Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2009/04

Paris, le 31 août 2009

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 devrait 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 la 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 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.dcssi@sgdn.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2009/04

Nom du produit

Netfilter sur un noyau Linux v2.6.27 – iptables v1.4.2

Référence/version du produit

Version 2.6.27

Critères d'évaluation et version

CERTIFICATION SECURITE DE PREMIER NIVEAU (CSPN, Phase expérimentale)

Développeur(s)

Netfilter Core Team

http://www.netfilter.org

Commanditaire

Secrétariat Général de la Défense Nationale
51, boulevard de la Tour Maubourg
75700 – Paris – 07 SP
France

Centre d'évaluation

Oppida

6, avenue du Vieil Etang 78180 Montigny Le Bretonneux
Tél : +33 (0)1 30 14 19 00, mél : christophe.blad@oppida.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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 « Netfilter sur un noyau Linux v2.6.27 – iptables v1.4.2 **»,** dénommé ci-après **Netfilter,** développé par la société Netfilter Core Team.

Netfilter est un pare-feu « stateful » (protection contre les attaques réseau de niveaux 3 et 4) et modulaire réservé aux noyaux Gnu/Linux 2.4.x et 2.6.x, distribué sous licence Gnu/GPL. Iptables est l'interface en « lignes de commandes » qui permet de configurer Netfilter. On désigne couramment ce pare-feu par l'association Netfilter-iptables.

Netfilter est principalement utilisé dans les interconnections de réseaux de confiance avec un ou plusieurs réseaux non maîtrisés comme Internet.

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 – pare-feu
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

Le numéro de version de Netfilter est vérifiable en tapant la commande « uname –a » et le numéro de version d'Iptables la commande « iptables –version ».

1.2.3 Services de sécurité

La fonctionnalité principale de Netfilter est de fournir au système la capacité de restreindre les flux d'informations en provenance ou à destination d'un réseau protégé dans le but de protéger les ressources de ce réseau contre des attaques en provenance d'autres réseaux (via l'interconnexion où est mis en œuvre Netfilter) :

- application d'une politique de filtrage ;
- audit/journalisation des flux IP.

Application de la politique de filtrage

Netfilter est un pare-feu qui offre des fonctionnalités de filtrage des flux entre des réseaux IP, basées sur des règles permettant de mettre en œuvre la politique de sécurité du système d'information concerné. Pour bénéficier d'un filtrage optimum, la politique de sécurité doit être cohérente et non ambiguë. Deux types de filtrage peuvent être distingués :

- le filtrage non contextuel : l'action de filtrage (acceptation, blocage, rejet, avec journalisation ou non) est déterminée en fonction du contenu d'un paquet réseau ;
- le filtrage contextuel : sur la base d'un premier filtrage non contextuel, Netfilter établit un contexte et des règles de filtrage adaptées, basées sur les caractéristiques du flux identifié (origine, destinataire, protocoles). La connaissance de ce contexte permet à Netfilter, d'une part de gagner en performance, et d'autre part d'augmenter la pertinence du filtrage et sa précision. Les fonctionnalités de filtrage, contextuel ou non, offertes par Netfilter s'appliquent uniquement aux flux portés par le protocole IP et prennent en compte les couches réseau, transport et applicatives (FTP).

Audit/journalisation des flux IP

Ce service permet de tracer tous les flux IP traités par Netfilter. Il permet aussi la définition des événements à tracer et leur consultation.

Sécurité du journal d'audit

Iptables fournit une directive (LIMIT) permettant de limiter la fréquence de journalisation des événements, ce qui peut prévenir certaines formes d'attaques par déni de service.

1.2.4 Configuration évaluée

Les fonctions de sécurité de Netfilter incluses dans le périmètre de l'évaluation sont les suivantes :

- **filtrage IP** (options de configuration CONFIG_IP_NF_FILTER, CONFIG_NETFILTER_XT_MATCH_CONNLIMIT, CONFIG_XP_MATCH_STATE et CONFIG_XP_MATCH_LIMIT) ;
- **suivi des connexions** (options de configuration CONFIG_NF_CONNTRACK et IP_CONNTRACK_IPV4) ;
- **gestion du protocole FTP (**option de configuration CONFIG_NF_CONNTRACK_FTP) ;
- **traduction d'adresses réseau (NAT)** (option de configuration CONFIG_NF_NAT) ;
- **configuration des règles via l'utilitaire iptables** (options de configuration CONFIG_XTABLES et CONFIG_IP_NF_IPTABLES) ;
- **journalisation** (option de configuration CONFIG_IP_NF_TARGET_LOG).

