Firewall: Architecture et déploiement

NetFilter par l'exemple

Ce document fait partie intégrante du stage "Firewall: Architecture et déploiement" mis en place au CFI, Fort de Vanves. Il permet la découverte du fonctionnement d'un filtre de paquets au travers de NetFilter, implémentation phare d'un filtre de paquets sous Linux. L'étude de différentes architectures d'interconnexion permet d'aborder très succintement les autres composants utilisés pour effectuer un filtrage, notamment au niveau applicatif.

Jean Baptiste Favre (jean.baptiste.favre@gmail.com)
24 mars 2006

Table des matières

- Chapitre I - Introduction

Il vaut mieux pomper même s'il ne se passe rien que risquer qu'il se passe quelque chose de pire en ne pompant pas

Devise Shadock

La sécurité ne révèle sa valeur qu'en cas de problème. Fort de ce constat, il vaut mieux appliquer de la sécurité avant d'être attaqué afin de, au minimum, limiter les dégâts. Après, il sera trop tard...

I.1 Présentation

Ce document a été rédigé dans le cadre du cours « Firewall: architecture et déploiement » du Centre de Formation à l'Informatique (CFI) du Ministère de la Défense.

Il s'agit d'une mise en situation pratique des différents points abordés durant le stage.

Le filtre de paquets retenu pour l'ensemble du document est NetFilter sur une plate-forme Linux. Les tests ont été réalisés sur Debian GNU/Linux mais devraient être transposables en l'état ou presque sur n'importe quelle autre distribution.

Il est possible, à l'avenir que j'aborde l'utilisation de PacketFilter, l'implémentation d'un filtre de paquets sous OpenBSD, pour une architecture particulière. Ceci n'est toutefois pas à l'ordre du jour actuellement.

I.1.1 Avertissements

- Le principe retenu dans tout ce document est celui d'une interconnexion avec Internet. Il va de soi que les architectures présentées peuvent être appliquées sans problème à des interconnexions différentes. Les interconnexions présentées dans ce document se veulent réalistes en fonction des situations envisagées.
- Ce document n'a pas la prétention de l'exhaustivité. Il est même possible, voire probable, que de nombreuses coquilles soient présentes. Sans doute seront-elles apparues dans le feu de l'action ;-)
- Ce document se focalise sur le filtre de paquets. Pour cette raison, la configuration des autres composants des architectures ne sera pas ou peu évoquée. De toute façon, il existe suffisamment de documentation librement disponible sur Internet pour contenter votre soif d'apprendre. Peut-être dans une version future... ou pas.
- Les puristes pourront toujours critiquer la configuration de telle ou telle architecture en arguant du fait qu'on peut mieux faire. C'est vrai. Toutefois, le but est d'obtenir une progression régulière tout au long du document. Pour ce faire, nous ferons l'impasse sur certaines fonctionnalités avancées du filtre de paquets lorsque l'architecture envisagée et l'analyse du risque sensément associée ne l'imposent pas.
- A partir des diagramme des flux évoqués pour chaque architecture, les règles de configuration des filtres de paquets seront données « en français ». Le but est, d'une part, de faciliter la compréhension de celles-ci, et d'offrir au lecteur la possibilité de s'entraîner en les traduisant en commandes `iptables` d'autre part.

I.2 Audience du document et pré-requis

I.2.1 Public

Essentiellement destiné aux personnels ayant suivi le stage « Firewall, Architecture et déploiement » du CFI pour leur permettre de prolonger la formation, ce document est également adapté à toute personne désireuse de s'informer sur le filtrage de paquets.

I.2.2 Pré-requis

I.2.2.1 Réseaux

Le filtrage de paquet peut rapidement devenir très pointu. De fait, une bonne connaissance du fonctionnements des réseaux TCP/IP est conseillée. Des rappels dans ce domaine étant effectués durant le stage, ce point est donc considéré comme acquis.

I.2.2.2 NetFilter

La description de l'architecture et du fonctionnement de NetFilter est donnée lors du stage. Cette partie est également considérée comme acquise. On pourra cependant se reporter au document « Firewall: Architecture et déploiement, Présentation de NetFilter »[1] pour voir ou revoir le fonctionnement de NetFilter. Un aide-mémoire est disponible en Annexe C. : Aide-mémoire NetFilter - Iptables.

I.2.2.3 Système d'exploitation

Les filtres de paquets mis en œuvre dans ce document reposent sur un système d'exploitation GNU/Linux. Une bonne connaissance du fonctionnement, de la mise en place et de l'administration de ce type de système est requise.

Ce document ce focalisant sur le filtrage de paquets et non l'administration Linux, il est acquis que le lecteur sait installer, configurer et sécuriser un système d'exploitation de type GNU/Linux.

I.3 Licence

Ce document (y compris les exemples et portions de code) est placé sous la licence « GNU Public Documentation License » conformément à l'indication donnée en page 2.

Les présentations associées à ce stage **ne sont pas** actuellement placées sous cette licence : ils utilisent en effet des éléments graphiques appartenant à la Marine Nationale.

Une version expurgée des éléments sous licence propriétaire sera diffusée dès que possible.

I.4 Versions du document

La dernière version de ce document est disponible au téléchargement sur mon site personnel:

http://jean.baptiste.favre.free.fr/_cfi/

Il ne sera pas fait d'annonce particulière lors de la sortie d'une nouvelle version.

I.5 Historique des versions

Date	*Numéro de version*	*Observations*
03 mars 2006	0.1	Rédaction initiale
30 mars 2006	0.5	Relecture et finalisation

1 A paraître.

- Chapitre II -
Interconnexion « Simple »

Pour bien faire, mille jours ne sont pas suffisants,
pour faire mal, un jour suffit amplement
Proverbe chinois

Nous commencerons notre plongée dans le monde merveilleux de Netfilter par l'étude d'une interconnexion simple. Ce type d'interconnexion, parfaitement adaptée à un usage domestique, se caractérise par de faibles exigences de sécurité et d'importants besoins de simplicité. Les moyens mis en place sont donc relativement limités. Voyons comment on peut, malgré tout, obtenir un niveau de sécurité acceptable.

II.1 Cible de l'architecture

Ce type d'architecture est destiné typiquement à une connexion Internet à domicile. Quelques machines, 4 maximum en général, se partagent un accès ADSL.

II.2 Contraintes

- Administration « zéro » ;
- Simplicité d'installation et de configuration ;
- Souplesse d'emploi pour éviter d'avoir à mettre les « mains dans le cambouis » à chaque installation d'une nouvelle application (par exemple, un jeu en réseau ou un logiciel de Peer to Peer[2]) ;
- Pas ou peu d'investissement en terme de matériel.

II.3 Choix techniques

II.3.1 Routeur seul

Il s'agit de l'interconnexion la plus simple qui soit. Les machines du réseau interne sont paramétrées avec une adresse IP conforme à la RFC1918, donc non routable sur Internet. Elles sont injoignables directement depuis Internet.

En revanche, aucun filtrage de paquet ne peut être effectué par défaut[3].

II.3.2 Partage de connexion sur un PC existant

Solution un peu plus élaborée, il devient alors possible de transformer une des machines du réseau local en routeur-filtrant. La machine est utilisée à la fois comme routeur et comme client.

Toutefois, ce type d'installation n'est absolument pas recommandé car cela augmente le risque de compromission de la machine : le principe de l'unicité de fonction n'est pas respecté.

II.3.3 Recyclage d'un « vieux » PC

Les systèmes d'exploitation, et notamment Microsoft Windows, évoluant rapidement, le matériel devient vite obsolète. Il est pourtant possible de recycler les « vieilleries » qui encombrent nos caves ou greniers en composants qui assureront la sécurité de nos interconnexions.

Ce type d'utilisation est le terrain de jeu favoris de diverses distribution Linux spécialisées dans le filtrage de paquet, par exemple IpCop. Cette distribution, à la fois légère et conviviale (administration au travers d'une interface Web) se contentera d'un vieux PC qui ne supporte pas les versions modernes de Windows[4] : un Pentium 266 avec 64 Mo de RAM fera l'affaire pour un réseau domestique. Il est bien entendu possible de se baser sur une distribution plus généraliste mais mieux maîtrisée.

II.4 Mise en œuvre

La solution routeur seul ne présentant aucun intérêt dans le cadre du stage, elle ne sera pas abordée. Les 2 solutions suivantes sont comparables en terme de fonctionnalités attendues, mais pas

2 Qu'il me soit permis de rappeler ici que seule l'utilisation que l'on fait de ces logiciels est illégale. Il n'est absolument pas interdit de récupérer une distribution Linux par l'intermédiaire de BitTorrent, bien au contraire.

3 Bien que les routeurs modernes proposent tous ce type de fonctionnalité, avec plus ou moins de bonheur et de simplicité.

4 A moins que cela ne soit l'inverse, allez savoir...

en terme de niveau de sécurité.

En l'occurrence, le choix se portera sur la solution « Recyclage d'un vieux PC ».

II.4.1 Diagramme de flux

Notre filtre de paquets devra:

- Interdire par défaut toute connexion entrante sur l'interface Internet, à l'exception de celles déjà initialisées (et donc, correspondant à des réponses)
- Filtrer les connexions sortant du filtre de paquets vers Internet
- Filtrer les connexions entrant dans le filtre de paquets en provenance du LAN
- Autoriser par défaut toutes les connexions sortantes des clients du LAN vers Internet.

II.4.2 Architecture

L'architecture de notre système est représentée ci contre. Le réseau local est protégé par un filtre de paquets placé en coupure.

