2011

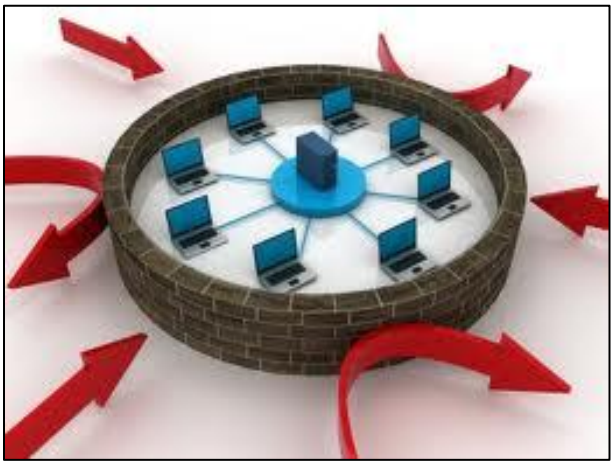
Pare-feu
Architecture et déploiement

Stéphane DUFOUR

09/09/2011

Pare-feu : Architecture et déploiement

V 1.0



Stéphane DUFOUR
(Architecte système et sécurité)

Table des matières

Introduction

Tout au long de ce cours nous allons nous attacher à la partie sécurité du Système d'Information (SI).

Cela conduit souvent à avoir une approche différente des fonctionnels. Il faudra systématiquement faire entendre vos arguments et parvenir à des compromis concernant les fonctionnalités attendues et le niveau de sécurité désiré.

Dans un premier temps nous allons faire un rapide rappel des concepts généraux liés à la sécurité informatique. Nous aborderons ici les fondamentaux de la sécurité informatique.
Cependant nous n'irons pas aussi loin qu'un livre traitant de la sécurité informatique en général : nous nous concentrerons sur la problématique engendrée par la mise en œuvre du pare-feu au sein d'une entreprise.

Considérant que pour se protéger d'une attaque il est nécessaire d'en connaître la nature nous dresserons dans un second temps un état des lieux des techniques de hacking connues à ce jour.
Cette partie sera fort utile au moment de choisir et mettre en œuvre votre pare-feu dans un SI existant ou en cours d'élaboration.

Ensuite nous expliquerons le rôle du pare-feu dans une architecture système sécurisée ou à sécuriser, puis nous en énumérerons les différents types.

Après cela il sera intéressant de présenter la démarche pour intégrer judicieusement cet élément dans votre SI existant. Dans cette partie il sera surtout question de réflexion et d'étude préliminaire. Certes fastidieuse cette dernière est incontournable pour une intégration réussie et pérenne de votre pare-feu. Comme toujours l'audit de l'existant sera une phase clef du projet de déploiement.

Enfin viendra le moment du choix technique et enfin du déploiement de votre pare-feu.
Cette partie beaucoup plus technique est relativement simple si l'on suit certaines règles, la plupart des solutions de pare-feu se ressemblant quasiment toutes.

Concepts de base

Rappel sécurité

Les fondamentaux

La sécurité informatique est avant tout une réflexion à mener de manière posée.
Croire que sécuriser un SI impose un lourd travail technique est faux. En fait si vous passer 75% de votre temps à bien ficeler votre étude alors la partie technique ne représentera que 25% de votre projet (et encore avec l'habitude …).

La plupart des pare-feu professionnels se paramètrent rapidement pour un expert en sécurité : la question étant surtout de savoir ce que l'on veut sécuriser et comment le faire efficacement avec les bonnes méthodes.

Nous ne parlerons pas ici de sécurisation des locaux etc.
Rappelons juste qu'un SI (ou l'un de ces éléments) accessible physiquement par l'assaillant est considéré comme compromis, ensuite l'effet domino fera le reste.

Concentrons-nous sur les architectures dites sécurisées, c'est-à-dire la partie systèmes et réseaux.

Quand on aborde le sujet de la sécurité informatique on pense, à tort, qu'il **suffit d'installer un pare-feu et un anti-virus** pour avoir sécurisé son système. Cela est **un bon point de départ** mais hélas au vu des attaques actuelles pas suffisant.
La règle une, en sécurité, veut que : le **niveau global de sécurité du SI est celui de l'élément ayant le niveau de sécurité le plus bas de ce SI …**
Dit en ces termes cela fait froid dans le dos mais il s'agit hélas de la réalité.

En prenant les exemples ci-dessous nous sommes déjà dans le rouge niveau sécurité et pourtant … :

- Wifi sauvage,
- Modems personnels,
- Inversion accidentelle câbles réseau intranet/internet,
- Session réseau non-verrouillée,
- Patchs de sécurité non appliqués,
- Anti-virus non à jour,
- Etc …

Partant de ce constat les experts en sécurité informatiques considèrent **qu'un système d'information (fonctionnel) sécurisé à 100% n'existe pas**.
Il faudra donc :

- faire des choix d'architecture,
- trouver le juste **équilibre entre sécurité et fonctionnalités**,
- trancher quant au **budget alloué à la sécurité**, en évaluant les risques,
- **sensibiliser et former des utilisateurs et administrateurs aux bonnes pratiques** de la sécurité,
- définir une **politique de sécurité globale qui sera suivie**,
- disposer de **plan de reprise après sinistre**.

Ceci étant une liste minimum.

Dans la prochaine partie nous allons voir les menaces réelles auxquelles un SI doit faire face au quotidien.

Les menaces

Dans cette partie nous allons donc nous intéresser aux côtés obscurs du réseau. Uniquement dans le but de mieux évaluer les risques encourus par votre SI. L'idée est donc de dresser une liste des menaces connues afin de voir si l'architecture de pare-feu retenue peut parer efficacement ces menaces.

De façon générale voici comment se déroule une attaque informatique :

- L'assaillant ?
  - Crackers « black hat » : cyber terrorisme, terroristes, cybercriminels, etc.
  - Hackers « Grey hat » : passionnés, recherche du défis, freelance, partagent du savoir etc.,
  - Hackers « White hat » passionnés, travaillant dans la sécurité informatique, vendent le savoir
- Cibler la victime,
  - Social Engineering (la faille humaine : faille numéro une !),
  - En utilisant les bons outils :

Outil	Description
nslookup	Recherche d'information DNS
dig	Recherche d'information DNS
dnsenum	Permet de récolter toutes les informations que peut fournir l'interrogation d'un DNS donné (champs MX, NS etc., brute force DNS, sous-domaines, transfert de zone etc.)
Dnsdic, dnsmap, dnsrecon, dnswalk, subdomainer	Scripts exploitant les informations des DNS
netcat	utilitaire permettant d'ouvrir des connexions réseau, que ce soit UDP ou TCP (socket) sous n'importe quel port pour un service quelconque. Sa flexibilité permet des usages plus exotiques : transferts de fichiers, backdoor, serveur proxy basique, ou encore messagerie instantanée
telnet	Permet d'établir une connexion TCP/IP et d'afficher en autre les bannières des services sous-jacents.
ssh	A la fois un programme informatique et un protocole de communication sécurisé. Il impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur, le VPN du pauvre.
nmap	Un scanner de ports incontournable
scapy	Il est capable, entre autres, d'intercepter le trafic sur un segment réseau, de générer des paquets dans un nombre important de protocoles, de réaliser une prise d'empreinte de la pile TCP/IP, de faire un traceroute, d'analyser le réseau informatique (il peut remplacer les commandes hping, 85% des fonctionnalités de nmap, arpspoof, arp-sk, arping, tcpdump, ethereal, p0f, etc.).
metasploit	Un framework puissant testant les vulnérabilités d'un système
maltego	Recherche d'information récursivement

	(personnes, sites web, réseaux sociaux, AS, mail, expressions, adresse ip etc.)
Siphon	Permet de connaître la topologie réseau du brin physique sur lequel le mappeur analyse les paquets. Cet outil n'envoie pas de paquets sur le réseau et est donc totalement indétectable par les NIDS.
Burp Suite, WebScarab, WebDeveloppeur Bar	Série d'outils d'analyse et de prise d'empreinte de site Web
Virus, Troyens, BackDoor	Cf.wikipedia
ettercap	Outils de sniffing et d'attaque réseau (repoison_arp, dns_spoof
Rootkit	Un ensemble de logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible.
Keyloggers	Cf.wikipedia
Log-wiper	Permet de nettoyer les traces d'un assaillant dans les journaux système de la cible
Modules lkm dans le noyau	
Metagoofil	Retrouver des documents accessibles sur un site via leur extension.
TheHarvester	Récupère des comptes mail, des noms d'utilisateurs et des noms d'hôtes de sous-domaines
Shodan	Moteur de recherche qui référence des éléments de tout type connectés au réseau Internet. Il récupère les bannières et services de ces éléments en indiquant ceux ayant des vulnérabilités
RobTex	Véritable boîte à outils de l'administrateur réseau il récolte une mine d'informations concernant les adresses IP et les noms de domaine
Hostmap	Permet d'établir une liste des sites web hébergés par un serveur mutualisé et de rechercher les éventuels serveurs de mail, de nom etc.
Hping3	Outil pour forger des paquets réseau standards ou non usuels. Permet de scanner, faire des DoS, identification d'OS, envoyer de fichiers de façon détourné etc.
Amap	Un scanner de protocole permettant de détecter le type de protocole caché derrière un port donné
HttpPrint	Outils de prise d'empreinte des serveurs Web
SnmpWalk	Un explorateur de la base MIB des cibles
Nessus	Scanner de vulnérabilités (payant)
OpenVAS	Scanner de vulnérabilités (Gratuit)
Sites de référencement d'exploits	Offensive Security, Metasploit, Security Focus, Packet Storm Security, sebug, BugTraq, Full Disclosure, Security reason …
BackTRack 5	Distribution complète dédiée à la sécurité informatique : l'outil du « PenTester »

    - Repérer les domaines possibles (whois, tracert …)
    - Google (hacking) is your friend, FaceBook, Twitter, 123people,
    - Découvrir le réseau (topologie, architecture, les systèmes en présence, les briques applicatives déployées),
- L'attaque à proprement parler,
    - L'anonymat,
    - Type : « Black box » (sans la moindre information concernant la cible), « Grey box » (en ayant connaissance de quelques d'informations sensibles), « White box » (en disposant d'une solide connaissance de la cible : propre personnel agissant par vengeance ou traitrise),
    - Profiter de la faille humaine : le Social Engineering (la faille humaine : faille numéro une !),
    - Ouvrir les portes du réseau : exploiter les failles (Sniffing, bases de failles/exploits en ligne ➔ Securityfocus etc., Nessus SAINT …)
    - L'attaque par le Web (injection SQL, XSS, WebScarab, NikTo),
    - La force au service de l'attaque (brute force, RainBow table, DoS, Buffer Overflow …)
- Introduire le système et assurer son accès,
    - Rester discret : en général une intrusion réussie ne laisse AUCUNE TRACE (journaux inchangés : on efface que ses propres traces via log-wiper, clear, zap, mots de passe non modifiés,
    - S'assurer un accès : via une backdoor locale ou distante, outils présents, rootkit, troyens …
    - Etendre son champ d'action : cibler les annuaires et serveurs de noms

Pour finir sachez qu'il existe des multitudes de scénario d'attaque : seule l'imagination de l'être humain est la limite, alors inutile de préciser que dans ce domaine **vouloir être exhaustif est de la pure utopie** ! …

Maintenant énumérons quelques attaques bien connues, des standards dira-t-on.

