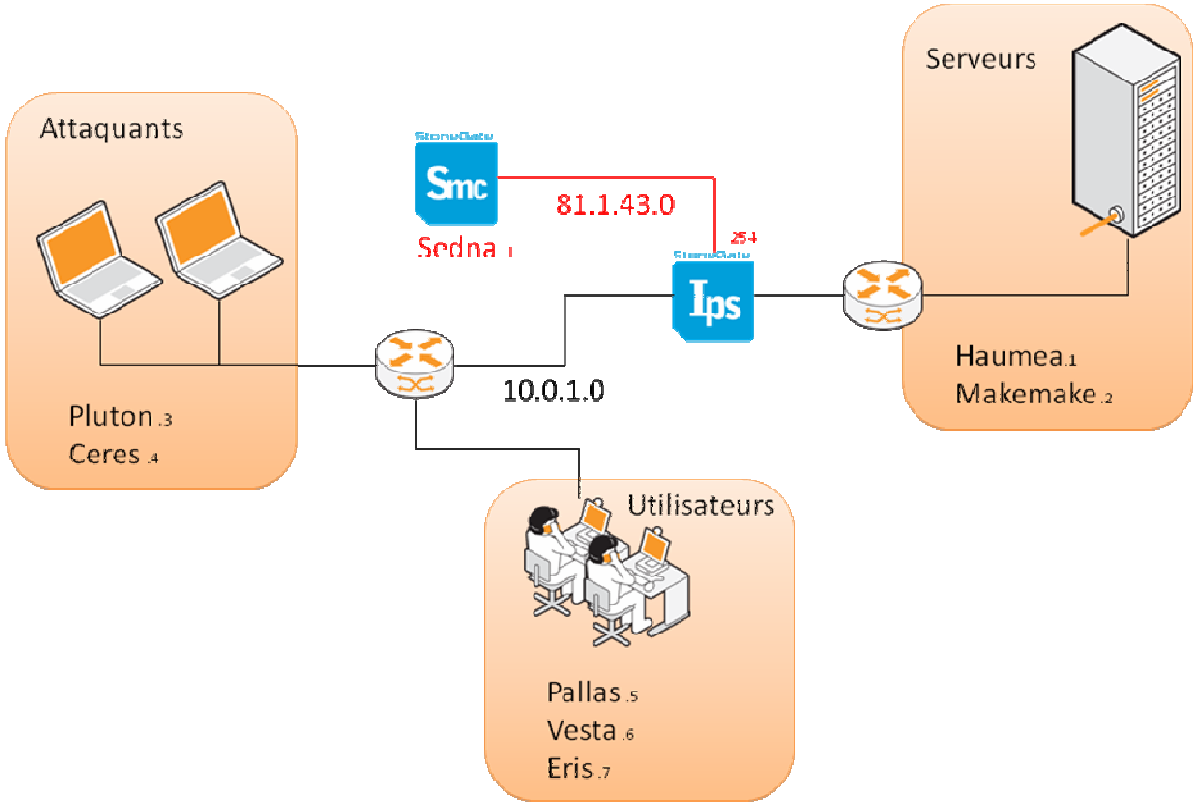
2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.3 « Utilisateurs typiques »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Le produit a été évalué dans la configuration suivante :



Les éléments de la plateforme de test utilisée sont les suivants :

- Attaquants (Pluton & Céres)
  - Pluton & Céres sont équipées d'un Linux Ubuntu 12.04 32 bits spécialisé avec des paquetages « Backtrack » ;
  - Céres peut aussi être démarrée en dual boot sous Windows Seven Pro 64 bits avec le logiciel Nessus 5.0.1.
- Utilisateurs (Pallas, Vesta et Eris)
  - Stations Ubuntu 10.0.4 32 bits et Slitaz 32 bits pour générer du trafic réseau légitime.
- Serveurs (Makemake et Haumea)
  - Makemake, serveur Ubuntu 12.04 32 bits contenant quelques services réseau à jour (Apache/PHP, OpenSSH…) ;
  - Haumea, serveur Ubuntu 11.10 32 bits contenant de nombreux services réseau non mis à jour (Apache/PHP, OpenSSH…).
- Appliance Stonegate 1205 IPS en version logicielle 5.4.1
  - Station Windows Seven Pro 64 bits avec le client / serveur SMC.