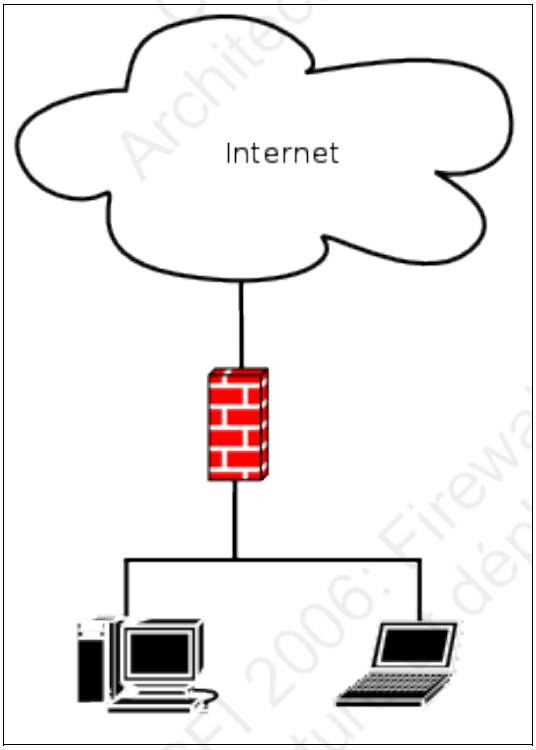


Figure 1: Architecture Simple

II.4.3 Configuration du filtre de paquets

Les règles de filtrage sont mises en place comme suit :

- Initialisation de Netfilter ;
- Politique par défaut :
  - ✔ `DROP` pour `INPUT`, `OUTPUT` et `FORWARD` ;
- Prise en compte des connexions déjà établies ;
- Autorisation de toutes les connexions arrivant sur l'interface `LAN` et à destination de l'interface `NET` ;
- Autorisation des connexions sortant du filtre de paquets :
  - ✔ à destination du serveur de mises à jour Internet sur le port `TCP/80`.
  - ✔ à destination des serveurs `DNS` du FAI en `UDP/53` ;
- Autorisation des connexions SSH (TCP/22) entrant sur le filtre de paquets par l'interface LAN pour les tâches d'administration du filtre de paquets.

II.5 Analyse de la solution et identification du risque résiduel

La configuration du filtre de paquets a pu être définie très rapidement. Bien évidemment, des problèmes potentiels subsistent. En voici quelques uns:

- Toutes les connexions sortantes sont autorisées. En cas de compromission d'une machine du LAN (virus mail par exemple), celle-ci a un accès plein et entier à Internet sans aucun contrôle ;
- Aucun filtrage n'est effectué au niveau applicatif. Ceci reporte, par exemple, l'examen anti-virus des mails sur les postes clients ;

- Tous les utilisateurs peuvent accéder à Internet (y compris « root » depuis le pare-feu).

Cette solution présente des vulnérabilités résiduelles relativement importantes[5]. Cependant, compte tenu de la cible désignée pour ce type d'architecture (cf II.1 Cible de l'architecture), la prise en compte de ce risque paraît disproportionnée avec les moyens disponibles pour le faire.

5 Il serait bien entendu possible de les corriger dès maintenant, au moins en partie. Cependant, on perdra alors en souplesse d'utilisation du système.

- Chapitre III - Interconnexion « sensible »

Citation de début de chapitre

Auteur de la citation

Après avoir étudié une interconnexion simple, sans réel besoin de sécurité, intéressons nous à présent à une interconnexion un peu plus sécurisée. Dans ce cas précis, on va chercher à contrôler ce qui entre, bien entendu, mais également ce qui sort. Un début de filtrage applicatif sera également mis en place.

III.1 Cible de l'architecture

Ce type d'interconnexion s'adresse au monde de l'entreprise, *a priori* une petite ou moyenne structure. L'accès internet s'effectue via une connexion de type ADSL.

III.2 Contraintes

D'ores et déjà, il est illusoire d'espérer obtenir un système qui vit tout seul. Le besoin de sécurité d'une entreprise, même petite, doit (ou plutôt devrait) l'inciter à investir suffisamment pour obtenir un système viable et fiable sur le long terme quitte à externaliser la prestation.

En l'occurrence, la seule contrainte retenue sera :

- Simplicité de configuration et d'administration[6]

III.3 Choix techniques

III.3.1 Filtre de paquets

C'est une quasi obligation. On ne peut se permettre en entreprise de se reposer sur un simple routeur.

Ce filtre de paquets peut être combiné sur un même socle matériel à des dispositifs d'analyse et de filtrage de flux applicatifs. C'est par exemple le cas de la plupart, pour ne pas dire la totalité, des "appliances" ou pare-feux matériels. Ces dispositifs peuvent se révéler particulièrement intéressants de par leur structure compacte. De plus, la maintenance, assurée par l'éditeur/intégrateur, peut être contractualisée.

III.3.2 Filtre applicatif séparé

Dans ce cas de figure, la nécessité de pouvoir analyser les flux applicatifs à la recherche de codes malveillants est très claire. Une entreprise, si petite soit-elle, possède des informations vitales pour sa survie. Leur divulgation, même suite à une attaque non intentionnelle, pourrait être une catastrophe pour l'entreprise.

Le fait de disposer de machines séparées peut se révéler particulièrement intéressant en fonction du type de trafic géré afin de maintenir des performances acceptables, même en cas de traitement de fichiers volumineux par l'anti-virus.

III.4 Mise en œuvre

III.4.1 Fonctionnalités

Les fonctionnalités à mettre en place sont:

- Filtrage des connexions ;
- Analyse des flux à la recherche de codes malicieux ;
- Mise en cache des documents les plus demandés.

III.4.2 Architecture

L'architecture de notre système est représentée ci-contre.

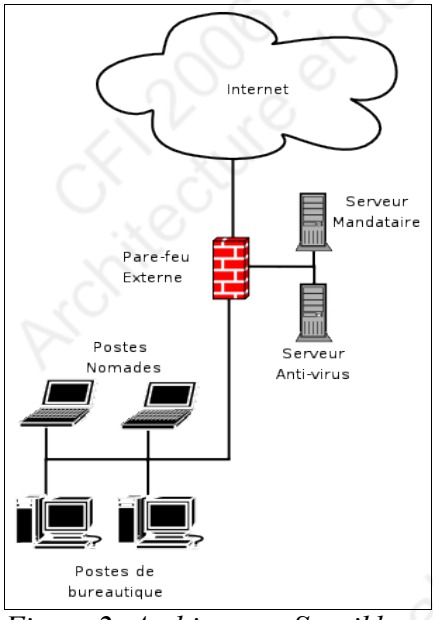


Figure 2: Architecture Sensible

6 Le risque associé à cette contrainte est la non-maîtrise du système. Ce risque peut être couvert en interne, c'est ce que nous ferons, ou transféré vers une autre entité, cas de l'externalisation. On peut également transférer un risque en contractant une assurance couvrant les dommages causés par la réalisation de ce risque.

La machine d'administration de la passerelle est installée dans le réseau local.

On voit apparaître le concept de DMZ. Ces zones particulières sont chargées de renforcer l'isolation du réseau interne vis-à-vis de l'extérieur en filtrant tout ou partie des flux qui la traversent. Les équipements situés dans une DMZ sont par définition plus exposés aux attaques. Leur rôle étant de protéger les clients situés sur le réseau interne, ils doivent être particulièrement surveillés et sécurisés.

Dans cet exemple, les requêtes HTTP et FTP des clients internes et leurs réponses des serveurs internet seront analysées par le serveur mandataire et l'anti-virus.

Il est possible de regrouper le serveur mandataire et l'anti-virus sur la même machine mais il ne s'agit pas nécessairement de la meilleure solution : l'anti-virus pourrait monopoliser les ressources de la machine pour analyser un fichier volumineux, ce qui grèverait les performances du serveur mandataire.

Il est enfin possible, et même conseillé, de programmer les mises à jour anti-virus de façon automatique de manière à profiter le plus rapidement possible de la meilleure protection.

Il arrive que la mise à jour provoque des faux-positifs (des fichiers sains détectés comme virus). Cela est en général dû à une base de signatures virales défectueuse. C'est gênant mais il vaut mieux risquer quelques faux-positifs de temps en temps que rater un vrai virus pourtant intégré dans la base de signatures.

III.4.3 Diagramme des flux

Les clients du LAN sont autorisés à:

- Effectuer des requêtes DNS vers les serveurs du FAI et eux seuls ;
- A envoyer et recevoir des mails vers et depuis les serveurs du FAI uniquement ;
- A visiter les sites Web ou effectuer des transferts de fichiers FTP au travers du serveur mandataire local. Ce dernier peut refuser l'accès aux données en fonctions de règles définies dans la politique de sécurité. Pour cela, tous les clients sont obligatoirement configurés pour utiliser le serveur mandataire ;
- La machine de l'administrateur est seule autorisée à se connecter sur le filtre de paquets ou les 2 serveurs en DMZ en utilisant le protocole SSH (TCP/22) pour réaliser les opérations d'administration.
- Le filtre de paquets et les serveurs en DMZ sont autorisés à effectuer des résolutions de nom sur les serveurs DNS du FAI seulement. Leur accès à Internet est limité aux sites diffusant les mises à jour du système ou de l'anti-virus.