Attaque par Social Engineering

Vieille comme le monde, cette attaque permet de **pousser une personne à faire certaines choses ou révéler des informations** sans les lui demander, d'où le terme de manipulation.
En fonction du contexte ou de la personnalité d'une victime, nous pouvons récupérer diverses informations suivant le niveau de coopération de cette personne.

⇨ A lire : Kevin Mitcnick, tout un art !

Les failles physiques et systèmes

Pour faire simple on peut dire qu'une fois l'accès physique à un système obtenu, sa compromission n'est qu'une question de temps, parfois très court.

Alors est-il utile de protéger physiquement l'ordinateur ou l'élément lui-même ?
Oui, car cela ralentira et découragera l'assaillant. Gardez à l'esprit que ces éléments (pare-feu, routeur, serveur, switchs, sondes, modem etc.) sont des briques systèmes sensibles en terme de sécurité.

Voici quelques failles exploitables :

- BIOS : retrait de la pile ou jumpers, CmosPwd,
- Keyloggers matériels et logiciels,
- Boot sur un LiveCD pour compromettre le système cible :
    - Dump base SAM (BackTrack:samdump2),
    - Registry (TrinityRescueKit, UBCD),

    - Hashes LM et NTLM via dump SAM puis exploitation sous « John the ripper », les tables Arc-en-ciel (« Rainbow tables », via « rtgen » ou « winrtgen »), « OPHCRACK », « CAIN&ABEL », etc.,
    - LiveCd spécialisé : kon-boot,
    - Exploitation des partitions de données si disque dur non cryptée (EFS etc.)
- Boot en mode maintenance/dégradé sur un système (*NIX, Windows, Mac …),
- Les attaques pré-boot, (utilisation des DSDT par exemple via le langage AML => Mac OS X sur PC)
- Branchement d'un périphérique type USB ou Firewire (faille DMA pour le protocole raw1394) exploitant une faille de ces protocoles pour attaquer le système via ces bus (ByPass authentification Windows),
  Note : ici on ne parle pas « d'Autorun » mais bien de couche basse, niveau pilote bas niveau.
- Une fois une session ouvert en simple utilisateur :
    - NESLSON (kernel inférieur à 2.6.37) accès au compte root,
    - RDS (kernel 2.3.30 à 2.6.36) accès au compte root,
    - login.scr/Utilman.exe (Windows NT à 7) en cmd.exe (Windows) via substitution de binaire offline, accès au compte « Administrateur local »
    - GONZOR-SWITCHBLADE, un véritable aspirateur d'informations sensibles sur le système en cours d'exécution,
    - Clef bootable Microsoft USB COFEE (150 outils pour mener une enquête de police),
    - Clef USB à technologie U3 (si l'« Autorun » est activé une série de logiciels sont lancés sur la cible … une porte ouverte pour glisser des softs style GONZOR-SWITCHBLADE),
    - Les flux ADS, permettent le masquage de tout type de fichiers (binaire, texte, configuration etc.) (http://www.heysoft.de/en/information/ntfs-ads.php?lang=EN),
    - Exploitation des dump mémoire, des fichiers de mise en hibernation du système, de la mémoire vive RAM via des outils spécialisés (BackTrack en contient quelques-uns),
    -
- Les vols de mots de passe, crackage de mots de passe (parfois trop simples),
- Les suid et sgid sous les *NIX,
- Les planificateurs de tâches des systèmes avec élévation des droits,
- Logiciels nécessitants des élévations de privilèges (su, runas, sudoer etc.),
- Injection de code dans des processus en mémoire,
- etc.

Vous noterez qu'un pare-feu de type professionnel (Appliance UTM) est difficilement piratable via une faille physique ou système : bien entendu c'est le but !
Il vous reste quand même le port console, le bouton RESET ou plus extrême le dump de ROM, bonne chance.

Les failles réseaux

Le gros souci à l'heure actuel concernant les failles réseau vient en partie du fait qu'IPV4 n'a pas été conçu à la base pour être un protocole sécurisé : il ne l'est pas et ne le sera jamais.

Tous nos réseaux sont fondés sur lui, d'où cette expression assez juste : Internet est un château de sable.
Rassurez-vous IPV6 devrait remettre un peu d'ordre à ce niveau.

Voici quelques classiques :

- **Encapsulation de protocole** : En général les flux http (via proxy ou non) sont toujours autorisés, il est trivial d'encapsuler n'importe quel protocole (SSH, RDP etc.) dans un flux HTTP/S. Hélas dans ce cas de figure votre pare-feu n'y verra … que du feu !
  Autre exemple **l'IP overDNS**, le protocole DNS (UDP 53) étant peu filtré vous pouvez encapsuler

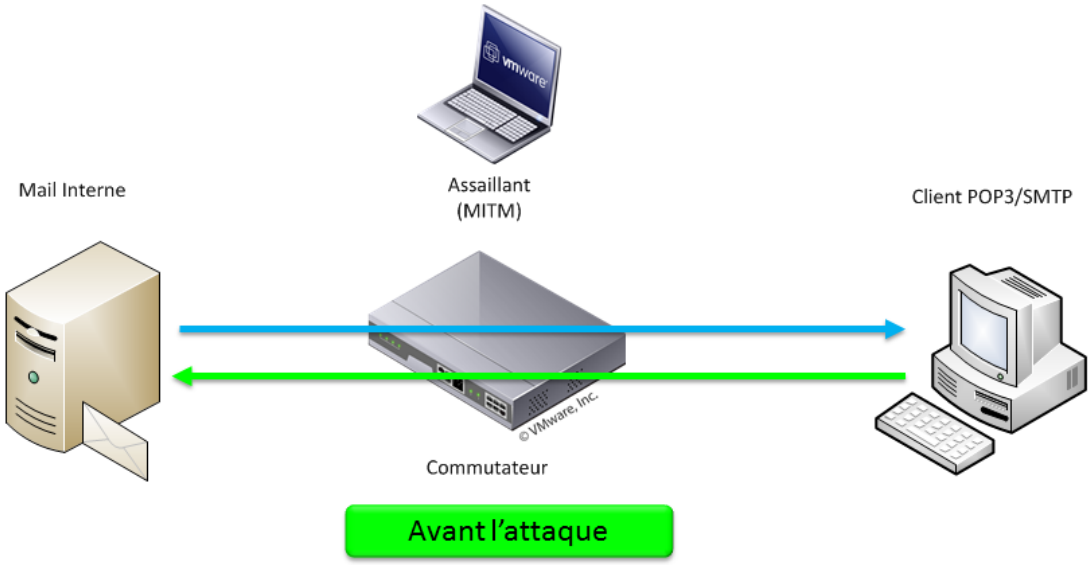
vos paquets TCP/UDP dans une requête DNS (via **Iodine**).
Ou encore sur le même principe **IP over ICMP**.

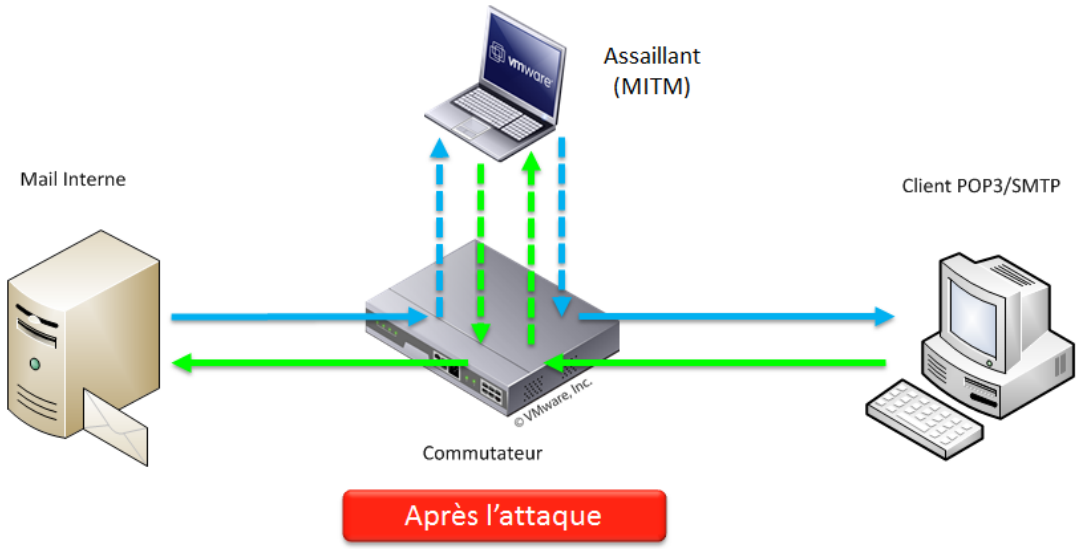
- **DoS** : le but est de saturer de requêtes le serveur ou le service proposé par une entreprise, si l'attaque est massive (réalisé par un BotNet) elle aboutit la plupart du temps. Combien de fois on entend dire « il n'y a plus de réseau », mais quelle en est la cause exacte ?