2 L’évaluation

2.1 Référentiels d’évaluation

L’évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. 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 20 hommes x jour. L’évaluation s’est déroulée au cours du mois de mars 2009.

2.3 Travaux d’évaluation

Ce paragraphe apporte des compléments sur la cible de sécurité [ST] 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 [ST].

2.3.1.2 Biens sensibles manipulés par le produit

Conforme à [ST].

2.3.1.3 Description des menaces contre lesquelles le produit apporte une protection

Conforme à [ST]. L’évaluateur a complété la cible en présentant les différents chemins permettant à un attaquant de stocker des informations dans des zones non accessibles ou non utilisées par le système ou l’utilisateur.

2.3.1.4 Fonctions de sécurité

Conforme à [ST].

2.3.1.5 Utilisateurs typiques

Conforme à [ST].

2.3.2 Installation du produit

2.3.2.1 Plate-forme de test

La distribution Linux qui a été retenue pour l’évaluation du produit est une distribution **Debian 5.0** (**Lenny**) compilée pour une architecture **x86**.

Architecture matérielle

Le produit Netfilter est installé sur un serveur x86 Dell Dimension 4500 dont les spécifications sont les suivantes :

- processeur Intel Pentium 4 cadencé à 2 Ghz ;
- chipset Intel 845E;
- 256 Mo de mémoire vive ;
- disque dur ATA 100 d'une capacité de 40 Go.

Architecture logicielle

La cible **[ST]** impose que le produit Netfilter soit installé sur un système d'exploitation Gnu/Linux en version **2.6.27**.

La version minimale (« base ») de la Debian a été installée afin de limiter le nombre de packages inutiles. Les caractéristiques de l'installation sont les suivantes :

- librairie « **libc6** » en version **2.7-18** ;
- compilateur « **gcc** » en version **4.3.2**.

Pré-requis pour l'installation du produit Netfilter

Le noyau **2.6.27.18** a été téléchargé à partir du site www.kernel.org. (Fichier **linux-2.6.27.18.tar.gz**)

L'outil de gestion « **iptables** » a été ensuite installé à partir des sources en version **1.4.2** récupérée à partir du site www.netfilter.org. (Fichier **iptables-1.4.2.tar.bz2**).

Architecture réseau

L'architecture réseau retenue pour l'évaluation du produit Netfilter conformément au guide de configuration **[Guide]** est la suivante :