III.4.4 Configuration du filtre de paquets

Les règles de filtrage sont mises en place comme suit :

- Initialisation de Netfilter ;
- Politique par défaut :
  - ✔ `DROP` pour `INPUT`, `OUTPUT` et `FORWARD` ;
- Prise en compte des connexions déjà établies ou en relation ;
- Autorisation du trafic sur l'interface de `loopback` ;
- Les flux `UDP/53` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du réseau local et à destination des serveurs `DNS` du FAI sont autorisés. Les autres sont enregistrés et interdits ;

- Les flux `TCP/21` ou `TCP/80` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du réseau local et à destination du serveur mandataire sont autorisés. Les autres sont enregistrés et interdits ;
- Les flux `TCP/25` ou `TCP/110` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du réseau local et à destination des serveurs `POP3` et `SMTP` du FAI sont autorisés. Les autres sont enregistrés et interdits ;
- Les flux `TCP/22` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance de la machine de l'administrateur et à destination des serveurs en `DMZ` sont autorisés ;
- Les flux `TCP/22` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance de la machine de l'administrateur et à destination du filtre de paquets sont autorisés ;
- Les flux `UDP/53` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) sortant du filtre de paquets à destination des serveurs `DNS` du FAI sont autorisés ;
- Les flux `TCP/80` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) sortant du filtre de paquets à destination du serveur de mises à jour système sont autorisés. Les autres sont enregistrés et interdits ;
- Les flux `TCP/21` ou `TCP/80` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance des serveurs de la `DMZ` et à destination d'Internet sont autorisés. ;

III.5 Analyse de la solution et identification du risque résiduel

- Les clients sont partiellement isolés d'Internet par une rupture de flux :
  - ✔ Les requêtes `HTTP` et `FTP` transitent obligatoirement par le serveur mandataire qui les soumettra d'une part à autorisation selon le principe de la liste noire (ou au contraire la liste blanche), et d'autre part à examen par l'anti-virus. Vis-à-vis d'Internet, c'est le serveur mandataire qui fait office de client.
- Les possibilités d'encapsulation dans des protocoles applicatifs autorisés sont limitées:
  - ✔ Les client du `LAN` ne peuvent effectuer de résolutions de noms de domaine sur d'autres serveurs `DNS` que ceux du FAI ;
  - ✔ Les clients du LAN ne peuvent utiliser les protocoles `POP3` et `SMTP` qu'avec les serveurs Mail du FAI ;
  - ✔ Le passage obligatoire par le serveur mandataire pour les protocoles `HTTP` et `FTP` limite les possibilités d'encaspulation `HTTP`.
- La gestion des mails pose plus de problèmes. La mise en place de solution de sécurité (anti-virus, anti-spam, ...) peut être contractualisée auprès du fournisseur d'accès. Néanmoins, le principal problème vient du fait que tous les clients peuvent sortir directement sur Internet. L'avantage du serveur mandataire dans ce cas de figure est que lui seul est directement exposé à Internet (limitation de la surface d'attaque).

Globalement, le niveau de sécurité est un peu plus élevé. On voit que les possibilités de contournement sont limitées. Pour autant, elles sont loin d'être inexistantes. Notamment, les logiciels de communication « modernes » pratiquent le tunneling HTTP qui est particulièrement délicat à contrer.

Néanmoins, le nombre relativement faible de machines dans le réseau local rend plus facile la maîtrise de leur configuration.

- Chapitre IV -
Interconnexion « Complexe »

Citation de début de chapitre

Auteur de la citation

Notre interconnexion monte encore en puissance. Le filtrage de niveau 7 (niveau applicatif) devient indispensable et sera donc généralisé.

IV.1 Cible de l'architecture

Dans ce cas de figure, l'on s'adresse à une structure conséquente. Celle-ci tient à maîtriser l'ensemble de son architecture d'interconnexion. Tous les flux amenés à la traverser devront être étudiés.

IV.2 Contraintes

- Administration centralisée
- Journalisation centralisée
- Seules les machines de l'entreprise ont accès au réseau

IV.3 Choix techniques

IV.3.1 Administration centralisée

L'entreprise a fait le choix de ne pas mettre en place de réseau d'administration dédié. Pour maintenir tout de même un bon niveau de sécurité, les flux liés à l'administration seront protégés par `IPSEC-ESP`.

IV.3.2 Journalisation centralisée

Afin de faciliter la tâche de l'administrateur de la sécurité, la journalisation des machines et équipements du réseau d'interconnexion est centralisée. Un serveur Syslog est donc mis en place et communique avec les autres composants de l'infrastructure grâce à `IPSEC-AH`.

Le serveur `Syslog` fait également office de serveur de temps afin de synchroniser les équipements, ce qui facilite d'autant la consolidation et l'analyse des journaux d'évènements.

Ces dernières, régulièrement effectuées, permettent d'assurer un suivi de l'état de santé de notre système et de dresser un tableau de bord à destination de l'échelon de décision.

IV.3.3 Limitation d'accès au réseau

La mise en place et l'utilisation du « `Trap & close` » permet de n'autoriser l'accès au réseau qu'aux machines identifiées, en se basant sur leur adresse MAC.

De même, on peut envisager d'effectuer un filtrage basé sur l'adresse MAC, en plus du filtrage IP, au niveau des filtres de paquets afin de détecter la connexion d'un équipement non autorisé.

IV.4 Mise en œuvre

IV.4.1 Fonctionnalités

- Filtrage des connexions entrantes ;
- Filtrage des connexions sortantes ;
- Mise en place de serveurs mandataires pour tous les protocoles applicatifs utilisés[7] :
  - ✔ POP ;
  - ✔ SMTP ;
  - ✔ HTTP ;
  - ✔ FTP ;

7 Ces serveurs mandataires seront installés sur le réseau local d'une part, mais également en DMZ

- ✔ DNS.

IV.4.2 Architecture

L'architecture de notre système est conforme à la figure ci-contre.

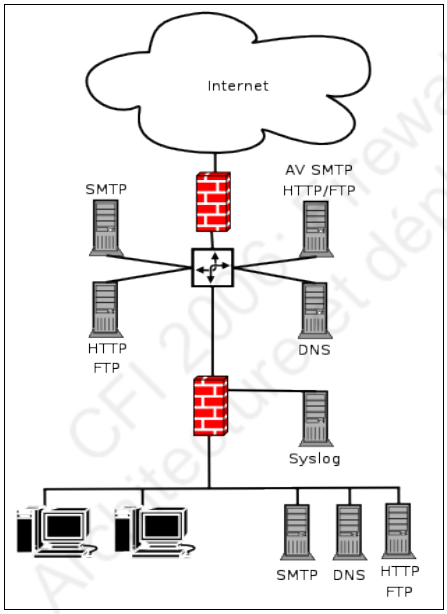


Figure 3: Architecture Complexe

- Les clients ne peuvent accéder directement à Internet. Ils sont obligés de passer par les serveurs mandataires du réseau local. Ceux-ci retransmettent les requêtes aux serveurs mandataires situés en `DMZ`. Ces derniers ont seuls accès à Internet.
- Les mails sortants sont envoyés par les serveurs mandataires et passés à l'anti-virus de la `DMZ`. Une analyse anti-virus est effectuée contractuellement sur le serveur du FAI, au niveau de la `DMZ` ainsi que, bien entendu, au niveau du client. De préférence, on cherchera à utiliser des anti-virus différents.
- Les requêtes `HTTP` et `FTP` sont effectuées par les clients vers les serveurs mandataires locaux. Un filtrage des requêtes est effectué en fonction de différents critères. Comme d'habitude, le contenu des requêtes et réponses est analysé par le serveur anti-virus de la `DMZ`. Le serveur mandataire du réseau local met en cache les réponses.
- La journalisation est assurée par le serveur `Syslog` situé dans une autre `DMZ`. Ce serveur regroupe tous les enregistrements des serveurs mandataires, internes comme externes et des filtres de paquets. Toutes les connexions sont protégées en intégrité par `IPSEC/AH`[8]. Il a été placé dans une `DMZ` spéciale pour le protéger d'attaques éventuelles provenant de la `DMZ` externe. ***En revanche, il est inconcevable de placer ce type de machine sur le réseau local***[9]***.***
- Enfin, l'administration de la passerelle d'interconnexion[10] est assurée à partir d'une machine unique, située dans le réseau interne. Toutes les connexions sont protégées par IPSEC/ESP.

IV.4.3 Diagramme des flux

Les exemples de diagramme de flux sont donnés ici pour les connexions des clients du réseau local vers Internet. Il est évidemment nécessaire de les adapter au contexte.

IV.4.3.1 Protocole DNS

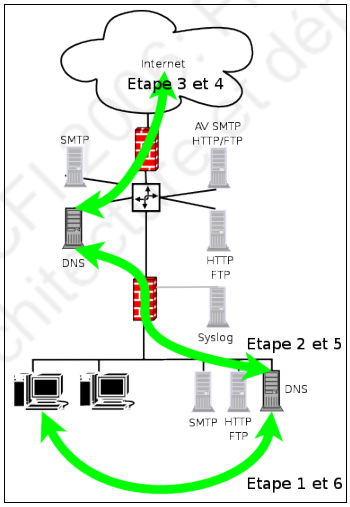


Figure 4: Flux DNS

- ***Étape 1*** : le client émet la requête vers le serveur mandataire interne. Le serveur mandataire regarde si la réponse se trouve en cache ;
- ***Étape 2*** : la réponse n'est pas en cache. Le serveur mandataire transmet la requête au serveur mandataire en

8 Il serait bien entendu possible de les protéger également en confidentialité en utilisant les fonctionnalités de chiffrement d'IPSEC. Néanmoins, l'analyse de risque a conclu au faible besoin en confidentialité pour la partie journalisation, au contraire de l'intégrité dont le besoin est jugé très élevé. De plus, cela permet de distinguer les flux liés à la journalisation de ceux liés à l'administration.

9 car cela créerait une route d'entrée vers l'intérieur, ce qui va à l'encontre des principes élémentaires de sécurité.

10 Les machines du réseau local, hors proxies, sont administrées « classiquement » par la machine « de bureautique » de l'administrateur.