- **Ecoutes réseaux** : le Sniffing réseau permet de capturer les informations qui transitent en claires ou cryptées sur un réseau commuté (avec un ARP Spoofing ou Poisoning au préalable) ou non via des protocoles type HTTP, POP3, SMTP, Telnet, FTP, etc. mais aussi SSL, NTLM et dernièrement Kerberos qui a été mis à mal.

- **MITM : Man In The Middle**, littéralement attaque de l'homme au milieu. Elle consiste à s'immiscer dans une connexion déjà établie en se faisant passer pour l'un des deux éléments communiquant.

  Ci-dessous un exemple d'attaque via ARP Spoofing, le but étant de charger la table ARP de chaque hôte cible avec de fausses informations les concernant (ou éventuellement la passerelle par défaut) :





- **L'ARP Poisoning** est une autre attaque qui consiste à saturer la table de MAC adresse du switch, il bascule ensuite en mode hub et broadcaste tout le trafic sur tous ses ports physiques. Le « sniffing » du trafic d'un hub devient trivial.

- **Le hijacking** :
  Le « vol de session TCP » (également appelé détournement de session TCP ou en anglais TCP session hijacking) est une technique consistant à intercepter une session TCP initiée entre deux machine afin de la détourner. Souvent il faut parvenir à prédire les numéros de séquence d'une session TCP.

  Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque (via source-routing ou blind attack) parvient à prendre possession de la connexion pendant toute la durée de la session.
  Proof of concept: « **shijack** », « **HUNT** », « HJKSuite », «P.A.T.H. », «JUGGERNAUT ».

- **Le « spoofing » d'adresse d'IP**
  C'est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auquel il a accès.

    - La première utilité de l'IP Spoofing va être de falsifier la source d'une attaque. Par exemple, lors d'une attaque de type déni de service, l'adresse IP source des paquets envoyés sera falsifiée pour éviter de localiser la provenance de l'attaque.
    - L'autre utilisation de l'IP Spoofing va permettre de profiter d'une relation de confiance entre deux machines pour prendre la main sur l'une des deux.

- **Failles WIFI** : WEP (via airodump-ng, airplay-ng, airecrack-ng) dans une moindre mesure WPA

- **Faux hot-spots WIFI (Rogue AP en anglais**, Ex. : Karmetasploit**)**, les « honey-pots » malicieux.
  Vous attendez quelqu'un, vous jouez avec votre Smartphone et soudain une pop-up vous signale un hot-spot WIFI libre d'accès, sans mot de passe ! : génial, pour surfer ou relever vos courriel plus rapidement sans utiliser votre bande passante de votre forfait à 39 euros.
  Pas de chance ce hot-spot est un véritable piège pour les RoadWarriors …backdoor et snifer y sont implémentés : tous vos accès non cryptés ont vu leur mot de passe dérobés en quelques minutes.

- La téléphonie sur IP :
  - Le phreaking, VOIPONG (permet d'enregistrer une conversation VOIP, fichier WAVE),
  - Le SIPCrack : usurpation de ligne à l'aide de SIP,

- Les outils d'attaque en IPV6 arrivent eux aussi, style THC-IPv6 qui permet entre autre de :
  - Simuler un routeur IPv6, « Fake_router6 »,
  - Attaquer en MITM avec « parasite6 »,
  - Etc.

<u>Les failles Web</u>

L'internet est un vaste réseau d'ordinateurs et d'éléments actifs sur lequel transitent des millions d'informations. Ces données sont de différentes nature (courriel, fichiers, page web, chat, flux vidéo, son, voip etc) et plusieurs méthodes sont utilisées pour les acheminer (HTTP/S, SMTP, POP3, FTP, etc.)

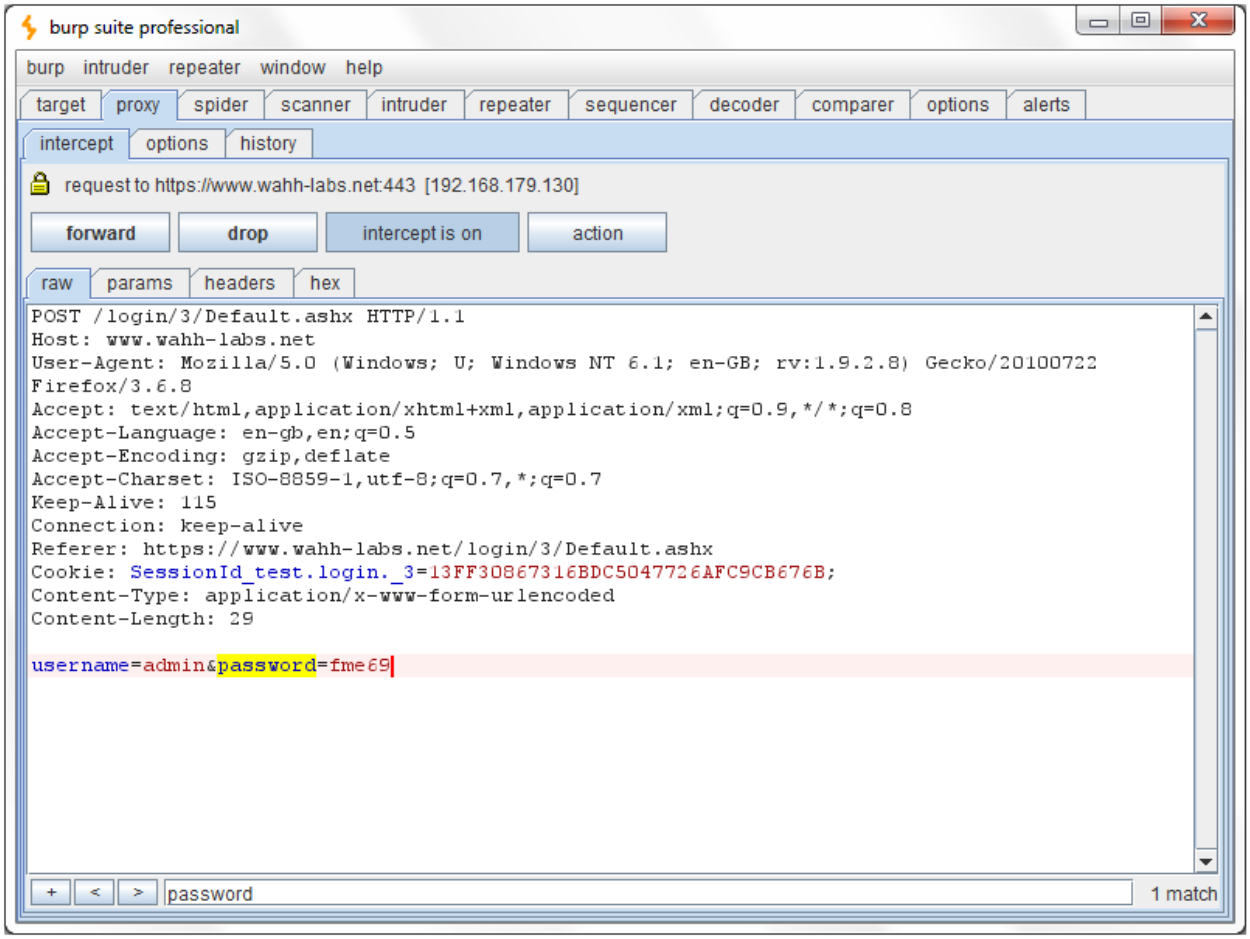
Tout comme IPv4, ces protocoles présentent des failles de sécurité d'autant plus qu'ils n'ont pas forcément été conçus dans une optique de sécurisation des données qu'ils acheminent.

Je commencerai par vous conseiller **d'héberger, dès que cela est possible, votre site Web** (et pourquoi pas votre « Relais mail » ?) à l'extérieur de votre infrastructure réseau, **chez un hébergeur dont c'est le cœur de métier** (OVH, PROXAD, O2SWITCH etc.).
Les contrats et le sérieux de certains prestataires peuvent être intéressants et **sont à étudier… en détail**. Une visite de l'infrastructure de l'hébergeur est également possible pour constater ce sérieux, la présence d'une équipe de spécialistes en sécurité pourra vous conforter dans votre choix.

En effet un serveur Web est tout le temps attaqué avec, chaque minute, de nouvelles trouvailles pour contourner les patchs et rustines mises en place sur des produits qui n'ont pas été conçus, à la base, pour la sécurité.

Cela étant dit voici les attaques les plus répandues sur le Web auxquelles vous serez confronté si vous hébergez un service de type Web en vos locaux :

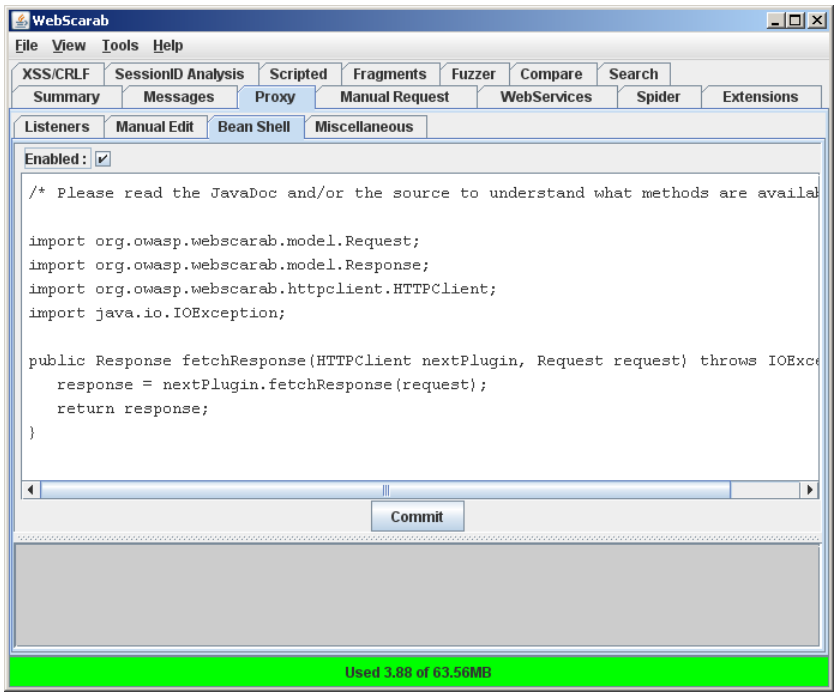
- Une attaque de site Web sera souvent précédée d'une **prise d'empreinte. Pour cela des outils comme « Burp Suite »** sont de véritables aspirateurs d'informations ciblant un site particulier.