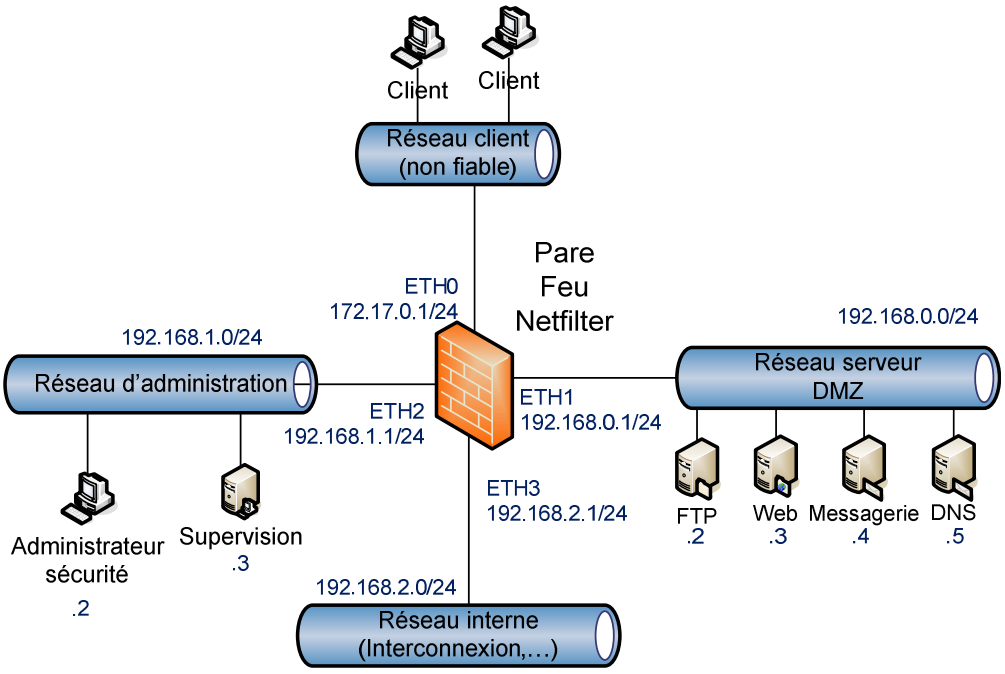

Figure 1: Architecture réseau retenue pour l'évaluation

L'équipement hébergeant le produit Netfilter possède 4 interfaces réseaux, chacune étant reliée à un réseau nécessitant un cloisonnement et le filtrage des flux vis-à-vis des autres réseaux :

- réseau d'administration ;
- réseau interne (de confiance) ;
- réseau hébergeant les serveurs en zone démilitarisée ;
- réseau externe (non fiable).

Le script de paramétrage du pare-feu via l'outil de gestion « **iptables** » correspondant à l'architecture réseau adoptée est décrit dans le guide d'installation **[Guide]**. Ce script est lancé automatiquement au démarrage du pare-feu.

2.3.2.2 Particularités de paramétrage de l'environnement

Paramétrage de la pile IP Linux :

Conformément au guide d'installation **[Guide]** dans le fichier « **/etc/sysctl.conf** », les options suivantes ont été retenues :

- **activation de la protection contre l'usurpation d'adresse IP**

  `net/ipv4/conf/all/rp_filter = 1`

- **autorisation de la journalisation des paquets ayant une adresse IP mal formée**

  `net/ipv4/conf/all/log_martians = 1` (les options de configuration CONFIG_IP_ADVANCED_ROUTER et CONFIG_IP_ROUTE_VERBOSE ont été sélectionnées à la compilation)

- **refus des redirections ICMP**

  ```
  net/ipv4/conf/all/send_redirects = 0
  net/ipv4/conf/all/accept_redirects = 0
  ```

- **refus des paquets dont la source a été routée**

  `net/ipv4/conf/all/accept_source_route = 0`

- **activation de la protection contre les dénis de service**

  `net/ipv4/tcp_syncookies = 1` (l'option CONFIG_SYN_COOKIES a été activée à la compilation)

- **refus de sollicitation de type ping broadcast**

  `net/ipv4/icmp_echo_ignore_broadcasts = 1`

- **autorisation du routage IP**

  `net/ipv4/ip_forward = 1`

2.3.2.3 Options d'installation retenues pour le produit

Les options de configuration du noyau retenues (Fichier .**config**.) comme spécifiées dans la cible de sécurité **[ST]** et le guide d'installation **[Guide]** afin de paramétrer le produit **Netfilter-iptables** sont les suivantes :

- **CONFIG_NETFILTER=y**
- **CONFIG_NF_CONNTRACK=y**
- **CONFIG_NF_CONNTRACK_FTP=y**
- **CONFIG_NETFILTER_XTABLES=y**
- **CONFIG_NETFILTER_XT_MATCH_CONNLIMIT=y**
- **CONFIG_NETFILTER_XT_MATCH_LIMIT=y**
- **CONFIG_NETFILTER_XT_MATCH_STATE=y**
- **CONFIG_NF_CONNTRACK_IPV4=y**
- **CONFIG_IP_NF_IPTABLES=y**
- **CONFIG_IP_NF_FILTER=y**
- **CONFIG_IP_NF_TARGET_LOG=y**
- **CONFIG_NF_NAT=y**

Les options du noyau qui ont dû être ajoutées sont les suivantes :

- **CONFIG_NETFILTER_ADVANCED=y**
  Cette option permet d'activer les options CONFIG_NETFILTER_XT_MATCH_CONNLIMIT et CONFIG_NETFILTER_XT_MATCH_LIMIT

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

Il n'a pas été relevé de non-conformité.

2.3.2.5 Durée de l'installation

Système d'exploitation hôte

L'installation du système d'exploitation linux **Debian 5.0**, des pré-requis d'installation du produit Netfilter et de son paramétrage prennent moins de **30 minutes**.