DMZ ;

- ***Étape 3*** : le serveur mandataire de la DMZ effectue la requête sur Internet ;
- ***Étape 4*** : la réponse arrive du serveur Internet ;
- ***Étape 5*** : l'information est transmise au serveur mandataire interne ;
- ***Étape 6*** : le client reçoit la réponse du serveur mandataire interne.

IV.4.3.2 Protocoles HTTP/FTP

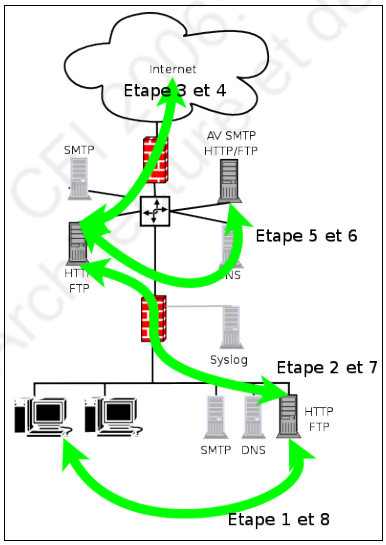


Figure 5: Flux HTTP et FTP

- ***Étape 1*** : le client émet la requête vers le serveur mandataire interne. Le serveur mandataire renvoie la ressource en cache si elle existe ;
- ***Étape 2*** : la ressource n'est pas en cache. Le serveur mandataire transmet la requête au serveur mandataire en DMZ. Celui-ci détermine la légitimité de la requête au regard des critères dont il dispose ;
- ***Étape 3*** : la requête est jugée légitime. Le serveur mandataire de la DMZ effectue la requête sur Internet ;
- ***Étape 4*** : la réponse arrive du serveur Internet ;
- ***Étape 5*** : le contenu de la réponse est transmis au serveur anti-virus de la DMZ pour analyse ;
- ***Étape 6*** : le serveur anti-virus renvoie le contenu en cas d'analyse négative (ou la réponse nettoyée dans le cas d'une page HTML par exemple) ;
- ***Étape 7*** : l'information est transmise au serveur mandataire interne ;
- ***Étape 8*** : le client reçoit la réponse du serveur mandataire interne.

IV.4.3.3 Protocole SMTP

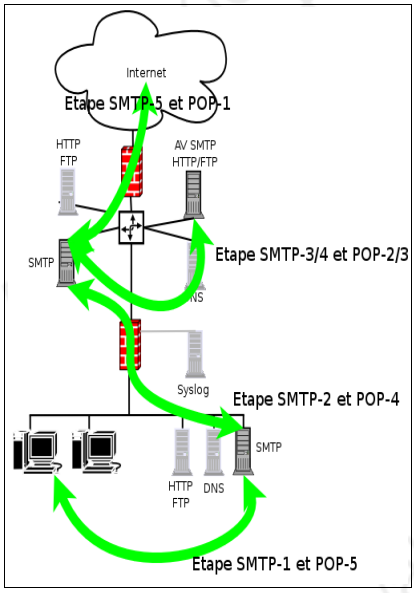


Figure 6: Flux SMTP et POP

- ***Étape 1*** : le client envoie le mail au serveur mandataire interne ;
- ***Étape 2*** : le serveur mandataire transmet le mail au serveur mandataire en DMZ ;
- ***Étape 3*** : le serveur mandataire de la DMZ fait analyser le courrier par l'anti-virus de la DMZ ;
- ***Étape 4*** : si l'analyse est négative, le mail est renvoyé au serveur mandataire ;
- ***Étape 5*** : le serveur mandataire envoie le mail sur Internet

IV.4.3.4 Protocole POP3

- ***Étape 1*** : le serveur mandataire en DMZ récupère les courriers stockés sur le serveur du FAI ;
- ***Étape 2*** : le serveur mandataire de la DMZ fait analyser le courrier par l'anti-virus de la DMZ ;
- ***Étape 3*** : le serveur anti-virus renvoie le mail au serveur mandataire de la DMZ en cas d'analyse négative. Celui-ci le stocke en local ;

- ***Étape 4*** : le serveur mandataire du réseau local récupère les mails stockés sur le serveur mandataire de la `DMZ` et les stocke en local ;
- ***Étape 5*** : les clients viennent chercher les mails.

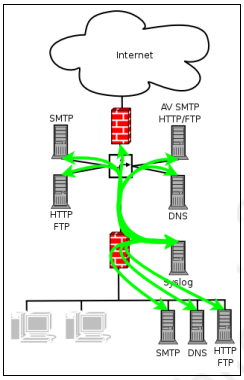


Figure 7: Flux Syslog IPSEC-AH

IV.4.3.5 Flux de journalisation[11]

Les flux de journalisation `Syslog` (`UDP/514`) sont protégés en intégrité par `IPSEC/AH`.

- ***Étape 1*** : Chaque serveur mandataire de la `DMZ` externe négocie une clef `IPSEC` avec le serveur `Syslog` ;
- ***Étape 1bis*** : Chaque serveur mandataire du réseau local négocie une clef `IPSEC` avec le serveur `Syslog` ;
- ***Étape 2*** : Chaque serveur mandataire de la `DMZ` externe envoie ses données de journalisation au serveur `Syslog` ;
- ***Étape 2bis*** : Chaque serveur mandataire du réseau local envoie ses données de journalisation au serveur `Syslog`.

IV.4.3.6 Flux d'administration[12]

Les flux d'administration `SSH` (`TCP/22`) sont protégés par `IPSEC/ESP`.

- ***Étape 1*** : La machine d'administration négocie une clef `IPSEC` avec chaque serveur mandataire ;
- ***Étape 2*** : La machine d'administration se connecte à la machine à administrer via `SSH` (`TCP/22`).
- ***Étape 2bis*** : La machine d'administration se connecte au serveur `Syslog` pour l'analyse des journaux via `SSH` (`TCP/22`).

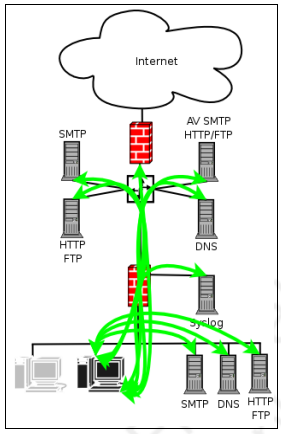


Figure 8: Flux Admin IPSEC-ESP

IV.4.4 Configuration des filtres de paquets

Il est possible, pour ne pas dire conseillé, d'utiliser intensivement les chaînes utilisateur. Elles serviront à répartir les règles, ce qui facilitera l'analyse[13].

IV.4.4.1 Filtre de paquets Interne

Les règles de filtrage sont mises en place comme suit :

- Initialisation de `Netfilter` ;
- Politique par défaut :
  - ✔ `DROP` pour `INPUT`, `OUTPUT` et `FORWARD` ;
- Prise en compte des connexions déjà établies ou en relation ;
- Autorisation du trafic sur l'interface de `loopback` ;

11 Bien que peu évident sur le schéma, le filtre de paquets interne envoie également ses informations de journalisation au serveur Syslog.
12 Dans le même esprit, le filtre de paquet dialogue naturellement avec la machine d'administration.
13 Exemple pour la négociation des clefs IPSEC: tout le trafic UDP/500 est envoyé dans la chaîne UDP_500. Dans cette chaîne, on vérifiera que la provenance et la destination du trafic est autorisée (une règle par adresse IP de serveur). Cela permettra également une journalisation avec un préfixe et un niveau de criticité particuliers, par exemple "Illegal IKE Trafic" avec criticité maximum.

- ***Négociation des clefs IPSEC :*** Les flux `UDP/500` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance de tous les serveurs mandataires et filtres de paquets, du réseau local et de la `DMZ`, à destination du serveur `Syslog` de la `DMZ` interne sont autorisés. Les autres sont enregistrés et interdits ;

  Négociation des clefs IPSEC : Les flux `UDP/500` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance de la machine d'administration et à destination de tous les serveurs mandataires, filtres de paquets et serveur Syslog, du réseau local et de la `DMZ`, sont autorisés. Les autres sont enregistrés et interdits ;

- ***Flux de journalisation :*** Les flux utilisant le protocole `IPSEC-AH` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance de la `DMZ` externe et à destination de la `DMZ` interne sont autorisés ;

  Flux de journalisation : Les flux utilisant le protocole `IPSEC-AH` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du réseau local et à destination de la `DMZ` interne sont autorisés ;

- ***Flux d'administration :*** Les flux utilisant le protocole `IPSEC-ESP` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du réseau interne et à destination du filtre de paquets lui-même ou d'un composant de la passerelle sont autorisés ;

  Flux SSH d'administration : Les flux `TCP/22` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en entrée du filtre de paquets et en provenance de la machine d'administration de la passerelle depuis le réseau local sont autorisés. Les autres sont enregistrés et interdits ;

- ***Flux DNS :*** Les flux `UDP/53` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du serveur mandataire `DNS` du réseau local et à destination du serveur mandataire `DNS` de la `DMZ` externe sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux FTP :*** Les flux `TCP/21` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du serveur mandataire `FTP` du réseau local et à destination du serveur mandataire `FTP` de la `DMZ` sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux HTTP :*** Les flux `TCP/80` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du serveur mandataire `HTTP` du réseau local et à destination du serveur mandataire `HTTP` de la `DMZ` sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux SMTP :*** Les flux `TCP/25` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du serveur mandataire `SMTP` du réseau local et à destination du serveur mandataire `SMTP` de la `DMZ` sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux POP :*** Le flux `TCP/110` non répertoriés dans la pseudo-table `CONNTRACK` (état `NEW`) en provenance du serveur mandataire `POP3` du réseau local et à destination du serveur mandataire `POP3` de la `DMZ` sont autorisés. Les autres sont enregistrés et interdits ;