2.3.2.2. Particularités de paramétrage de l'environnement

Aucune dépendance logicielle n'est requise pour installer le produit. La seule contrainte est que l'utilisateur doit disposer des droits administrateur pour l'installation et l'utilisation du produit.

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*) sur un serveur.

La politique d'inspection est configurée par défaut. La politique est donc la suivante :

- bloquer et loguer les attaques avérées ;
- laisser passer et loguer les attaques potentielles ;
- laisser passer et loguer les dénis de service ;
- laisser passer et loguer les scans réseau.

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

L'installation du produit nécessite l'installation préalable du centre de configuration qui permet de configurer le moteur de l'IPS et de l'installer sur l'*appliance*. L'administrateur peut faire cette dernière étape de deux façons :

- soit il connaît l'adresse IP de l'IPS et peut s'y connecter directement via le centre de configuration ;
- soit il enregistre la configuration sur une clé USB et redémarre l'IPS avec la clé branchée.

Le centre de configuration permet également de télécharger la dernière version du moteur de l'IPS.

2.3.2.5. Durée de l'installation

En prenant en compte la configuration du réseau et de l'IPS, la durée de l'installation est de l'ordre d'une journée.

2.3.2.6. Notes et remarques diverses

L'installation est simple mais une configuration du produit et du réseau est nécessaire pour rendre le produit opérationnel.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est très complète et aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

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

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Détection des intrusions	**Réussite**
Blocage des intrusions	**Réussite**
Mise à jour de la base de signatures	**Réussite**
Corrélation d'évènements	**Réussite**
Liste noire	**Réussite**
Gestion des alertes et des journaux	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

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

La vérification de conformité des fonctionnalités de détection et de blocage des intrusions a permis de valider que le produit détectait et bloquait des attaques dont les signatures étaient présentes dans sa base mais elle ne présume pas de la complétude de la base de signature elle-même.

De la même manière, la vérification de la conformité de la fonctionnalité de corrélation d'évènements a permis de valider que les fonctionnalités de corrélation décrites dans la cible de sécurité [CDS] étaient bien présentes mais elle n'atteste pas que cette fonctionnalité puisse bloquer l'ensemble des attaques connues.

2.3.8. Avis d'expert sur le produit

Les tests menés sur l'IPS Stonegate 1205 montrent que ce dernier détecte correctement les paquets réseau non conformes aux standards et les tentatives d'intrusion dont la signature est présente dans sa base.

Lorsque l'évaluation a mis en avant des attaques non détectées par le produit, le développeur a été extrêmement réactif pour fournir les signatures appropriées qui ont permis de détecter les attaques concernées.

L'IPS a également été utilisé en coupure entre plusieurs machines clientes et internet. Aucun ralentissement n'a été noté et le produit n'a émis aucun faux positif lors d'une utilisation classique du web (navigation, mails, sites https, ftp, etc.).

Pour finir, l'évaluateur attire l'attention de l'utilisateur sur le nombre important d'options de configuration proposées par le logiciel SMC. Cette richesse fonctionnelle se traduit par une certaine complexité. C'est pourquoi il est recommandé de suivre une formation avant toute utilisation et de lire attentivement la documentation.

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
Autoprotection du produit face aux dénis de service
Détection d'attaques avancées

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Bien qu'aucune vulnérabilité mettant l'IPS hors d'état de fonctionner n'ait été détectée, il est important de noter que, comme c'est le cas pour la plupart des matériels réseaux, le produit ne peut gérer seul une surcharge importante et que l'architecture globale du réseau doit être proportionnée et adéquate pour limiter le risque de dénis de service.

Dans sa configuration par défaut et avec la base de signature utilisée durant l'évaluation, le produit n'a pas réussi à détecter ni à bloquer des attaques avancées ou des mutations d'attaques connues. Cette limitation est inhérente aux produits s'appuyant sur des bases de signatures.