- **Malformation/modification d'URL** (méthode GET/POST etc.) volontaire en exploitant les failles des sites dynamiques (à base d'ASP, PHP, JAVA, JS etc.), ici il s'agit avant tout de maitriser parfaitement les langages de programmation du site ciblé, ensuite les recherches de failles deviennent simples. Par exemple les add-ons des CMS sont de véritables nids de bug et failles.

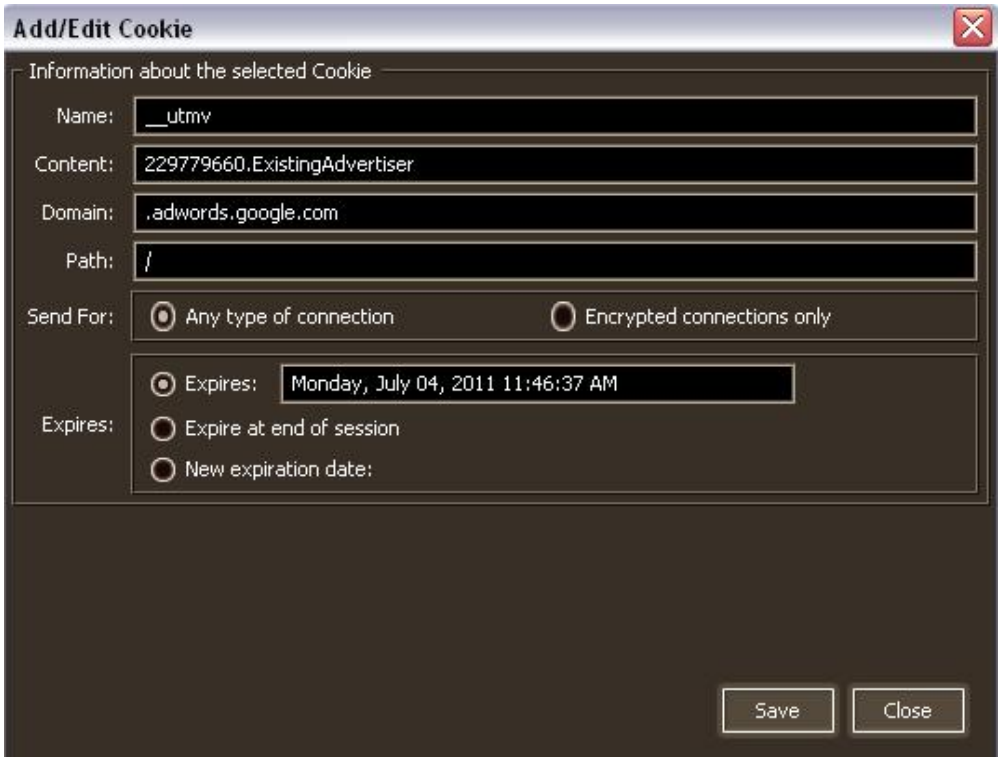
- Mise en place d'un s**ite/pages Web hébergeant des Backdoor, troyens, vers, code malicieux** etc. qui exploiterons des failles de votre navigateur Web ou encore en mettant en place des redirections de code pour planter le serveur Web du site visé. (Ex. : <script>document.location=http://tools.mal.com</script>, ou encore les <iframe>).

- Envoi de **formulaires** de réponse piégés en exploitant les **champs non ou mal filtrés** (SLQ Injection possible via « SQL Inject Me », ou XSS « XSS Me », « HackBar », etc.). Encore une fois les outils comme « **Webscarab** » et « **Wfuzz** » qui permettent de modifier à la volée, avant envoi, le contenu des commandes type POST etc. seront fort utiles.




```
********************************************************
* Wfuzz  2.0 - The Web Bruteforcer                     *
* Coded by:                                            *
* Christian Martorella (cmartorella@edge-security.com) *
* Xavier Mendez aka Javi (xmendez@edge-security.com)   *
* Carlos del ojo (deepbit@gmail.com)                   *
********************************************************

Target: http://localhost:8888/MAMP/FUZZ
Payload type: file,wordlist/general/common.txt

Total requests: 950
=====================================================================================================================
ID      Response   Lines      Word         Chars                 Server                                  Redirect   Request
=====================================================================================================================

00244:  C=301      9 L        30 W         330 Ch     Apache/2.0.63 (Un                http://localhost:8888/MAMP/css/   " - css"
00324:  C=301      9 L        30 W         334 Ch     Apache/2.0.63 (Un              http://localhost:8888/MAMP/english/   " - english"
00440:  C=200     10 L        37 W         586 Ch     Apache/2.0.63 (Un                                                " - index"
00430:  C=301      9 L        30 W         333 Ch     Apache/2.0.63 (Un             http://localhost:8888/MAMP/images/   " - images"
00470:  C=301      9 L        30 W         329 Ch     Apache/2.0.63 (Un                 http://localhost:8888/MAMP/js/   " - js"
00620:  C=301      9 L        30 W         330 Ch     Apache/2.0.63 (Un                http://localhost:8888/MAMP/php/   " - php"
00628:  C=302      0 L         0 W           0 Ch     Apache/2.0.63 (Un                             /phpMyAdmin/   " - phpmyadmin"
00783:  C=301      9 L        30 W         334 Ch     Apache/2.0.63 (Un              http://localhost:8888/MAMP/spanish/   " - spanish"
```

- Falsification de Cookie :



- Le **dépôt de fichier malicieux**. Par exemple un fichier .php à la place d'une image .jpg attendue par le moteur du site cible qui propose un formulaire d'upload. Une fois ce fichier déposé sur le serveur cible il suffit d'appeler l'URL avec ce .php et l'accès est ouvert …

- Corruption **de bases de données sensibles** via SQL Injection. Attention il s'agit du vecteur d'attaque le plus utilisé sur le Web.

- Mauvaise configuration de votre serveur Web, SMTP (qui relaye tous les domaines), FTP etc.

- Enfin les nouvelles technologies regorgeant de nouvelles failles toujours plus surprenantes les unes que les autres :
  - AJAX,
  - HTML5,
  - Flash,
  - PDF.

Les failles applicatives

Les attaques par « **BufferOverFlow** » sont les plus répandues : environ 60% des failles applicatives connues.
Il s'agit d'exploiter un bug connu ou non dans la gestion de zones mémoires déclarées dans le programme ciblé. Le but étant de lui faire exécuter du code qu'il ne devrait pas exécuter.

Un binaire avec le SUID root (permettant de lancer, via un utilisateur de base, un programme qui s'exécute dans un contexte avec des droits plus élevés « root ») qui se lance avec les droits administrateur sous les *NIX est une cible privilégiée (Ex : « passwd »).

Il ne faut bien évidemment pas oublier les classiques virus, troyens, vers, spyware, ad-ware etc.

Pour résumer ce petit tour d'horizon je dirai tout simplement qu'à l'heure où ces lignes sont écrites ces attaques sont déjà dépassées. Les meilleurs « Black hat » sont sur d'autres types d'attaques ou de failles … qui seront inévitablement des failles 0 Day, 6 mois après le début de leur exploitation par les crackers … !

La question qui vient de suite à l'esprit : « Mais comment notre pare-feu va-t-il faire pour stopper tout ça ? »

La réponse est simple : il ne peut et ne pourra jamais tout stopper, il aura cependant un rôle très important à jouer pour **canaliser ces menaces et en stopper certaines**.

Alors rien n'est perdu, voyons maintenant les bons automatismes à adopter, les « Best practices ».

Best practice

Maintenant que nous avons dressé un aperçu non exhaustif des principales menaces voici les concepts minimaux à appliquer pour s'en prémunir. La technique ou la connaissance parfaite des produits assurant la sécurité » de votre SI (sonde, NIDS, pare-feu etc.) ne suffiront pas, il faudra toujours garder à l'esprit certains concepts pour voir la sécurité dans sa globalité.

Être méthodique et rigoureux va grandement vous aider pour mettre en œuvre ces bonnes pratiques. La sécurité de votre SI sera à ce prix.

« Know your enemy ? »

Littéralement « connaître son ennemi », en effet on considère souvent, lors de la mise en œuvre d'un pare-feu, qu'il faille se protéger des attaques provenant de l'extérieur : c'est effectivement un bon point de départ.
Les Box de nos chers FAI, par défaut, partent de ce constat : par conséquent les flux entrants sont tous bloqués par défauts : c'est bien …

Mais dans les faits on constate que bien souvent cette attaque tant redoutée provient souvent de l'intérieur même de la zone réseau à sécuriser. **L'attaquant c'est nous !!!** … parfois sans même le savoir ce qui est bien pire.
Car une fois le moindre troyen ou malware activé sur votre ordinateur, ce dernier pourra sortir sans le moindre souci … : un accès est donc ouvert vers l'extérieur contre votre grés.

Pire cet intrus pourra également mettre hors d'usage votre réseau privé.

La paranoïa est donc de mise pour un expert en sécurité informatique, rien ne doit être écarté, tout doit être considéré comme potentiellement compromis … jusqu'aux éléments sensés sécuriser votre réseau : le pare-feu en fait partie !

De nouvelles réflexions concernant la sécurité partent du principe que tout élément du SI peut être compromis et par conséquent on considère ces éléments comme briques jetables et remplaçables à la volée. La virtualisation est une réponse à cette problématique, le pare-feu virtualisé entre dans cette stratégie.

Plan d'adressage réseau sécurisé

La règle une en terme de choix d'adressage IP sécurisé est que **votre réseau privé se base sur un classe d'adresse privée**. Ces adresses n'étant pas routables elles constituent un bon début de protection.
Cela semble évident mais, hélas, on trouve toujours des plans d'adressage réseau avec des adresses publics sur des réseaux privées.