IV.4.4.2 Filtre de paquets externe

Les règles de filtrage sont mises en place comme suit :

- Initialisation de Netfilter ;
- Politique par défaut :

  - ✔ DROP pour INPUT, OUTPUT et FORWARD ;

- Prise en compte des connexions déjà établies ou en relation ;
- Autorisation du trafic sur l'interface de loopback ;
- ***Négociation des clefs IPSEC :*** Les flux UDP/500 non répertoriés dans la pseudo-table CONNTRACK (état NEW) en sortie du filtre de paquets et à destination du serveur Syslog de la DMZ interne sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux de journalisation :*** Les flux UDP/514 non répertoriés dans la pseudo-table CONNTRACK (état NEW) en sortie du filtre de paquets et à destination du serveur Syslog de la DMZ interne sont autorisés. Les autres sont enregistrés et interdits ;

  Flux de journalisation : Les flux utilisant le protocole IPSEC-AH non répertoriés dans la pseudo-table CONNTRACK (état NEW) en sortie du filtre de paquets et à destination du serveur Syslog de la DMZ interne sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux d'administration :*** Les flux utilisant le protocole IPSEC-ESP non répertoriés dans la pseudo-table CONNTRACK (état NEW) en entrée du filtre de paquets et à destination de la machine d'administration du réseau local sont autorisés. Les autres sont enregistrés et interdits ;

  w Les autres sont enregistrés et interdits ;
- ***Flux DNS :*** Les flux UDP/53 non répertoriés dans la pseudo-table CONNTRACK (état NEW) en provenance du serveur mandataire DNS de la DMZ externe et à destination des serveurs DNS du FAI sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux FTP :*** Les flux TCP/21 non répertoriés dans la pseudo-table CONNTRACK (état NEW) en provenance du serveur mandataire FTP de la DMZ et à destination du port TCP/21 de n'importe quelle machine sur Internet sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux HTTP :*** Les flux TCP/80 non répertoriés dans la pseudo-table CONNTRACK (état NEW) en provenance du serveur mandataire HTTP de la DMZ et à destination du port TCP/80 de n'importe quelle machine sur Internet sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux SMTP :*** Les flux TCP/25 non répertoriés dans la pseudo-table CONNTRACK (état NEW) en provenance du serveur mandataire SMTP de la DMZ et à destination du port TCP/25 de n'importe quelle machine sur Internet sont autorisés. Les autres sont enregistrés et interdits ;
- ***Flux POP :*** Le flux TCP/110 non répertoriés dans la pseudo-table CONNTRACK (état NEW) en provenance du serveur mandataire POP3 de la DMZ et à destination du port TCP/110 des serveurs de mail du FAI sont autorisés. Les autres sont enregistrés et interdits ;

IV.5 Analyse de la solution et identification du risque résiduel

On voit que les connexions sont toujours initialisées dans le sens « réseau de confiance le plus haut vers réseau de moindre confiance ». C'est un principe absolu en matière de sécurité réseau. Si vous décidez de ne retenir qu'une chose après la lecture de ce document, faites en sorte que ce soit ce principe.

Problèmes résiduels:

- Le filtrage anti-spam s'effectue toujours au niveau du client. Ceci n'est pas problématique tant que la structure n'est pas trop imposante. Dans le cas contraire, on risque d'une part d'avoir une charge réseau non négligeable, et d'autre part de compliquer inutilement le paramétrage anti-spam du système. Un filtre anti-spam centralisé est plus facile à maintenir. Néanmoins, on estime ici que le besoin n'est pas clairement avéré.
- Les mails, rapatriés du serveur du FAI, transitent par la `DMZ` externe. Ils y restent stockés tant que le serveur de mail du réseau local ne les récupère pas. Il est donc important de programmer la récupération de façon régulière afin de limiter le temps d'attente dans la `DMZ` externe. Une autre solution consiste à isoler le serveur de mails dans sa propre `DMZ` afin de le protéger, lui et les mails stockés.
- La disponibilité de l'interconnexion est liée à la disponibilité du FAI. Il peut être indispensable d'envisager, en fonction du besoin, une redondance de l'interconnexion.
- Il n'existe aucun dispositif de surveillance « temps-réel ». Les `IDS-IPS` permettent une détection, et donc une réaction plus rapide en cas de problème mais demandent une veille 24h/24 par du personnel spécialisé pour être réellement efficaces.

- Chapitre V - Conclusion

Il est clair que le risque zéro n'existe pas. En être convaincu est déjà un grand pas vers une meilleure sécurité. Cela vous permettra d'affronter le plus sereinement possible les différentes étapes de la mise en œuvre d'une architecture d'interconnexion sécurisée.

Les scénarios envisagés nous ont permis d'appréhender progressivement la mise œuvre d'un dispositif de filtrage de paquets.

Le niveau de sécurité atteint dans les différents cas de figure est, bien entendu, fonction du besoin de sécurité identifié. Il est important de comprendre que celui-ci ne peut être correctement défini qu'au terme d'une analyse de risque cohérente. Cette démarche s'inscrit dans celle, plus globale, de la gestion du risque.

Les logiciels libres n'ont pas à rougir devant leurs concurrents commerciaux[14], bien au contraire. Leur disponibilité constitue même, d'après moi, un avantage indéniable:

- Il s'agit souvent de produits de qualité et ils sont gratuits. Voilà un sacré challenge à relever pour les concurrents payants.
- Leur diffusion Open-Source permet une modularité quasi infinie. Cette modularité permet une adaptation maximum au besoin, ceci au prix, il est vrai, d'un investissement, humain notamment, plus conséquent.

Tout a un prix, y compris et peut-être surtout la sécurité. Le vrai problème consiste à chiffrer les investissements nécessaires de façon raisonnable et réaliste.

Afin d'élargir le périmètre de réflexion, le lecteur curieux pourra trouver quelques pistes de réflexion et pointeurs divers à l'Annexe D. : Pour aller plus loin.

14 Certains produits du commerce, notamment des pare-feux matériels, s'appuient d'ailleurs sur les logiciels libres.

Annexes

Annexe A. : Licence Creative Commons

Paternité - Pas d'Utilisation Commerciale - Partage Des Conditions Initiales A l'Identique 2.0

Creative Commons n'est pas un cabinet d'avocats et ne fournit pas de services de conseil juridique. La distribution de la présente version de ce contrat ne crée aucune relation juridique entre les parties au contrat présenté ci-après et Creative Commons. Creative Commons fournit cette offre de contrat-type en l'état, à seule fin d'information. Creative Commons ne saurait être tenu responsable des éventuels préjudices résultant du contenu ou de l'utilisation de ce contrat.

Contrat

L'Oeuvre (telle que définie ci-dessous) est mise à disposition selon les termes du présent contrat appelé Contrat Public Creative Commons (dénommé ici « CPCC » ou « Contrat »). L'Oeuvre est protégée par le droit de la propriété littéraire et artistique (droit d'auteur, droits voisins, droits des producteurs de bases de données) ou toute autre loi applicable. Toute utilisation de l'Oeuvre autrement qu'explicitement autorisée selon ce Contrat ou le droit applicable est interdite.

L'exercice sur l'Oeuvre de tout droit proposé par le présent contrat vaut acceptation de celui-ci. Selon les termes et les obligations du présent contrat, la partie Offrante propose à la partie Acceptante l'exercice de certains droits présentés ci-après, et l'Acceptant en approuve les termes et conditions d'utilisation.

1. Définitions

a. « **Oeuvre** » : oeuvre de l'esprit protégeable par le droit de la propriété littéraire et artistique ou toute loi applicable et qui est mise à disposition selon les termes du présent Contrat.
b. « **Oeuvre dite Collective** » : une oeuvre dans laquelle l'oeuvre, dans sa forme intégrale et non modifiée, est assemblée en un ensemble collectif avec d'autres contributions qui constituent en elles-mêmes des oeuvres séparées et indépendantes. Constituent notamment des Oeuvres dites Collectives les publications périodiques, les anthologies ou les encyclopédies. Aux termes de la présente autorisation, une oeuvre qui constitue une Oeuvre dite Collective ne sera pas considérée comme une Oeuvre dite Dérivée (telle que définie ci-après).
c. « **Oeuvre dite Dérivée** » : une oeuvre créée soit à partir de l'Oeuvre seule, soit à partir de l'Oeuvre et d'autres oeuvres préexistantes. Constituent notamment des Oeuvres dites Dérivées les traductions, les arrangements musicaux, les adaptations théâtrales, littéraires ou cinématographiques, les enregistrements sonores, les reproductions par un art ou un procédé quelconque, les résumés, ou toute autre forme sous laquelle l'Oeuvre puisse être remaniée, modifiée, transformée ou adaptée, à l'exception d'une oeuvre qui constitue une Oeuvre dite Collective. Une Oeuvre dite Collective ne sera pas considérée comme une Oeuvre dite Dérivée aux termes du présent Contrat. Dans le cas où l'Oeuvre serait une composition musicale ou un enregistrement sonore, la synchronisation de l'oeuvre avec une image animée sera considérée comme une Oeuvre dite Dérivée pour les propos de ce Contrat.
d. « **Auteur original** » : la ou les personnes physiques qui ont créé l'Oeuvre.
e. « **Offrant** » : la ou les personne(s) physique(s) ou morale(s) qui proposent la mise à disposition de l'Oeuvre selon les termes du présent Contrat.
f. « **Acceptant** » : la personne physique ou morale qui accepte le présent contrat et exerce des droits sans en avoir violé les termes au préalable ou qui a reçu l'autorisation expresse de l'Offrant d'exercer des droits dans le cadre du présent contrat malgré une précédente violation de ce contrat.
g. « **Options du Contrat** » : les attributs génériques du Contrat tels qu'ils ont été choisis par l'Offrant et indiqués dans le titre de ce Contrat : Paternité - Pas d'Utilisation Commerciale - Partage Des Conditions Initiales A l'Identique.