Installation du produit Netfilter

Le temps requis pour la compilation et l'installation du noyau **2.6.27.18** va dépendre de la puissance du serveur hôte ainsi que du nombre d'options (inutiles) désactivées lors du paramétrage du noyau. Lors des tests, il a fallu environ **45 minutes** pour compiler et installer le noyau d'évaluation ainsi que l'outil « **iptables** ».

2.3.2.6 Notes et remarques diverses

Néant.

2.3.3 Analyse de la conformité

2.3.3.1 Analyse de la documentation

Le **[Guide]** est clair, didactique et étayé par de nombreux exemples. Il contient les informations essentielles à la compréhension du produit Netfilter, tandis que le **[Man]** se focalise sur l'utilisation de l'outil de configuration en ligne de commande « **iptables** ».

2.3.3.2 Revue du code source

Le code est clair, modulaire, structuré et très lisible. De nombreux commentaires très judicieux sont présents, certains se rapportant aux RFC.

2.3.3.3 Fonctionnalités testées

Filtrage IP « sans états » ou « stateless »

Le pare-feu a été évalué comme un routeur filtrant selon l'ip source, l'ip de destination, le port source, le port de destination, le protocole de niveau 4, l'interface d'entrée (gestion de l'anti-spoofing) et les drapeaux TCP activés (scan des ports).

Filtrage IP « avec états » ou « stateful »

Les états suivants ont été évalués :

- NEW pour nouvelle connexion ;
- ESTABLISHED pour connexion établie ;
- RELATED pour une nouvelle connexion dépendant d'une autre connexion déjà établie.

L'état « RELATED » a été testé dans le cas du protocole « FTP » actif ou passif selon les modes PORT, EPRT, PASV et EPSV.
Les fonctions en charge de l'analyse des paquets FTP requête et réponse de chaque mode ont été testés en envoyant manuellement des paquets :

- mal délimités ;
- comportant des caractères non attendus ;
- comportant des données non attendues ;
- comportant un gros volume de données afin de générer un dépassement de tampon mémoire.

L'IP du serveur devant héberger le service DATA est contrôlée et correspond à l'IP de l'initiateur de la connexion de contrôle. Il a également été vérifié que seul le port de destination de la connexion « FTP – DATA » négocié auparavant est autorisé.

Translation d'adresse IP

La fonction NAT a été testée en destination (chaîne PREROUTING) – DNAT et en source (chaîne **POSTROUTING**) – **SNAT.**

La fonction « CONNLIMIT »

Pour tester la fonction « CONNLIMIT », l'évaluateur a généré un nombre important de demandes de connexion et observé le comportement de la table de connexion.

Audit/journalisation des flux IP

Les fonctions d'audit et la journalisation ont été testées pour vérifier qu'elles génèrent les informations suivantes propres aux flux IP :

- la date et l'heure
- le protocole encapsulé dans IP : ICMP, TCP, UDP ;
- les IP source et destination ;
- les ports source et destination dans le cas des protocoles TCP et UDP ;

- le type et le code ICMP ;
- les drapeaux activés et les numéros de séquence dans le cas du protocole TCP ;
- les interfaces mises en jeu ;
- le TTL (« Time To Live ») ;
- l'action effectuée : DROP, REJECT, ACCEPT.

Sécurité du journal d'audit

L'évaluateur a vérifié que la directive « LIMIT » limite bien l'écriture des évènements dans le fichier de journalisation.

2.3.3.4 Fonctionnalités non testées

Les fonctionnalités de Netfilter qui sont hors du périmètre de l'évaluation n'ont pas été testées.

2.3.3.5 Synthèse des fonctionnalités testés / non testées et des non-conformités

L'ensemble des fonctionnalités testées s'est avéré conforme à sa cible de sécurité.

2.3.3.6 Avis d'expert sur le produit

Le produit est conforme à sa cible de sécurité. Toutes les fonctionnalités testées sont implémentées.

2.3.4 Analyse de la résistance des mécanismes et des fonctions

2.3.4.1 Liste des fonctions testées et résistance

Les mécanismes mis en jeu sont :

- le filtrage de paquets réseaux ;
- la journalisation ;
- la protection des journaux.