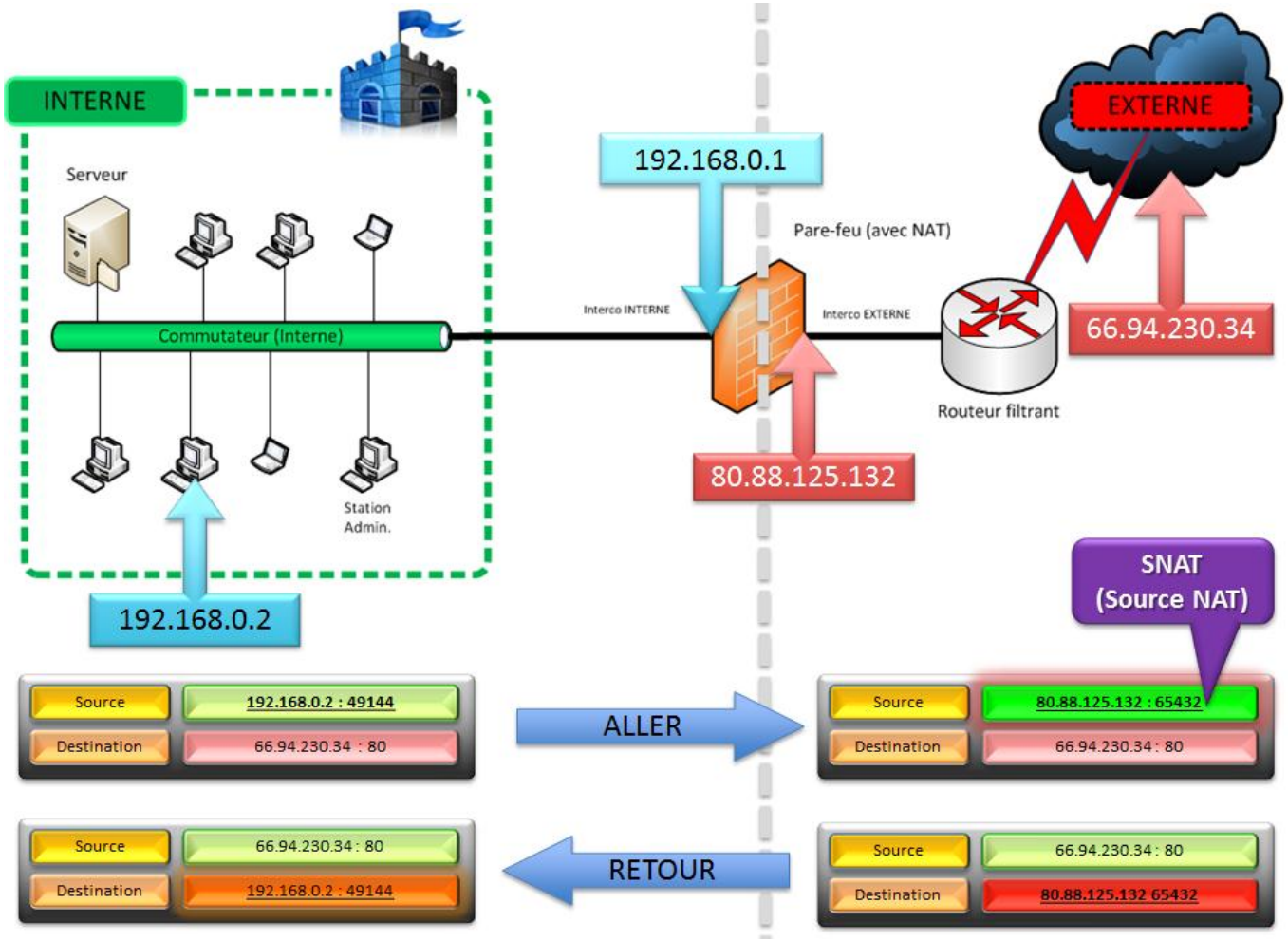
C'est pour cela que les grandes entreprises adoptent la plupart du temps un adressage interne en 10.x.y.z.

Rappel :

Classe	Préfixe	Bloc	Plage IP	Nombre d'adresses
A	10.0.0.0/8	24 bits	10.0.0.0 – 10.255.255.255	16 777 216
B	172.16.0.0/12	20 bits	172.16.0.0 – 172.31.255.255	1 048 576
C	192.168.0.0/16	16 bits	192.168.0.0 – 192.168.255.255	65 536

Le NAT (translation d'adresse réseau) constitue un deuxième rempart aux éventuels accès non autorisés provenant des réseaux public ou extérieur.
En réseau informatique, on dit qu'un routeur (ou un pare-feu) fait du ***Network Address Translation*** (NAT) lorsqu'il fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.

Lorsqu'une **machine du réseau local (192.168.0.2)** envoie des paquets à un **serveur à l'extérieur (66.94.230.34)**, l'adresse d'origine est une adresse privée. Le destinataire ne pourra pas répondre à cette adresse. Pour résoudre ce problème, le routeur NAT remplace l'adresse et le port d'origine par l'adresse Internet publique du routeur et un numéro de port libre choisi au hasard en notant adresse et port associés à la machine locale (voir sur le dessin ci-après).



La machine de destination renvoie la réponse sur l'adresse et le port visible de l'Internet au routeur NAT. Celui-ci fait alors la transformation inverse pour renvoyer les paquets vers la machine locale. Dans ce cas de figure, il n'y a rien de spécial à configurer. C'est comme cela que fonctionnent les messageries instantanées. Le logiciel de la machine sur le réseau privé se connecte au serveur de messagerie qui connaît ainsi l'adresse externe et le numéro de port du routeur qui permet de contacter cette machine.

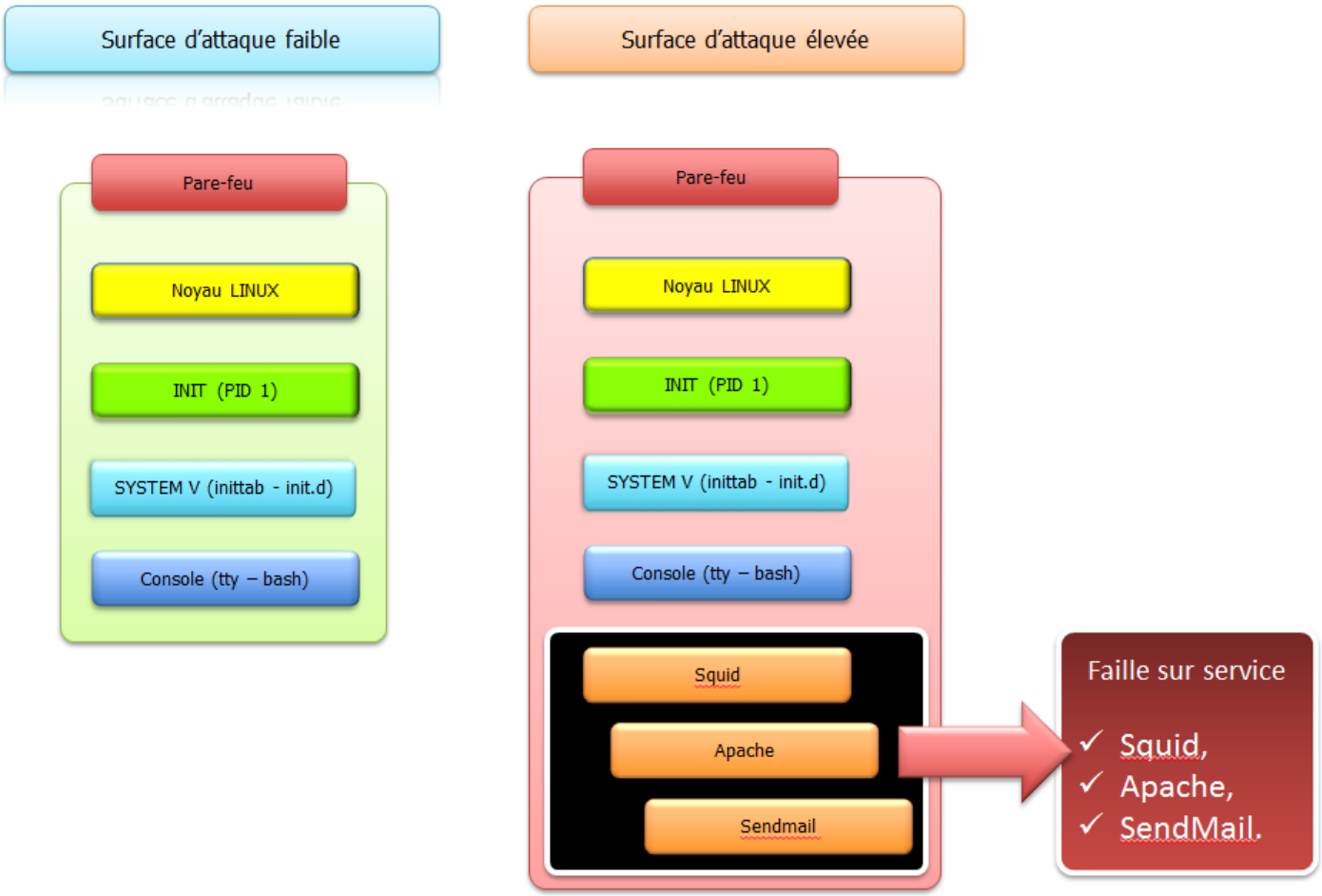
En revanche, une machine qui envoie un paquet en initiant une connexion depuis l'Internet pour atteindre une adresse privée n'a aucun moyen d'y arriver puisque le routeur ne sait pas sur quelle machine du réseau Interne, il faut router le paquet. De plus le Nat permet de ne laisser sortir sur Internet que quelques machines (Les Proxies).

Pour de plus ample information : http://en.wikipedia.org/wiki/Network_address_translation

Atomicité des fonctionnalités

Bien que cette **règle d'atomicité (unicité) des fonctions** n'aille pas de pair avec la rationalisation des moyens elle reste **un des fondements de la sécurité informatique** : les systèmes *nix dont la philosophie est d'être modulaire en sont le parfait exemple.
Par exemple OpenBSD peut se targuer du slogan : « Seulement deux vulnérabilités à distance dans l'installation par défaut, depuis plus de 14 ans ! » …
Cela est toutefois « normal » : aucun service n'est lancé par défaut soit … zéro fonctionnalité accessible depuis l'extérieur du pare-feu. Extrême mais efficace.