2. Exceptions aux droits exclusifs. Aucune disposition de ce contrat n'a pour intention de réduire, limiter ou restreindre les prérogatives issues des exceptions aux droits, de l'épuisement des droits ou d'autres limitations aux droits exclusifs des ayants droit selon le droit de la propriété littéraire et artistique ou les autres lois applicables.

3. Autorisation. Soumis aux termes et conditions définis dans cette autorisation, et ceci pendant toute la durée de protection de l'Oeuvre par le droit de la propriété littéraire et artistique ou le droit applicable, l'Offrant accorde à l'Acceptant l'autorisation mondiale d'exercer à titre gratuit et non exclusif les droits suivants :

a. reproduire l'Oeuvre, incorporer l'Oeuvre dans une ou plusieurs Oeuvres dites Collectives et reproduire l'Oeuvre telle qu'incorporée dans lesdites Oeuvres dites Collectives;
b. créer et reproduire des Oeuvres dites Dérivées;
c. distribuer des exemplaires ou enregistrements, présenter, représenter ou communiquer l'Oeuvre au public par tout procédé technique, y compris incorporée dans des Oeuvres Collectives;
d. distribuer des exemplaires ou phonogrammes, présenter, représenter ou communiquer au public des Oeuvres dites Dérivées par tout procédé technique;
e. lorsque l'Oeuvre est une base de données, extraire et réutiliser des parties substantielles de l'Oeuvre.

Les droits mentionnés ci-dessus peuvent être exercés sur tous les supports, médias, procédés techniques et formats. Les droits ci-dessus incluent le droit d'effectuer les modifications nécessaires techniquement à l'exercice des droits dans d'autres formats et procédés techniques. L'exercice de tous les droits qui ne sont pas expressément autorisés par l'Offrant ou dont il n'aurait pas la gestion demeure réservé, notamment les mécanismes de gestion collective obligatoire applicables décrits à l'article 4(e).

4. Restrictions. L'autorisation accordée par l'article 3 est expressément assujettie et limitée par le respect des restrictions suivantes :

a. L'Acceptant peut reproduire, distribuer, représenter ou communiquer au public l'Oeuvre y compris par voie numérique uniquement selon les termes de ce Contrat. L'Acceptant doit inclure une copie ou l'adresse Internet (Identifiant Uniforme de Ressource) du présent Contrat à toute reproduction ou enregistrement de l'Oeuvre que l'Acceptant distribue, représente ou communique au public y compris par voie numérique. L'Acceptant ne peut pas offrir ou imposer de conditions d'utilisation de l'Oeuvre qui altèrent ou restreignent les termes du présent Contrat ou l'exercice des droits qui y sont accordés au bénéficiaire. L'Acceptant ne peut pas céder de droits sur l'Oeuvre. L'Acceptant doit conserver intactes toutes les informations qui renvoient à ce Contrat et à l'exonération de responsabilité. L'Acceptant ne peut pas reproduire, distribuer, représenter ou communiquer au public l'Oeuvre, y compris par voie numérique, en utilisant une mesure technique de contrôle d'accès ou de contrôle d'utilisation qui serait contradictoire avec les termes de cet Accord contractuel. Les mentions ci-dessus s'appliquent à l'Oeuvre telle qu'incorporée dans une Oeuvre dite Collective, mais, en dehors de l'Oeuvre en elle-même, ne soumettent pas l'Oeuvre dite Collective, aux termes du présent Contrat. Si l'Acceptant crée une Oeuvre dite Collective, à la demande de tout Offrant, il devra, dans la mesure du possible, retirer de l'Oeuvre dite Collective toute référence au dit Offrant, comme demandé. Si l'Acceptant crée une Oeuvre dite Collective, à la demande de tout Auteur, il devra, dans la mesure du possible, retirer de l'Oeuvre dite Collective toute référence au dit Auteur, comme demandé. Si l'Acceptant crée une Oeuvre dite Dérivée, à la demande de tout Offrant, il devra, dans la mesure du possible, retirer de l'Oeuvre dite Dérivée toute référence au dit Offrant, comme demandé. Si l'Acceptant crée une Oeuvre dite Dérivée, à la demande de tout Auteur, il devra, dans la mesure du possible, retirer de l'Oeuvre dite Dérivée toute référence au dit Auteur, comme demandé.
b. L'Acceptant peut reproduire, distribuer, représenter ou communiquer au public une Oeuvre dite Dérivée y compris par voie numérique uniquement sous les termes de ce Contrat, ou d'une version ultérieure de ce Contrat comprenant les mêmes Options du Contrat que le présent Contrat, ou un Contrat Creative Commons iCommons comprenant les mêmes Options du Contrat que le présent Contrat (par exemple Paternité - Pas d'Utilisation Commerciale - Partage Des Conditions Initiales A l'Identique 2.0 Japon). L'Acceptant doit inclure une copie ou l'adresse Internet (Identifiant Uniforme de Ressource) du présent Contrat, ou d'un autre Contrat tel que décrit à la phrase précédente, à toute reproduction ou enregistrement de l'Oeuvre dite Dérivée que l'Acceptant distribue, représente

ou communique au public y compris par voie numérique. L'Acceptant ne peut pas offrir ou imposer de conditions d'utilisation sur l'Oeuvre dite Dérivée qui altèrent ou restreignent les termes du présent Contrat ou l'exercice des droits qui y sont accordés au bénéficiaire, et doit conserver intactes toutes les informations qui renvoient à ce Contrat et à l'avertissement sur les garanties. L'Acceptant ne peut pas reproduire, distribuer, représenter ou communiquer au public y compris par voie numérique l'Oeuvre dite Dérivée en utilisant une mesure technique de contrôle d'accès ou de contrôle d'utilisation qui serait contradictoire avec les termes de cet Accord contractuel. Les mentions ci-dessus s'appliquent à l'Oeuvre dite Dérivée telle qu'incorporée dans une Oeuvre dite Collective, mais, en dehors de l'Oeuvre dite Dérivée en elle-même, ne soumettent pas l'Oeuvre Collective, aux termes du présent Contrat.

c. L'Acceptant ne peut exercer aucun des droits conférés par l'article 3 avec l'intention ou l'objectif d'obtenir un profit commercial ou une compensation financière personnelle. L'échange de l'Oeuvre avec d'autres Oeuvres protégées par le droit de la propriété littéraire et artistique par le partage électronique de fichiers, ou par tout autre moyen, n'est pas considéré comme un échange avec l'intention ou l'objectif d'un profit commercial ou d'une compensation financière personnelle, dans la mesure où aucun paiement ou compensation financière n'intervient en relation avec l'échange d'Oeuvres protégées.
d. Si l'Acceptant reproduit, distribue, représente ou communique au public, y compris par voie numérique, l'Oeuvre ou toute Oeuvre dite Dérivée ou toute Oeuvre dite Collective, il doit conserver intactes toutes les informations sur le régime des droits et en attribuer la paternité à l'Auteur Original, de manière raisonnable au regard au médium ou au moyen utilisé. Il doit communiquer le nom de l'Auteur Original ou son éventuel pseudonyme s'il est indiqué ; le titre de l'Oeuvre Originale s'il est indiqué ; dans la mesure du possible, l'adresse Internet ou Identifiant Uniforme de Ressource (URI), s'il existe, spécifié par l'Offrant comme associé à l'Oeuvre, à moins que cette adresse ne renvoie pas aux informations légales (paternité et conditions d'utilisation de l'Oeuvre). Dans le cas d'une Oeuvre dite Dérivée, il doit indiquer les éléments identifiant l'utilisation l'Oeuvre dans l'Oeuvre dite Dérivée par exemple « Traduction anglaise de l'Oeuvre par l'Auteur Original » ou « Scénario basé sur l'Oeuvre par l'Auteur Original ». Ces obligations d'attribution de paternité doivent être exécutées de manière raisonnable. Cependant, dans le cas d'une Oeuvre dite Dérivée ou d'une Oeuvre dite Collective, ces informations doivent, au minimum, apparaître à la place et de manière aussi visible que celles à laquelle apparaissent les informations de même nature.
e. Dans le cas où une utilisation de l'Oeuvre serait soumise à un régime légal de gestion collective obligatoire, l'Offrant se réserve le droit exclusif de collecter ces redevances par l'intermédiaire de la société de perception et de répartition des droits compétente. Sont notamment concernés la radiodiffusion et la communication dans un lieu public de phonogrammes publiés à des fins de commerce, certains cas de retransmission par câble et satellite, la copie privée d'Oeuvres fixées sur phonogrammes ou vidéogrammes, la reproduction par reprographie.