Lorsque l'équipement est dimensionné correctement (voir §2.3.6.2) pour son usage et que l'administrateur n'a pas commis d'erreurs de configuration et de paramétrage, un attaquant ne pourra ni outrepasser le filtrage mis en place, ni rendre ses actions furtives lorsque celles-ci sont journalisées, ni provoquer un déni de service par une attaque SYN Flood.

2.3.4.2 Avis d'expert sur la résistance des mécanismes

Les mécanismes de sécurité sont robustes.

2.3.5 Analyse des vulnérabilités (conception, construction…)

2.3.5.1 Liste des vulnérabilités connues

Aucune vulnérabilité publique n'est recensée sur cette version du produit Netfilter liée au noyau linux 2.6.27.18.

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

Aucune vulnérabilité n'a été découverte lors de l'évaluation.

2.3.6 Analyse de la facilité d'emploi et préconisations

2.3.6.1 Cas où la sécurité est remise en cause

Un paquet ayant le drapeau « ACK » activé, ne faisant partie d'aucune connexion en cours au niveau de la table de suivi des connexions mais correspondant à une règle de filtrage valide, sera reconnu comme un paquet « NEW » par le pare-feu. Si la destination ne répond pas par un paquet « RST », la connexion possède un timeout de cinq jours.

L'administrateur doit ajouter un filtrage supplémentaire sur les drapeaux TCP (option **–syn**) lors de toute tentative de connexion (règles de filtrage sur l'état « **NEW** », Mode « **stateless** » - Test de la chaine « FORWARD » - Filtrage sur le **drapeau TCP »**).

La notion de connexion dans l'état « NEW » dans le cas de l'emploi du protocole TCP peut être trompeuse. En effet, les paquets TCP SYN et les paquets TCP ACK sont concernés par cet état. Il faut donc spécifier l'option –syn lors de l'écriture d'une règle dans l'état « NEW » concernant une initiation de connexion TCP.

2.3.6.2 Recommandations pour une utilisation sûre du produit

Durcissement de la pile IP :

Afin de durcir la pile IP du système d'exploitation Linux, il est nécessaire d'activer ou de désactiver les fonctions suivantes :

- **ignorer les broadcast ICMP.** (attaque smurf)
  ```
  sysctl-w net.ipv4.icmp_echo_ignore_broadcasts = 1
  ```
- **ignorer les erreurs ICMP bogus**
  ```
  sysctl-w net.ipv4.icmp_ignore_bogus_error_responses = 1
  ```
- **désactiver l'envoi et la réponse aux ICMP redirects.**
  ```
  sysctl-w net.ipv4.conf.all.accept_redirects = 0
  sysctl -w net.ipv4.conf.all.send_redirects=0
  ```
- **activer les SYN Cookies** (attaque syn flood)
  ```
  sysctl-w net.ipv4.tcp_syncookies = 1
  ```
- **enregistrer les paquets martiens**
  ```
  sysctl-w net.ipv4.conf.all.log_martians = 1
  ```
- **activer l'antispoofing niveau Noyau**
  ```
  sysctl-w net.ipv4.conf.all.rp_filter = 1
  ```
- **ignorer le source routing**
  ```
  sysctl-w net.ipv4.conf.all.accept_source_route = 0
  ```

Politique par défaut

La politique par défaut à utiliser doit être « **DROP** » afin de respecter la règle « **Tout ce qui n'est pas explicitement autorisé est interdit** ».

Activation du routage sur le pare-feu

Pour éviter que des flux non autorisés ne transitent par le pare-feu sans avoir été préalablement filtrés, il est nécessaire de désactiver par défaut le routage. Le routage ne doit être activé que lorsque l'ensemble des règles de filtrage du pare-feu ont été chargées. Dans ces conditions, aucun paquet non autorisé ne sera transmis par le pare-feu.

Anti-spoofing

Aucune fonction anti-spoofing n'est implémentée dans le produit Netfilter. Les attaques de type usurpation d'identité « **spoofing** » sont contrées par le filtrage de Netfilter et l'activation de la fonctionnalité Linux « **rp_filter** ».

