1. Identification du produit

Organisation éditrice	Netfilter Project (communauté opensource)
Lien vers l'organisation	www.netfilter.org
Nom commercial du produit	Netfilter-iptables
Numéro de la version évaluée	Netfilter sur un noyau Gnu/Linux v2.6.27 - iptables v1.4.2
Catégorie de produit	Firewall

2. Argumentaire (description) du produit

a. Description générale du produit

Le principal usage des pare-feu tels que Netfilter-Iptables réside dans l'interconnexion de réseaux de confiance avec un ou plusieurs réseaux non maîtrisés comme Internet. L'interconnexion doit pouvoir se faire sans dégrader le niveau de sécurité du ou des réseaux de confiance grâce à des règles de filtrage pouvant couvrir les niveaux 2 à 5.

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, les premiers développements sont le fait de Paul Russel à partir d'Octobre 1999. Aujourd'hui, une communauté de développeurs a repris le projet en main et assure le portage sous les noyaux 2.6. Iptables est l'interface en « lignes de commandes » qui permet de configurer Netfilter. On désigne couramment ce pare-feu par l'association Netfilter-iptables.

b. Description de la manière d'utiliser le produit

Le produit est démarré au lancement du système hôte et reste actif en permanence.

c. Description de l'environnement prévu pour son utilisation

L'environnement d'utilisation de Netfilter est exclusivement orienté vers les systèmes Gnu/Linux ; cela exige par conséquent des compétences pointues au niveau de l'OS en plus d'une maîtrise de l'édition des règles sous Netfilter.

Le contexte opérationnel du pare-feu Netfilter est relativement large. Il s'étend depuis la petite entreprise souhaitant se connecter à Internet à l'opérateur de télécommunications désirant protéger ses serveurs publics (messagerie, web, news, etc.) en passant par les postes personnels.
La polyvalence de Netfilter est liée à la nature même du système Gnu/Linux. Celui-ci peut tout aussi bien être déployé sur une passerelle réseau, un serveur ou un simple poste de travail. Les règles de filtrage de Netfilter s'adaptent à chaque situation :

- Installé sur une passerelle, Netfilter protègera essentiellement les flux de transit et assurera des opérations de translation d'adresses, de marquage de paquets, de contrôle de la volumétrie, etc.
- Installé sur un serveur, Netfilter protègera essentiellement les flux entrants destinés à des applications locales comme des bases de données, des serveurs Web, des serveurs de messagerie.

Installé sur un poste de travail, Netfilter contrôlera les flux sortants (par PID, UID, GID, nom du processus) tout en bloquant les connexions entrantes non explicitement autorisées.

d. Description des hypothèses sur l'environnement

Netfilter-iptables doit être installé sur un système *sain*, correctement mis à jour, en particulier concernant les correctifs liés à la sécurité. Il convient également de sécuriser le système, par désactivation des services et partages inutiles.

Les administrateurs et les utilisateurs de Netfilter-iptables sont considérés comme non hostiles.

- Audit

Il est supposé que l'administrateur consulte régulièrement les événements d'audit générés par Netfilter-Iptables.

- Alarme

Il est supposé que l'administrateur de sécurité analyse et traite les alarmes de sécurité générées et remontées par Netfilter-Iptables.

- Administrateur

Les administrateurs sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

- Local

Les équipements contenant les services de Netfilter-Iptables (firewall et équipements d'administration), ainsi que tous supports contenant les biens sensibles de Netfilter-Iptables (papier, disquettes, sauvegardes,...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

- Maitrise de la configuration

L'administrateur dispose des moyens de contrôler la configuration matérielle et logicielle de Netfilter-Iptables par rapport à un état de référence, ou de la regénérer dans un état sûr. Cette hypothèse s'étend à la maîtrise du bien sensible "Politique de filtrage" du fait que Netfilter-Iptables ne peut à elle seule garantir son intégrité.

- Maitrise du système

Le système d'exploitation supportant Netfilter-Iptables est correctement administré et configuré. En particulier, les accès aux différents composants de Netfilter-Iptables ne sont accessibles qu'aux seuls utilisateurs autorisés.

e. Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit**.**

La plupart sinon toutes les distributions majeures du système open source Gnu/Linux intègrent d'origine le pare-feu Netfilter-iptables. Cependant la cible de sécurité spécifie que le noyau doit être dans sa version d'origine 2.6.27, disponible sur le site http://www.kernel.org.

f. Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts…) et de leur rôle particulier dans l'utilisation du produit.

Le contexte d'emploi organisationnel et relatif au personnel pour le produit est le suivant :

- un ou plusieurs administrateurs dont le rôle est de procéder aux opérations d'installation, de configuration et de maintenance. Ces administrateurs disposent de droits d'accès privilégiés au système d'exploitation Gnu/Linux : compte *root* ou similaire.
- des utilisateurs non privilégiés du système dont les possibilités se limitent à de simples tests, voire à l'obtention d'informations non sensibles sur la configuration du pare-feu.

g. Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concernées par l'évaluation.

Les fonctions de sécurité inclues 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).

3. Description de l'environnement technique dans lequel le produit doit fonctionner

a. Matériel compatible ou dédié

Aucune contrainte matérielle particulière.

b. Système d'exploitation retenu

Noyau Gnu/Linux v2.6.27

4. Description des biens sensibles que le produit doit protéger

Le produit contribue à protéger des biens utilisateurs de type informations et services du réseau protégé, par le filtrage des flux susceptibles d'accéder ou de modifier ces biens.

Les biens sensibles de Netfilter-iptables (politique de filtrage, journaux d'évènements, etc) doivent être protégés par le système d'exploitation sous lequel s'exécute Nefilter-iptables.

5. Description des menaces

Les différents agents menaçants sont :
- les attaquants internes : tout utilisateur autorisé du réseau protégé ;
- les attaquants externes : toute personne extérieure au réseau protégé.

Par hypothèse, les administrateurs ne sont pas considérés comme des attaquants potentiels.

Description des menaces :

- Un attaquant externe transmet un flux non autorisé sur le SI protégé par le firewall.
- Un attaquant interne transmet des flux non autorisés depuis le SI protégé.
- Un attaquant interne ou externe provoque un déni de service sur le firewall avec comme conséquences :
    - Les flux légitimes ne peuvent plus transiter d'un réseau à l'autre.
    - Le firewall ne peut plus assurer ses fonctions de filtrage et laisse transiter des flux interdits.

6. Description des fonctions de sécurité du produit

La fonctionnalité principale de Netfilter-Iptables 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-Iptables) :

- Application d'une politique de filtrage ;
- Audit/journalisation des flux IP.

Fonctions de sécurité de Netfilter-Iptables **:**

- Application de la politique de filtrage

Netfilter-Iptables est un firewall 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-Iptables 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-Iptables 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-Iptables 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-Iptables. 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 évènements, ce qui peut prévenir certaines formes d'attaque par déni de service.