5. Garantie et exonération de responsabilité

a. En mettant l'Oeuvre à la disposition du public selon les termes de ce Contrat, l'Offrant déclare de bonne foi qu'à sa connaissance et dans les limites d'une enquête raisonnable :
    i. L'Offrant a obtenu tous les droits sur l'Oeuvre nécessaires pour pouvoir autoriser l'exercice des droits accordés par le présent Contrat, et permettre la jouissance paisible et l'exercice licite de ces droits, ceci sans que l'Acceptant n'ait aucune obligation de verser de rémunération ou tout autre paiement ou droits, dans la limite des mécanismes de gestion collective obligatoire applicables décrits à l'article 4(e);
b. L'Oeuvre n'est constitutive ni d'une violation des droits de tiers, notamment du droit de la propriété littéraire et artistique, du droit des marques, du droit de l'information, du droit civil ou de tout autre droit, ni de diffamation, de violation de la vie privée ou de tout autre préjudice délictuel à l'égard de toute tierce partie.
c. A l'exception des situations expressément mentionnées dans le présent Contrat ou dans un autre accord écrit, ou exigées par la loi applicable, l'Oeuvre est mise à disposition en l'état sans garantie d'aucune sorte, qu'elle soit expresse ou tacite, y compris à l'égard du contenu ou de l'exactitude de l'Oeuvre.

6. Limitation de responsabilité. A l'exception des garanties d'ordre public imposées par la loi applicable et des réparations imposées par le régime de la responsabilité vis-à-vis d'un tiers en raison de la violation

des garanties prévues par l'article 5 du présent contrat, l'Offrant ne sera en aucun cas tenu responsable vis-à-vis de l'Acceptant, sur la base d'aucune théorie légale ni en raison d'aucun préjudice direct, indirect, matériel ou moral, résultant de l'exécution du présent Contrat ou de l'utilisation de l'Oeuvre, y compris dans l'hypothèse où l'Offrant avait connaissance de la possible existence d'un tel préjudice.

7. Résiliation

a. Tout manquement aux termes du contrat par l'Acceptant entraîne la résiliation automatique du Contrat et la fin des droits qui en découlent. Cependant, le contrat conserve ses effets envers les personnes physiques ou morales qui ont reçu de la part de l'Acceptant, en exécution du présent contrat, la mise à disposition d'Oeuvres dites Dérivées, ou d'Oeuvres dites Collectives, ceci tant qu'elles respectent pleinement leurs obligations. Les sections 1, 2, 5, 6 et 7 du contrat continuent à s'appliquer après la résiliation de celui-ci.
b. Dans les limites indiquées ci-dessus, le présent Contrat s'applique pendant toute la durée de protection de l'Oeuvre selon le droit applicable. Néanmoins, l'Offrant se réserve à tout moment le droit d'exploiter l'Oeuvre sous des conditions contractuelles différentes, ou d'en cesser la diffusion; cependant, le recours à cette option ne doit pas conduire à retirer les effets du présent Contrat (ou de tout contrat qui a été ou doit être accordé selon les termes de ce Contrat), et ce Contrat continuera à s'appliquer dans tous ses effets jusqu'à ce que sa résiliation intervienne dans les conditions décrites ci-dessus.

8. Divers

a. A chaque reproduction ou communication au public par voie numérique de l'Oeuvre ou d'une Oeuvre dite Collective par l'Acceptant, l'Offrant propose au bénéficiaire une offre de mise à disposition de l'Oeuvre dans des termes et conditions identiques à ceux accordés à la partie Acceptante dans le présent Contrat.
b. A chaque reproduction ou communication au public par voie numérique d'une Oeuvre dite Dérivée par l'Acceptant, l'Offrant propose au bénéficiaire une offre de mise à disposition du bénéficiaire de l'Oeuvre originale dans des termes et conditions identiques à ceux accordés à la partie Acceptante dans le présent Contrat.
c. La nullité ou l'inapplicabilité d'une quelconque disposition de ce Contrat au regard de la loi applicable n'affecte pas celle des autres dispositions qui resteront pleinement valides et applicables. Sans action additionnelle par les parties à cet accord, lesdites dispositions devront être interprétées dans la mesure minimum nécessaire à leur validité et leur applicabilité.
d. Aucune limite, renonciation ou modification des termes ou dispositions du présent Contrat ne pourra être acceptée sans le consentement écrit et signé de la partie compétente.
e. Ce Contrat constitue le seul accord entre les parties à propos de l'Oeuvre mise ici à disposition. Il n'existe aucun élément annexe, accord supplémentaire ou mandat portant sur cette Oeuvre en dehors des éléments mentionnés ici. L'Offrant ne sera tenu par aucune disposition supplémentaire qui pourrait apparaître dans une quelconque communication en provenance de l'Acceptant. Ce Contrat ne peut être modifié sans l'accord mutuel écrit de l'Offrant et de l'Acceptant.
f. Le droit applicable est le droit français.

Creative Commons n'est pas partie à ce Contrat et n'offre aucune forme de garantie relative à l'Oeuvre. Creative Commons décline toute responsabilité à l'égard de l'Acceptant ou de toute autre partie, quel que soit le fondement légal de cette responsabilité et quel que soit le préjudice subi, direct, indirect, matériel ou moral, qui surviendrait en rapport avec le présent Contrat. Cependant, si Creative Commons s'est expressément identifié comme Offrant pour mettre une Oeuvre à disposition selon les termes de ce Contrat, Creative Commons jouira de tous les droits et obligations d'un Offrant.

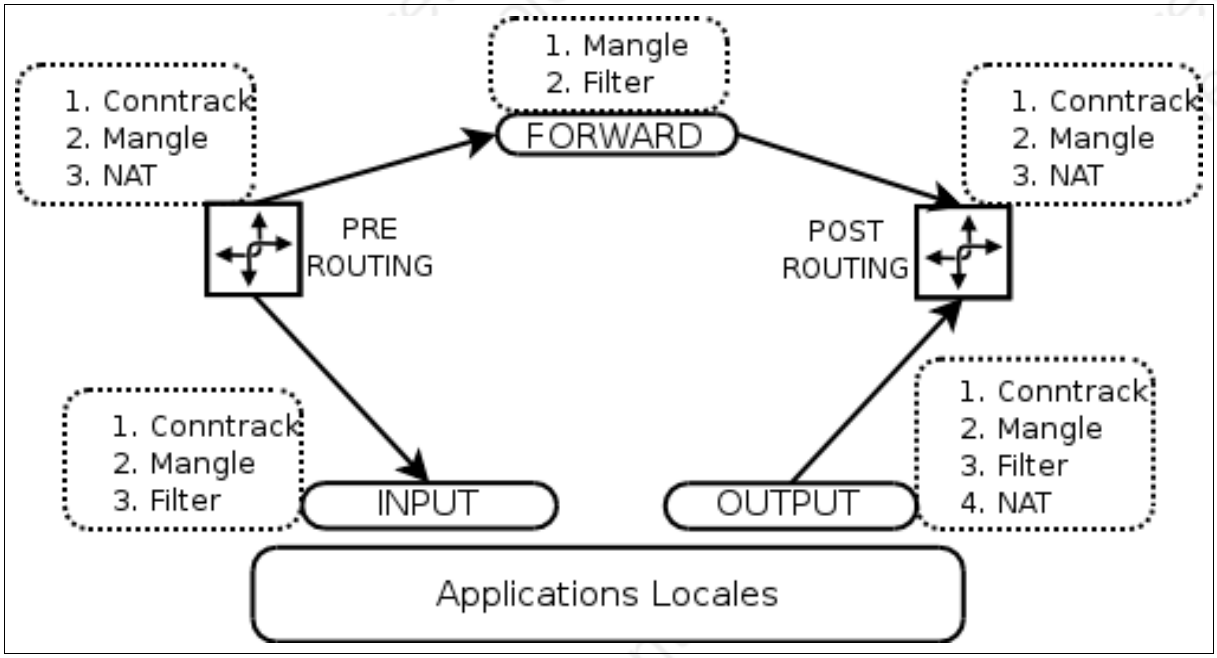
A l'exception des fins limitées à informer le public que l'Oeuvre est mise à disposition sous CPCC, aucune des parties n'utilisera la marque « Creative Commons » ou toute autre indication ou logo afférent sans le consentement préalable écrit de Creative Commons. Toute utilisation autorisée devra être effectuée en conformité avec les lignes directrices de Creative Commons à jour au moment de l'utilisation, telles qu'elles sont disponibles sur son site Internet ou sur simple demande.

Creative Commons peut être contacté à http://creativecommons.org/.

Annexe B. : Index des illustrations

Annexe C. : Aide-mémoire NetFilter - Iptables

1. Architecture de NetFilter et priorité des tables



2. Définition de variables

```
IPT="/sbin/iptables"
Def-Tables="filter, nat, mangle"
Def-Chains="INPUT, FORWARD, OUTPUT"
Def-Conntrack="INPUT, FORWARD, OUTPUT"
```

3. Initialisation de Netfilter

```
for table in $Def-Tables; do
       $IPT -t $table -F
       $IPT -t $table -X
done
for chain in $Def-Chains; do
       $IPT -t filter -P $chain DROP
done
$IPT   -t filter -A INPUT -i lo -j ACCEPT
$IPT   -t filter -A OUTPUT -o lo -j ACCEPT
for chain in $Def-Conntrack; do
       $IPT    -t filter -A $chain \
               -m state -state RELATED,ESTABLISHED \
               -j ACCEPT
done
```

4. Gabarits de règles par fonction de machine

1. Client

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p tcp --syn --dport $Tcp-Port --sport $Tcp-Port \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A OUTPUT \
```

```
       -d $Ip-Destination  \
       -p udp --dport $Udp-Port --sport $Udp-Port \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination  \
       -p icmp --icmp-type $Icmp-Type \
       -m state --state NEW \
       -j ACCEPT
```

2. Serveur

```
$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p tcp --syn --dport $Tcp-Port --sport $Tcp-Port \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination  \
       -p udp --dport $Udp-Port --sport $Udp-Port \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination  \
       -p icmp --icmp-type $Icmp-Type \
       -m state --state NEW \
       -j ACCEPT
```

3. filtre de paquets