Par conséquent plus vous implémentez de services sur votre pare-feu plus vous élargissez la surface d'attaque de ce dernier. Cela peut être caractérisé par le schéma ci-dessous :



Note : par défaut « Sendmail » est installé sous Centos 5.2.

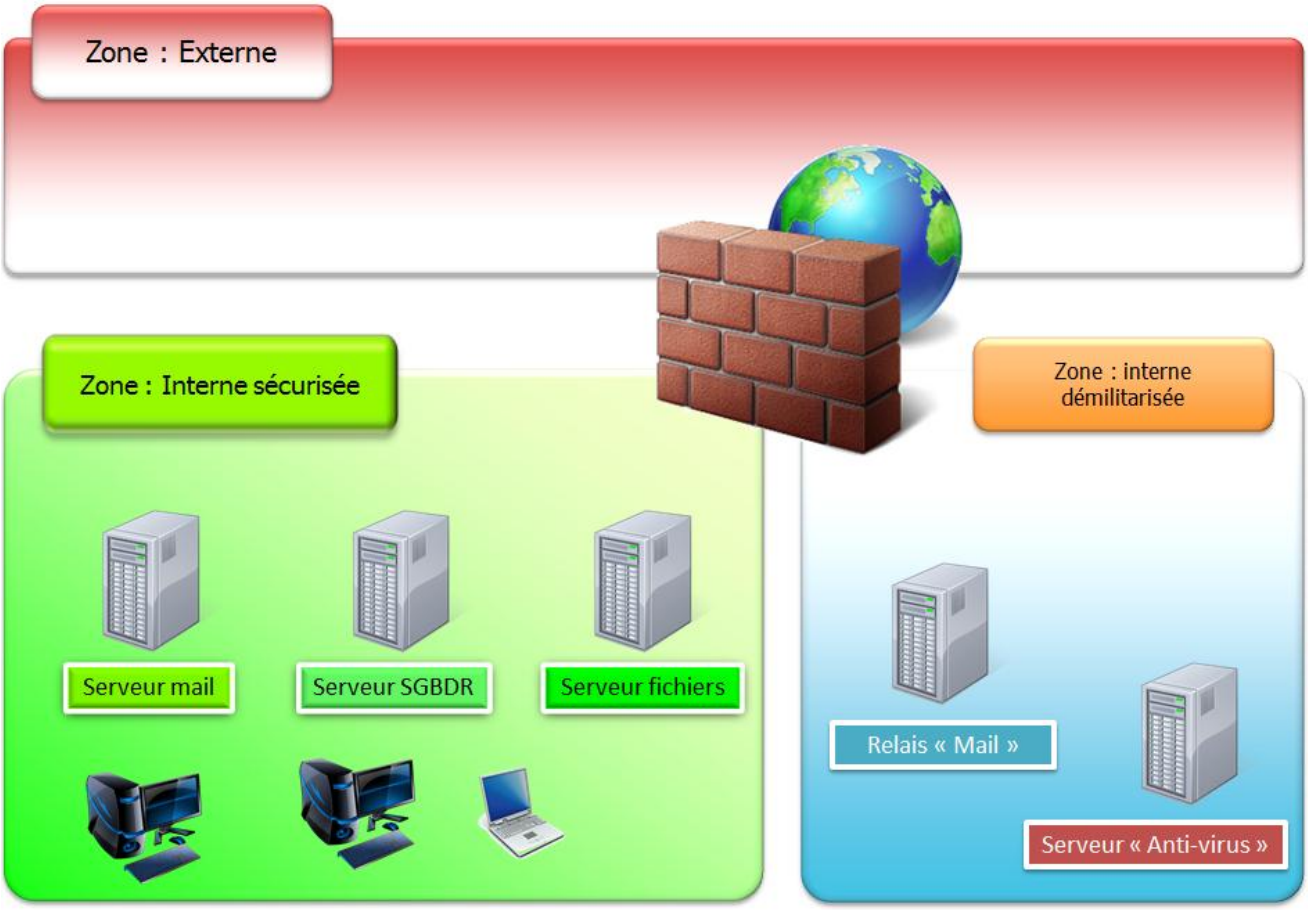
Astuce : Il est impératif de « **Chrooter », dès que cela est possible, les services sur des systèmes** *Nix : la compromission sera ainsi localisée.

Partant de ce concept il n'est pas compliqué de comprendre **qu'il est préférable qu'un pare-feu ne fasse que ce qu'il sait bien faire : du filtrage de paquet, en couche 3 et 4**.

Néanmoins nous verrons par la suite qu'en ces temps de restriction budgétaire les constructeurs proposent de plus en plus des produits travaillant également sur d'autres couches (Ex. en couche 7 L7, les UTM).

Règle d'isolement

Le principe de l'isolement est un raccourci pour dire que certaines **zones du SI** ne doivent pas être accessibles de l'extérieur, par qui que ce soit. Si cette règle est parfaitement mise en œuvre, elle garantit (dans une certaine mesure tout de même …) qu'aucune attaque ne peut arriver dans la zone isolée sans une action provenant d'un système de la zone en question. Elle présente cependant l'inconvénient de complexifier bien des opérations qui semblent naturelles.



Si on considère le scénario classique ci-dessus.
On s'aperçoit que pour recevoir un mail provenant de l'extérieur il faut que le « Serveur de mail » de la zone interne (type Exchange) effectue la « ramasse » du courrier sur le « Relais mail » situé en DMZ : on respecte ainsi la règle d'isolement.
En effet seul le **« *Serveur mail* » *interne*** est autorisé à communiquer dans le **sens « Zone : interne sécurisée » vers « Zone : interne démilitarisée (DMZ) »** sur le serveur le ***Relais « Mail »***.

Nous verrons plus loin qu'il existe une multitude de type de zones permettant de répondre aux multiples cahiers des charges en ce que concerne les règles d'isolement.

Mix des technologies

Cette règle consiste à dire que si une vulnérabilité est trouvée sur un équipement de sécurité, le seul salut est dans la mise en œuvre, quelque part dans la chaine de communication, d'un élément ayant les mêmes fonctionnalités, mais s'appuyant sur une autre technologie.

Cette règle induit une contrainte au niveau de l'exploitation : il faut maitriser, maintenir deux technologies (ou Appliance) différentes.

Néanmoins il ne faut pas oublier qu'au moins 75% des pare-feu actuels se basent sur un noyau Linux …
Si ce dernier présente une faille connue non patchée par le fabricant ou inconnue, je vous laisse entrevoir l'étendue des dégâts sur votre pare-feu
C'est pour cela qu'il peut être judicieux de choisir un pare-feu à base de **GNU/Linux en frontal** et un autre s'appuyant sur du **OpenBSD en deuxième pare-feu**.

Note : OpenBSD est un très bon choix de pare-feu car il s'agit d'un OS beaucoup moins connu, donc moins sensible aux « Script kiddies » et autres « hackers du dimanche ».

Dans l'exemple ci-dessus on aura par exemple pris soin de choisir :

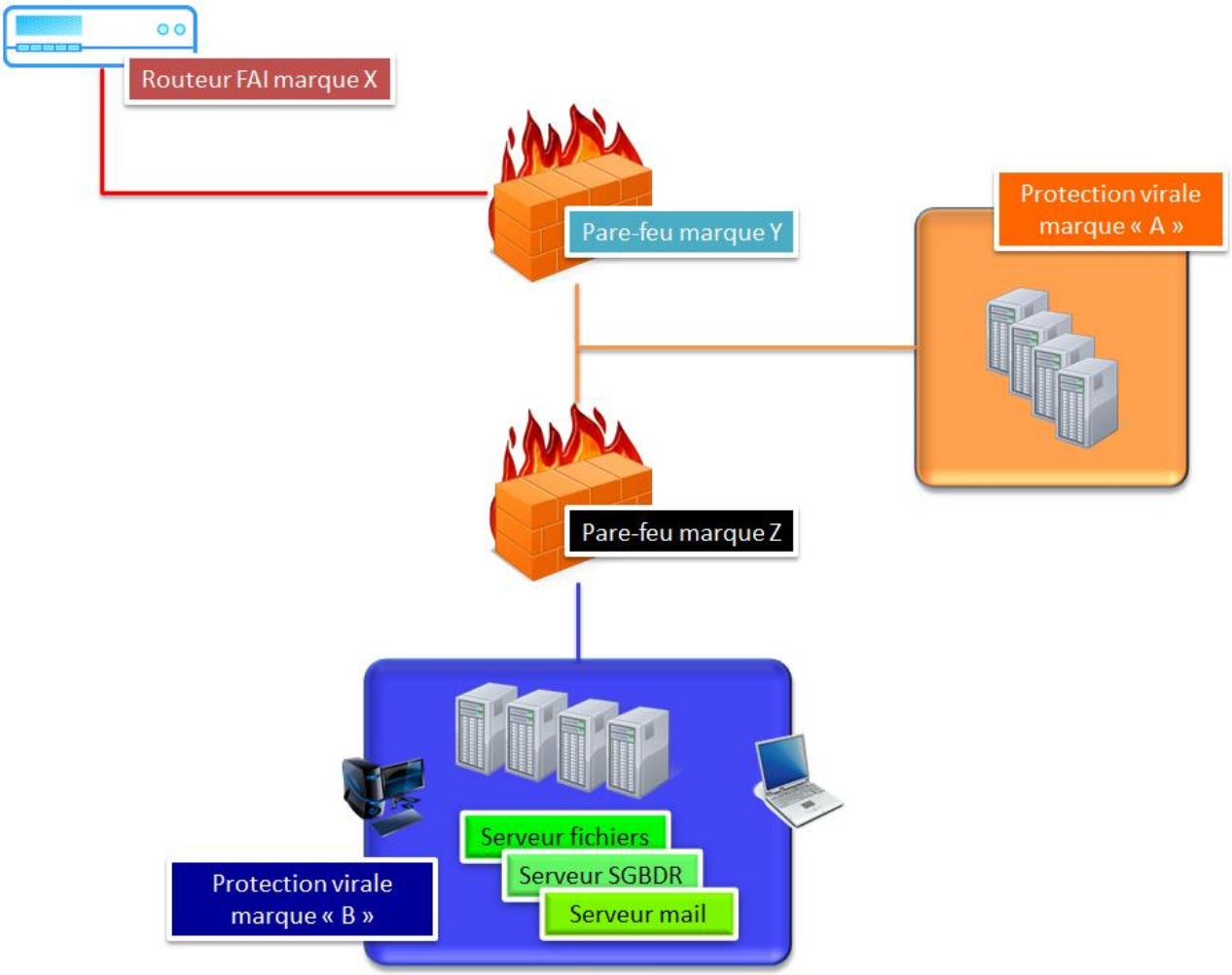
- un serveur de messagerie interne « Microsoft Exchange » (moteur SMTP Microsoft)
- un relais de messagerie en DMZ « Postfix » (moteur SMTP GNU/GPL)

Dans l'exemple suivant on peut voir un bon exemple en termes de mix des technologies.
La compromission du « Pare-feu de marque Y » suite à :

- la présence d'une faille « 0 day »,
- la découverte de votre mot de passe d'administration,
- etc.