Pour palier ce défaut, et comme indiqué dans [CSPN-IDS], l'évaluateur a étudié la rapidité de réaction et la fréquence des mises à jour de la base par Stonesoft : le développeur s'est montré très réactif et les mises à jour proposées étaient fonctionnelles. L'évaluateur a également testé la fonction d'ajout manuel de signature. Cette fonctionnalité est facile à prendre en main et a été jugée opérationnelle et efficace.

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 cette version du produit en particulier.

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

Aucune.

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

Sans objet.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Comme indiqué dans le §1.2.3 du présent rapport, la configuration évaluée est celle par défaut et il est nécessaire de l'adapter à ses besoins. Notamment, l'évaluateur estime que, pour augmenter le niveau de sécurité du produit, les options suivantes peuvent être envisagées :

- activer « ***Enforce Password Settings*** » du *Management Client* afin de forcer la complexité des mots de passe. Les paramètres par défaut (nombre de caractères, durée de validité, nombre d'essais, etc) sont modifiables dans le fichier « SGConfiguration.txt ».
- désactiver le démon SSH permettant d'accéder à la configuration des pare-feux en ligne de commande lorsqu'il n'est pas utilisé ;
- activer le mode « ***Strict TCP for Deep Inspection*** » ;
- désactiver dans la fenêtre de dialogue le bouton « ***Keep previous configuration definitions*** » pour obliger l'*appliance* à mettre en place la nouvelle politique sur toutes les connexions.

Par ailleurs, en fonction des menaces contre lesquelles le réseau doit être protégé, il est conseillé d'ajouter à la configuration par défaut certaines situations devant être bloquées ou journalisées. Par exemple, si l'on veut bloquer certains types de *scan* réseau, les règles suivantes peuvent être ajoutées à la configuration par défaut :

Exceptions | Inspection

ID	Logical Interface	Situation	Source	Destination	Severity	Protocol	Action	Logging
1.1.1	ANY	TCP_SYN_Scan_Started	ANY	My Scan Target Net	ANY	ANY	Terminate	Stored
1.1.2	ANY	DOS_TCP_SynAck_Started	ANY	My SynFlood Protected Server	ANY	ANY	Terminate	Stored
1.1.3	ANY	ICMP_Ping_Scan_Started UDP_Scan_Started	ANY	My Scan Target Net	ANY	ANY	Permit	Stored

Enfin, le poste d'administration doit héberger un système d'exploitation à jour concernant les correctifs de sécurité et être correctement administré. Le poste doit être durci afin d'être protégé contre des codes malveillants (voir le guide d'hygiène informatique [GUIDE-ANSSI], notamment ses règles 14 et 15).

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

De par sa nature, l'IPS Stonegate 1205 est destiné à être utilisé par un administrateur possédant des connaissances avancées dans ce domaine.

Comme indiqué dans le §2.3.8, les nombreuses possibilités offertes par le produit rendent sa configuration complexe et il est nécessaire que l'utilisateur les étudie avec minutie pour les appréhender au mieux.

2.3.12.4. Notes et remarques diverses

Néant.

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 « IPS Stonegate**,** version 5.4.1 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

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]	*Cible de sécurité StoneGate IPS ;* Version 1.1 ; Date : *21/06/2012.*
[RTE]	*Stonesoft – Rapport Technique d'Évaluation CSPN ;* Référence : *TON001C3-RTE-1.00 ;* Date : *23/11/2012.*
[GUIDES]	Guide d'installation : *StoneSoft IPS and Layer 2 Firewall Installation Guide ;* Référence : *GIRG_20120828* ; Date : *28/08/2012.* Guide d'administration : *StoneGate Administrator's Guide ;* Référence : SGIRG_20120829; Date : *29/08/2012.*
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.

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
[CSPN-IDS]	Méthodologie pour l'évaluation des systèmes de détection d'intrusion réseau en vue d'une certification de sécurité de premier niveau, phase expérimentale.