```
$IPT   -t filter -A FORWARD \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p tcp --syn --dport $Tcp-Port --sport $Tcp-Port \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p udp --dport $Udp-Port --sport $Udp-Port \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -s $Ip-Source \
       -d $Ip-Destination \
       -p icmp --icmp-type $Icmp-Type \
       -m state --state NEW \
       -j ACCEPT
```

5. Gabarits de règles par protocole applicatif

1. FTP (TCP/21)

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p tcp --syn --dport 21 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p tcp --syn --dport 21 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
```

```
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p tcp --syn --dport 21 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT
```

2. SSH (TCP/22)

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p tcp --syn --dport 22 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p tcp --syn --dport 22 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p tcp --syn --dport 22 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT
```

3. SMTP (TCP/25)

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p tcp --syn --dport 25 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p tcp --syn --dport 25 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p tcp --syn --dport 25 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT
```

4. DNS (UDP/53)

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination  \
       -p udp --dport 53 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination  \
       -p udp --dport 53 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -s $Ip-Source \
       -d $Ip-Destination \
       -p udp --dport 53 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT
```

5. HTTP (TCP/80)

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p tcp --syn --dport 80 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p tcp --syn --dport 80 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p tcp --syn --dport 80 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT
```

6. POP3 (TCP/110)

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p tcp --syn --dport 110 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p tcp --syn --dport 110 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p tcp --syn --dport 110 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT
```

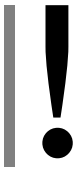
7. HTTPS (TCP/443)

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p tcp --syn --dport 443 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p tcp --syn --dport 443 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p tcp --syn --dport 443 --sport 1024: \
       -m state --state NEW \
       -j ACCEPT
```

8. IPSEC



Petite précision sur le fonctionnement d'`IPSEC` avec un noyau `linux 2.6` : le trafic rentre par l'interface `$Int-Entree` dans la machine cible, est déchiffré par la pile IP et réinjecté dans la pile IP en clair comme s'il venait d'arriver sur la machine. La principale conséquence est qu'il faut alors 2 règles minimum : une pour gérer le trafic `IPSEC` et une pour gérer le trafic en clair.

Autorisation de la négociation de clefs IKE/ISAKMP

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p udp --dport 500 --sport 500 \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p udp --dport 500 --sport 500 \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p udp --dport 500 --sport 500 \
       -m state --state NEW \
       -j ACCEPT
```

Autorisation du protocole ESP

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p esp \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p esp \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p esp \
       -m state --state NEW \
       -j ACCEPT
```

Autorisation du protocole AH

```
$IPT   -t filter -A OUTPUT \
       -d $Ip-Destination \
       -p ah \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A INPUT \
       -s $Ip-Destination \
       -p ah \
       -m state --state NEW \
       -j ACCEPT

$IPT   -t filter -A FORWARD \
       -i $Int-Entree -o $Int-Sortie \
       -s $Ip-Source \
       -s $Ip-Destination \
       -p ah \
```

```
      -m state --state NEW \
      -j ACCEPT
```

6. Activation du routage

Les règles de NetFilter pour la table `FORWARD` ne suffisent pas. Il faut activer le routage dans la pile TCP/IP du noyau directement. Cette instruction se situe en général en toute fin du script d'initialisation du filtre de paquets, après que toutes les règles de filtrage aient été mises en place.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

7. La translation d'adresse

Il est recommandé d'effectuer la `SNAT` avant le traitement du paquet (donc dans la chaîne `PREROUTING`) et la `DNAT` au dernier moment (donc dans le chaîne `POSTROUTING`).

1. Translation d'adresse source

Le système détermine lui-même l'adresse IP à utiliser, c'est-à-dire l'adresse IP de l'internface `$Int-Sortie`.

```
$IPT   -t nat -A POSTROUTING \
       -o $Int-Sortie \
       -j MASQUERADE
```

Les paquets correspondant au motif (ici tous les paquets arrivant par l'interface `$Int-Entree`) font l'objet d'une translation d'adresse source avec l'adresse `$Ip-Source`.

```
$IPT   -t nat -A POSTROUTING \
       -o $Int-Sortie \
       -j SNAT --to-source $Ip-Source
```

2. Translation d'adresse destination

Les paquets correspondant au motif (ici tous les paquets sortant par l'interface `$Int-Sortie`) font l'objet d'une translation d'adresse destination avec l'adresse `$Ip-destination` et le port `$Port-Destination`.

```
$IPT   -t nat -A PREROUTING \
       -i $Int-Entree \
       -j DNAT --to-destination $Ip-Destination:$Port-Destination
```

8. Règles particulières

1. Journalisation

Les paquets correspondant au motif (ici tous les paquets) sont enregistrés à concurrence de `--limit` (ici, 10 paquets par minute) avec le niveau de criticité `--log-level` (ici, 3) et le préfixe `--log-prefix` (ici, "Illegal DNS request.").

L'utilisation de l'option `--limit` est ***très fortement*** recommandée afin d'éviter une saturation du journal d'évènements qui pourrait conduire à un déni de service sur le filtre de paquets.

```
$IPT   -t filter -A INPUT \
       --limit 10/min
       -j LOG \
       --log-level 3 --log-prefix "Illegal DNS Request."
```

2. Chaînes Utilisateur

Création de la chaîne utilisateur

```
$IPT   -N User-Chain
```

Exemple de filtrage des connexions à envoyer dans cette chaîne: Tout le trafic `UDP/53` routé par la machine est envoyé pour traitement dans la chaîne `User-Chain`.

```
$IPT   -t filter -A FORWARD \
       -i eth0 -o eth1 \
       -p udp --dport 53 \
       -j User-Chain
```

Les connexions à destination des adresses IP `ADDRESS_IP_*_DNS_SERVER` (sous entendu, les connexions `UDP/53` puisque nous sommes dans la chaîne `User-Chain`, dans laquelle est envoyé tout le trafic `UDP/53`.) sont acceptées. Les autres sont enregistrées à concurrence de `10 par minute` avec le niveau de criticité `3` et le préfixe `"Illegal DNS Request."`. Les paquets ne correspondant à aucun motifs (ie, à destination d'autres adresses IP que celles spécifiées) sont renvoyés dans la chaîne appelante (ici `FORWARD`).

```
$IPT   -t filter -A User-Chain \
       -d ADDRESS_IP_PRIMARY_DNS_SERVER \
       -j ACCEPT
$IPT   -t filter -A User-Chain \
       -d ADDRESS_IP_SECONDARY_DNS_SERVER \
       -j ACCEPT
$IPT   -t filter -A User-Chain \
       --limit 10/min
       -j LOG \
       --log-level 3 --log-prefix "Illegal DNS Request."
```

3. Redirection de port

Est utilisée lorsque le serveur mandataire est situé sur la même machine que le filtre. Il s'agit de la forme la plus simple de mise en place d'un serveur mandataire transparent. Si ce dernier est situé sur une autre machine, il devient beaucoup plus délicat de mettre en place ce type de redirection de trafic.

```
$IPT   -t nat -A PREROUTING \
       --dport 80 \
       -j REDIRECT --to-port 8888
```

Annexe D. : Pour aller plus loin

1. Organisation

Les aspects techniques de la SSI ne résolvent pas tous les problèmes, loin s'en faut. Il est même communément admis que 80% des solutions sont des solutions organisationnelles, contre « seulement » 20% de solutions techniques.

Ce document n'a pas abordé les thèmes organisationnels de la SSI. Il faut pourtant impérativement les étudier, ne serait-ce que pour cadrer l'action des techniciens.

2. Analyse et gestion du risque

Un bon moyen d'estimer la pertinence de telle ou telle mesure est d'appliquer une démarche de gestion du risque. Cette pratique va au delà de la « simple » analyse du risque puisqu'elle permet de justifier les investissements liés à la sécurité du système.

3. Gestion de la sécurité

Lorsque la taille du système ou les enjeux de sécurité qui y sont rattachés le justifie, il devient alors intéressant d'étudier la mise en place d'un centre de gestion de la sécurité, de la même façon que le centre de gestion réseau est chargé de garantir un fonctionnement optimal du ou des réseaux. Les principales missions opérationnelles d'un CGS sont:

- ✔ Veille
  - La veille relative à la publication de vulnérabilités et / ou de correctifs de sécurité affectant le système.
- ✔ Alerte
  - L'information des responsables des systèmes concernés par la veille évoquée ci-dessus ;
  - Liaisons et échanges avec leurs homologues extérieurs ;
  - Détection des attaques par divers moyens (IDS, Analyse de logs, HotLine, ...).
- ✔ Réponse
  - Le suivi des incidents de sécurité et la coordination des actions correctrices.

Ce type de structure peut également être chargée d'un certain nombre de tâches plus stratégiques, comme:

- La coordination des efforts de l'entité en matière de sécurité des systèmes d'information ;
- L'organisation de la réflexion post-incident et l'émission de recommandations pour pallier le problème ;
- La tenue à jour de tableaux de bord de la sécurité à destination des instances dirigeantes ;
- Participation à l'élaboration ou la modification de la politique sécurité de l'entité. Cette participation peut prendre diverses formes comme des avis techniques ou du conseil en organisation.

Bref, les pistes d'amélioration de la sécurité dans un organisme sont particulièrement vastes. Il vaut mieux avancer doucement mais sûrement, que de mettre en place une structure ambitieuse sans lui donner les moyens de son action. Les démarches d'amélioration constante de la sécurité entrecoupées de périodes de consolidation de l'existant sont souvent les plus payantes.

Toutefois, on s'aperçoit parfois que mettre en place de telles structures provoque une espèce d'électrochoc qui fait bouger les choses.

L'important est donc de parvenir à trouver un juste milieu avec les moyens dont on dispose.