… sur ce dernier **n'entrainera pas obligatoirement** celle du « Pare-feu de marque Z »
Il en sera de même pour l'anti-virus. Si un virus, malware etc. (contenu dans un mail) n'existe pas dans la base de signatures de la « Protection virale de marque A » **peut-être** sera-t-il connu dans la base de signatures de la « Protection virale de marque B ».

Il s'agit là du minima pour assurer un début de sécurité.



« No information leak »

On peut traduire cette règle par « aucune information ne doit filtrer ».
Cela est d'autant plus paradoxal que la majeur partie du temps elle doit s'appliquer à des éléments qui doivent fournir de l'information au « monde extérieur » (serveur Web, Mail etc.).
On peut donc adoucir cette règle en disant plutôt :

Seules les informations explicitement désignées comme « devant être accessibles » peuvent sortir

Bien souvent on voit des services informatiques mettre en œuvre un pare-feu en réalisant une installation par défaut à savoir :

- mot de passe par défaut : là c'est très grave,
- blocage de tous les flux entrants : soit,
- mais surtout, et c'est ce qui nous intéresse ici, **autorisation de tous les flux sortants.**

Or bien souvent la compromission intervient à l'intérieur de la zone sensée être protégée. En gros la zone que vous estimiez sûre est en fait une zone ultra vérolée …
Dans le cas d'une installation de pare-feu par défaut l'assaillant pourra exfiltrer sans la moindre difficulté une masse considérable d'informations sensibles vers l'extérieur … grâce aux éléments compromis de votre SI (serveurs, station de travail etc.).

Pire l'assaillant pourra se servir de votre SI comme principale plateforme de tir vers d'autres cibles potentielles internes ou externes : **protégez également les flux sortant du SI**.

De plus il est impératif de rendre le moins bavard possible les briques de votre SI en :

- Désactivant les bannières par défauts des serveurs mail, web, SSH, pare-feu, proxy, IDS etc.,
- Sécurisant vos serveurs DNS (attention aux transferts de zones, etc.),
- Sécurisant vos serveurs mail,
- Faites en sorte que vos serveurs en sachent le moins possible sur les autres serveurs concomitants,
- Etc.

Les mises à jour

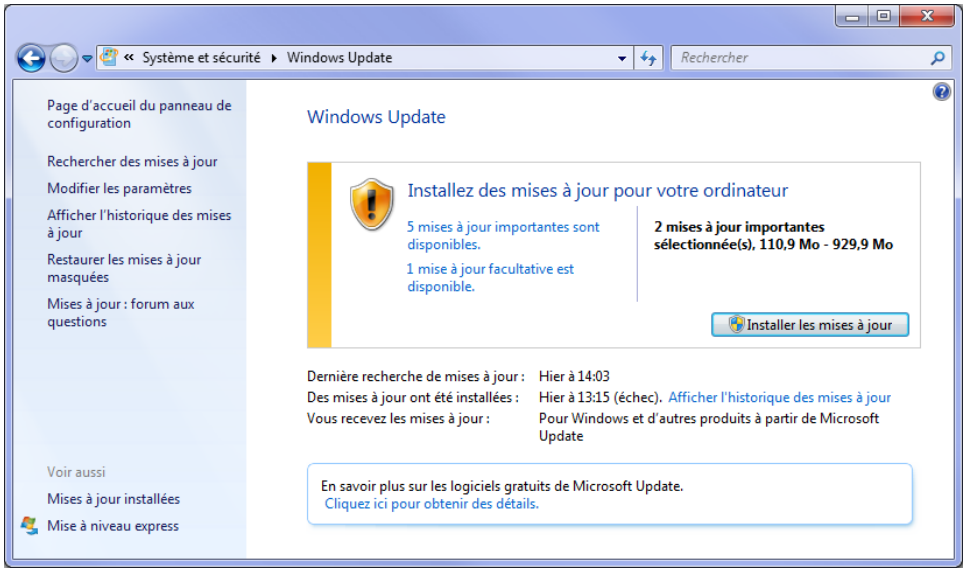
Tout comme les sauvegardes**, la gestion stricte des mises à jour des briques du SI (pare-feu, firmware, signature et moteur virale, patch de sécurité système etc.)** est une tâche ingrate néanmoins elle est vitale et constitue la base de l'exploitation d'un système d'information sain et sécurisé.

Cette règle est d'autant valable si elle s'applique aux briques du SI exposées aux flux provenant de l'extérieur.

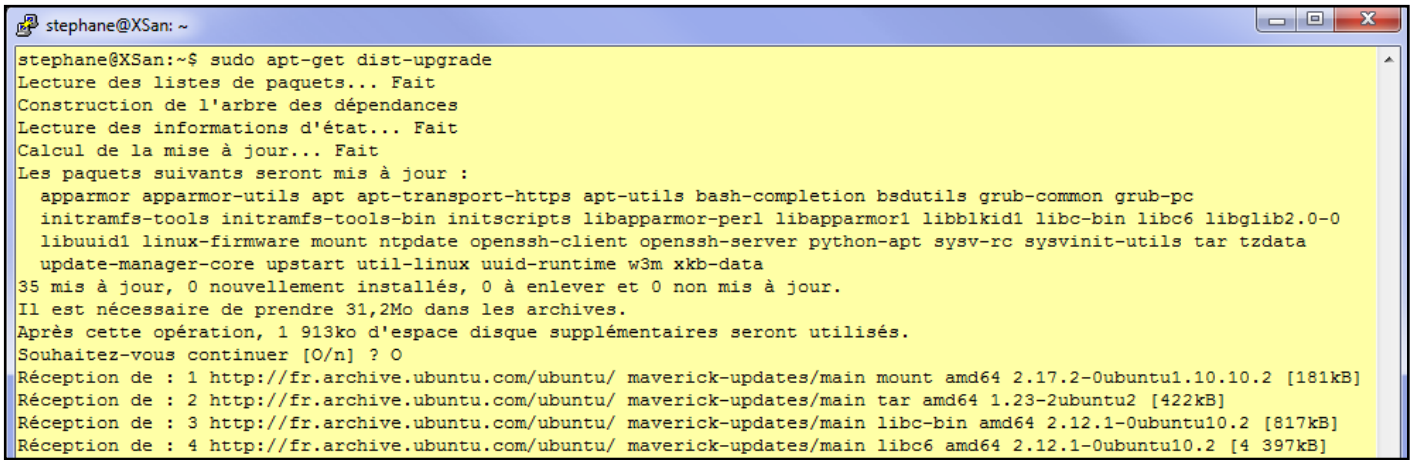
Chaque jour des failles de sécurité exploitables (on trouve en quasi-simultané les « proof of concept » pour les exploiter) sont découvertes sur la plupart des produits du marchés (du pare-feu en passant par le switch et finissant par notre cher système d'exploitation favoris dont le service IIS est truffé de failles …)

De nos jours effectuer une installation de base d'une brique du SI et ne plus s'en occuper n'est pas seulement à considérer comme une hérésie, c'est une provocation.

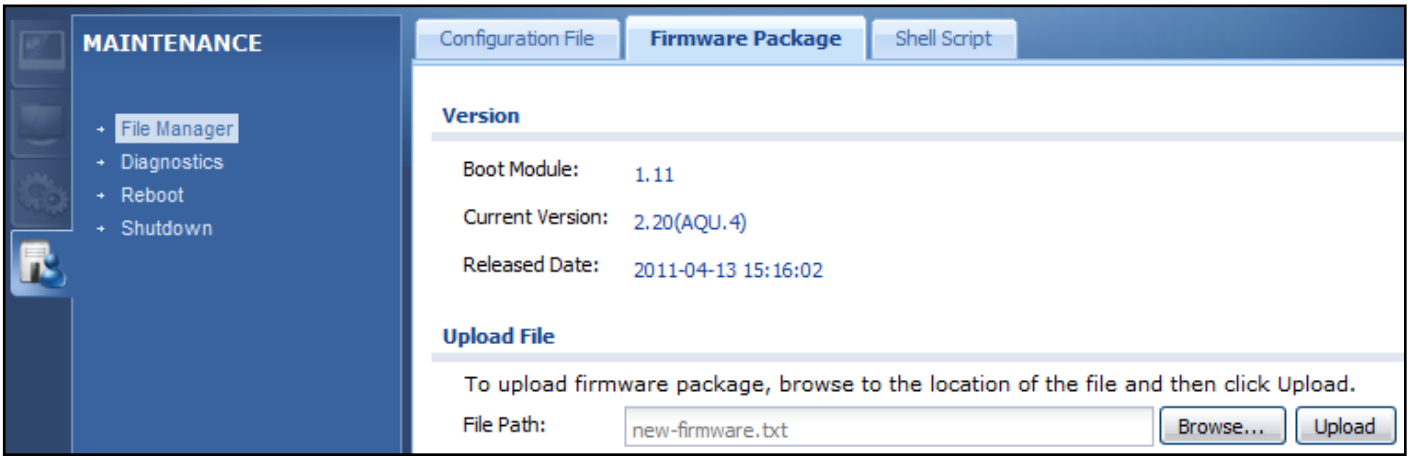
Sous Windows :



Sous GNU/Linux :



Sur un pare-feu matériel :



Finissons cette partie en signalant que les mises à jour ont-elles aussi leurs limites, pourquoi ?
Pour une raison défendable vous êtes obligé de garder ce bon vieux serveur sous Windows NT4, il est en SP6a (dernier en date), les correctifs « Rollup sont appliqués », et de toute manière Microsoft ne supporte plus cet OS et ne diffuse plus de mise à jour à son sujet …
Mais voilà : NT4 ne parle pas Kerberos, et ne sait pas ce qu'est un KDC …

Votre niveau de sécurité de votre réseau est donc abaissé à celui de … NT4 surtout si ce serveur accède aux ressources de votre domaine AD en 2000 ou supérieur (et son légendaire NTLM, protocole parfaitement piratable, à cause du hachage trop faible, avec des outils style CAIN & ABEL).