L'implémentation de la topologie d'un réseau à protéger est à la charge de l'administrateur sécurité.
Dans le cas de l'architecture cible, nous avons 4 réseaux :

- le réseau externe non fiable modélisé par la variable EXTNET=0.0.0.0/0 ;
- le réseau interne fiable modélisé par la variable INTNET=192.168.2.0/24 ;
- le réseau DMZ modélisé par la variable DMZNET=192.168.0.0/24 ;
- le réseau d'administration modélisé par la variable ADMNET=192.168.1.0/24,

Il est nécessaire de créer des règles de filtrages afin d'empêcher les attaques de type usurpation d'identité. Pour cela, il est nécessaire de recenser tous les réseaux « derrière » une interface du pare-feu et d'interdire le transit par le pare-feu de tous les paquets ayant une adresse faisant partie des réseaux identifiés auparavant sur les autres interfaces.

Les règles d'interdiction doivent être positionnées avant toutes les règles d'autorisation.

Dans le cas de l'architecture cible, cela va se traduire de la manière suivante :
Sur l'interface eth0 attachée au réseau externe, l'anti-spoofing va se traduire par les commandes suivantes :

- Sur la chaine « **INPUT** »

```
iptables –A INPUT –i eth0 –s 192.168.0.0/24 -j LOG –-log-prefix “Attaque spoofing “
iptables –A INPUT –i eth0 –s 192.168.0.0/24 -j DROP
iptables –A INPUT –i eth0 –s 192.168.1.0/24 -j LOG –-log-prefix “Attaque spoofing “
iptables –A INPUT –i eth0 –s 192.168.1.0/24 -j DROP
iptables –A INPUT –i eth0 –s 192.168.2.0/24 -j LOG –-log-prefix “Attaque spoofing “
iptables –A INPUT –i eth0 –s 192.168.2.0/24 -j DROP
```

- Sur la chaine « **FORWARD** »

```
iptables –A FORWARD –i eth0 –s 192.168.0.0/24 -j LOG –-log-prefix “Attaque spoofing “
iptables –A FORWARD –i eth0 –s 192.168.0.0/24 -j DROP
iptables –A FORWARD –i eth0 –s 192.168.1.0/24 -j LOG –-log-prefix “Attaque spoofing “
iptables –A FORWARD –i eth0 –s 192.168.1.0/24 -j DROP
iptables –A FORWARD –i eth0 –s 192.168.2.0/24 -j LOG –-log-prefix “Attaque spoofing “
iptables –A FORWARD –i eth0 –s 192.168.2.0/24 -j DROP
```

Module de suivi des sessions

Lors des tests il a été noté que les paquets ayant le drapeau « **ACK** » activé sont acceptés en tant que nouvelle session s'ils ne correspondent pas à une session en cours.

Pour éviter l'acceptation de ces paquets et ne laisser passer que les paquets TCP « SYN », il est nécessaire de spécifier l'option « --syn » aux règles correspondant aux états « NEW ».
Dans le cas d'une règle acceptant les flux FTP à destination d'un serveur interne (en DMZ), cela va se traduire par :

```
iptables –A FORWARD –s 0.0.0.0/0 –d 192.168.0.2 –p tcp --dport 21 --syn –m
state –-state NEW –j ACCEPT
```

Dimensionnement du pare-feu

Le dimensionnement du pare-feu est effectué de façon automatique en fonction de la mémoire vive disponible sur l'équipement. Ce dimensionnement s'effectue selon la règle suivante :

```
nf_conntrack_htable_size = (((num_physpages << PAGE_SHIFT) / 16384) / sizeof(struct hlist_head));
nf_conntrack_max = max_factor * nf_conntrack_htable_size;
max_factor = 4;
```

Le nombre de connexions simultanées correspond donc à la taille de la table de hachage * 4.
Dans notre cas, le pare-feu possède 256 Mo de mémoire vive :

- la table de hachage à une taille de 4096 entrées .
- le nombre de connexions simultanées est donc de 16384.

Ces valeurs peuvent être modifiées de façon dynamique ou au démarrage de l'équipement. Le document [Performance Conntrack] permet de calculer les performances théoriques que pourrait avoir un pare-feu dédié au filtrage en fonction de sa mémoire et ainsi outrepasser les limites par défaut de Netfilter.

Valeurs limites :

La taille de la table de hachage varie par défaut entre 16 et 16384 selon la mémoire RAM disponible. Cela nous donne le tableau suivant dans le cas d'une utilisation typique :

Mémoire RAM disponible	Taille de la table de hachage	Nombre de connexions simultanées
128 Mo	2048	8192
256 Mo	4096	16384
512 Mo	8192	32768
1024 Mo	16384	65536

Dans le cas où le pare-feu dispose de plus de 1 Go de mémoire, il est nécessaire de modifier les valeurs par défaut afin d'outrepasser les limites imposées. Ces limites peuvent être repoussées en modifiant les paramètres suivants :

• Modification du nombre maximum de connections simultanées

```
echo « nouvelle valeur » > /proc/sys/net/ipv4/netfilter/ip_conntrack_max
```

Cette valeur peut être modifiée dynamiquement. Rajouter des connexions revient à allonger les listes chaînées de la table de hachage.

• Modification de la taille de la table de hachage

Cette valeur doit être modifiée avant le chargement du code Netfilter dans le cas où la fonction de suivi des connexions est intégrée au noyau (monolithique). Au démarrage de la distribution Linux, il faut spécifier le paramètre suivant :

```
nf_conntrack.hashsize= « nouvelle valeur »
```

Dans le cas où la fonction de suivi de connexions est chargée en tant que module, la valeur de la taille de la table de hachage peut être modifiée dynamiquement avant son chargement en mémoire :

```
echo « nouvelle valeur » > /sys/module/nf_conntrack/parameters/hashsize
```

Lors de la modification de la taille de la table de hachage, le ratio est de 1 pour 8 connexions supplémentaires.

Réglages par défaut du *timer* de session

Le *timer* des sessions établies expire par défaut au bout de 5 jours d'inactivité. Ce temps semble bien trop long sachant qu'en général, ce *timer* est de 3 600s sur des produits commerciaux. En partant du principe que les applications réseaux gèrent leurs connexions (envoi de *keep-alive*), ce timer peut être drastiquement diminué.

Pour modifier ce *timer*, il est possible d'ajouter certaines entrées dans le fichier « **/etc/sysctl.conf** » :

```
net/netfilter/nf_conntrack_tcp_timeout_established = 3 600
```

Injection des règles

Lorsque de nouvelles règles doivent être injectées, les connexions en cours peuvent ne plus fonctionner tant que les règles validant ces connexions ne sont pas chargées. Il en est de même pour les nouvelles connexions. Il va s'écouler un certain laps de temps dépendant de la puissance de l'équipement et du nombre de règles contenues dans le script pendant lequel des paquets « légitimes » seront rejetés par le pare-feu (exemple : 1 mn pour 4 000 règles).

2.3.6.3 Avis d'expert sur la facilité d'emploi

Le produit Netfilter est simple d'utilisation dans le cas d'une architecture ne devant comporter qu'un petit nombre de règles.

Dans le cas d'une architecture complexe pouvant comporter plusieurs milliers de règles, la gestion des règles par le produit Netfilter peut s'avérer difficile. En effet, le nombre de règles augmente très facilement puisque :

- journaliser une règle revient à rajouter une règle ;
- il n'existe pas de notion de « groupe » (regroupement d'adresses IP, de services) ;
- la gestion d'une connexion peut engendrer trois règles (la règle « **NEW** » à sens unique, la règle « **ESTABLISHED** » dans les deux sens de la connexion et la règle « **RELATED** » le cas échéant).

2.3.7 Accès aux développeurs

Le code source complet est disponible depuis le site de netfilter.org. L'évaluateur n'a pas eu de contact avec la communauté de développeurs de Netfilter durant l'évaluation.

2.4 Analyse de la résistance des mécanismes cryptographiques

Le produit évalué ne comporte pas de mécanismes cryptographiques.

3 La certification

3.1 Conclusion

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

Ce certificat atteste que le produit Netfilter soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

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 [ST], suivre les recommandations énoncées dans le présent rapport de certification au paragraphe 2.3.6.2 ainsi que celles se trouvant dans les guides fournis [GUIDES] avec le produit.

Annexe 1. Références documentaires du produit évalué

[CDS]	CdS-CSPN-Netfilter-Iptables_v2.1.pdf du 22 novembre 2007
[RTE]	OPPIDA/CESTI/NETFILTER/RTE/1.2 du 10 juin 2009
[Guides]	« **Guide de configuration de Netfilter** » AUA_-_Guide_de_configuration_Netfilter_v1.4.pdf
[Man]	« **Man de la commande iptables** » iptables_fr.tar.gz

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2.4, phase expérimentale, n°915/SGDN/DCSSI/SDR/CCN, 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1.4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1.3.