Stratégie de mot de passe

Les règles ne sont plus à définir, tout administrateur système ou réseau doit avoir conscience du fait que les mots de passe :

- ne doivent jamais être laissé par défaut (SGBDR, pare-feu, Switch, Sondes, Outils divers etc.)
- doivent avoir une durée de vie limitée et périodicité (1 mois est judicieux, 24 mois de retention),
- doivent respecter certaines règles de complexité (longueur minimale, non basé sur des mots des dictionnaires, caractères spéciaux etc.),
- ne doivent jamais être stockés sur papier accessible à tous (un logiciel comme KeyPass GNU/GPL vaut mieux qu'un Post-it, une feuille de papier volante ou un carnet à spirale …)

Le « Hardenning »

Mais qu'est-ce que le « Hardenning » ?

Simple :

Il s'agit d'un processus visant à sécuriser un système afin de le protéger contre tout accès non autorisé, tout en prenant des mesures pour rendre le système d'exploitation plus fiable. Généralement tout ce qui est fait au nom du « **Hardenning** » **assure que le système d'exploitation soit à la fois sécurisé et fiable**.

Le « Hardenning » est souvent nécessaire après **une installation par défaut** dit OOB : "Out Of the Box ».
En effet **certains systèmes d'exploitation ont tendance à être conçus pour être principalement facile à utiliser, plutôt que sécuritaire**. On se retrouve donc avec des failles potentielles de sécurité dès l'installation.
A contrario des systèmes sont, par défaut, déjà conçus dans cette optique : OpenBSD en fait partie.

Utilisation systématique du cryptage

Dès que vous pouvez utiliser des communications chiffrées faites-le !

En 2011 il est **inconcevable** de voir encore des administrateurs systèmes UNIX, GNU/Linux ou des techniciens réseaux travailler encore en **Telnet**.

Cela est également vrai pour les Appliance/éléments réseaux en sous-traitance : un VPN hébergé par un fournisseur d'accès peut très bien être sous le coup d'une faille généralisée (Ex. : faille IOS de Cisco en 2003) et donc ne **plus proposer le niveau de sécurité stipulé dans les contrats**.

Dès cet instant vous serez content de **travailler en SSH ou SSL, votre prestataire n'assurant plus le minima en termes de sécurisation de vos flux réseaux** !

Voici des moyens de chiffrement relativement robustes à l'heure où sont écrites ces lignes :

- SSH,
- SSL,
- IP Sec.

Oubliez le **Wifi** ! C'est une passoire, en WEP 10 mn suffisent pour faire parler ce protocole.
En WPA ce sera plus dur à casser mais certains sont déjà parvenus à mettre par terre des hot-spots protégés par ce protocole dans sa version numéro 2.

Voici un tableau des principaux protocoles à utiliser pour administrer ou superviser vos équipements avec un minimum de risque de compromission :

Plateforme	Protocole
GNU/Linux – UNIX	SSH
Windows	RDP (version 7 ou supérieure)
SWITCH	SSH (ou directement via port console)
Pare-feu	SSH, Console, HTTPS

Présence d'un expert sécurité sur chaque projet informatique

En effet combien de projet informatique voit le jour sans qu'aucun consultant ou expert en sécurité n'y soit associé ?
La sécurité doit être prévu en phase préparatoire d'un projet, pas en phase finale.
Mais disposez-vous d'un référent compétent et immédiatement opérationnel en matière de sécurité informatique dans vos ressources ?

Auditez et surveillez votre SI

De plus sachez que des audits de sécurité effectués par des intervenants extérieurs réguliers vous permettront d'avoir une vision plus claire du niveau de sécurité de votre SI. Vous pourrez ainsi prendre les mesures adéquates en toute connaissance de cause.

N'hésitez pas non plus à vous appuyer sur une équipe/personne experte en sécurité. Cette personne/équipe correctement formée pourra :

- Superviser et surveiller efficacement vos éléments de sécurité (sondes, NIDS, pare-feu, proxy, ~~annuaire~~…),
- Faire des tests d'intrusion en « White, Grey et Black Box »,
- Assurer la veille technologique (consultation des sites réputés et revues spécialisées ➔ MiSC),
- De par sa connaissance du site être réactif en cas de sinistre.

Comme nous l'avons signalé en introduction on peut même bloquer des attaques encore inconnues si notre pare-feu ne laisse passer que les comportements normaux et uniquement eux.
Un trafic n'étant pas conforme à la RFC peut être les prémices d'un nouveau type d'attaque : certains pare-feu haut de gamme peuvent bloquer ce genre d'attaque.
En fonction des données à sécuriser il ne faut donc pas hésitez à se doter de pare-feu haut de gamme disposant des dernières avancées en matière de détection de menaces informatiques.

Le plan de reprise après sinistre

Ici le but n'est pas de donner la démarche pour élaborer un plan de reprise après sinistre : cela dépasse largement le cadre de ce cours. Par contre il est important d'intégrer cette démarche dans la mise en œuvre de votre pare-feu.

Aujourd'hui il est difficile de nier le fait que les entreprises sont de plus en plus dépendantes de leur système d'information et par conséquent, de plus en plus menacées en cas de défaillance de ce dernier.

Dans le domaine de la sécurité liée aux attaques malveillantes, **le risque est plus ou moins bien estimé, mais paradoxalement assez mal appréhendé**. Le constat est simple : la mise en œuvre d'un plan de secours pour assurer la continuité de services, est souvent jugée trop complexe et coûteux.

Autre constat alarmant, la plupart des **entreprises qui possèdent un PRA (Plan de Reprise d'Activité), ne testent pas le processus de remise en état opérationnel du SI**, comme si la mise en place du système de secours ne pouvait pas subir lui-même de défaillance et que le système d'information n'évoluait jamais.

Partant de ce constat il est impératif de prendre le temps de réfléchir sur les conséquences que peuvent entraîner la compromission de telles ou telles briques de sécurité du SI. Et ensuite de disposer **d'un « story board » de reprise, d'une solution palliative rapide à mettre en œuvre**.

Pour se faire ayez le minimum pour un élément actif réseau : la sauvegarde de votre configuration à l'abri. Vous pourrez ainsi :

- Dans un premier stocker le pare-feu compromis pour analyse,
- Remettre à zéro votre pare-feu (effaçant la plupart des backdoor ou code malicieux présents),
- Réinjecter une configuration en durcissant votre politique de filtrage (offline) dans un premier temps (le temps d'analyser l'origine de l'attaque).

Ensuite bien entendu il sera nécessaire de comprendre pourquoi le sinistre a eu lieu afin de ne pas se retrouver devant la même situation, autrement dit **apprendre par l'erreur**.

Les **journaux systèmes (envoyé sur un système type SYSLOG déporté) seront dans ce cas de puissants atouts**, bien qu'ils puissent être, eux aussi, compromis !

En sécurité informatique la vie d'un expert, vu le niveau technique actuel de la cyber-guerre informatique qui se joue actuellement, sera irrémédiablement faite d'erreurs et de remises en question fréquentes.

N'oublies pas : il suffit d'une fois, une seule compromission et c'est tout l'édifice qui s'écroule. Il faut donc être rigoureux et rester vigilants à tout instant en matière de sécurisation des SI. Ce sont les qualités requises pour intégrer une équipe chargée d'assurer la sécurité du SI

Rôle du pare-feu

Parmi les briques permettant la sécurisation d'un SI il en est une qui revient souvent à l'esprit de tout administrateur système ou réseau : le pare-feu.
Hélas ce sentiment de sécurité, une fois le précieux installé, est bien trop souvent exagéré.
On entend trop souvent dire : « On a un **pare-feu** à X000 € **donc nous sommes protégés** » ….

Bien entendu cela est **complétement faux.**

Il faut avoir conscience que le **pare-feu** constitue un des éléments de votre **défense parmi d'autres**.
L'architecture du réseau, les services qui tournent sur vos serveurs, les systèmes d'exploitation sont tout aussi importants. La **compromission** de l'un, aura de forte chance d'entrainer celle des autres via des techniques aussi simple que le **rebond**.
De plus un pare-feu laisse passer un trafic mais n'examine pas forcément le contenu de ce trafic …

De nos jours définir le rôle exact d'un pare-feu est impossible. Si vous consultez 20 constructeurs de pare-feu vous obtiendrez 20 réponses différentes en fonction du produit qu'ils voudront vous vendre.

En fonction du budget que vous allez allouer pour l'achat de votre produit vous pouvez vous retrouver avec :

- un produit gratuit faisant du filtrage de paquet basique (style NetFilter, paquet Filter, etc.),

- ou bien avec un véritable UTM (Unified Thread Management) coûtant quelques milliers d'euros.

Partant de ce principe donnons une définition du pare-feu basique tel que l'on peut le trouver dans un OpenBSD (Packet Filter : pf) ou GNU/Linux (NetFilter : NF) mise en œuvre dans un ordinateur type x86 (PC).

Ce qu'il fait …

Le pare-feu était, jusqu'à ces dernières années, considéré comme une des pierres angulaires de la sécurité d'un réseau informatique. De nos jours il perd en importance au fur et à mesure que les communications basculent vers le HTTP sur SSL, court-circuitant tout filtrage. **Il permet d'appliquer une politique d'accès aux ressources réseau (serveurs, etc.) via des règles clairement définies**.

Il a pour principale tâche de **contrôler (autoriser ou bloquer) le trafic entre différentes zones de confiance**, en **filtrant les flux de données qui y transitent**. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).

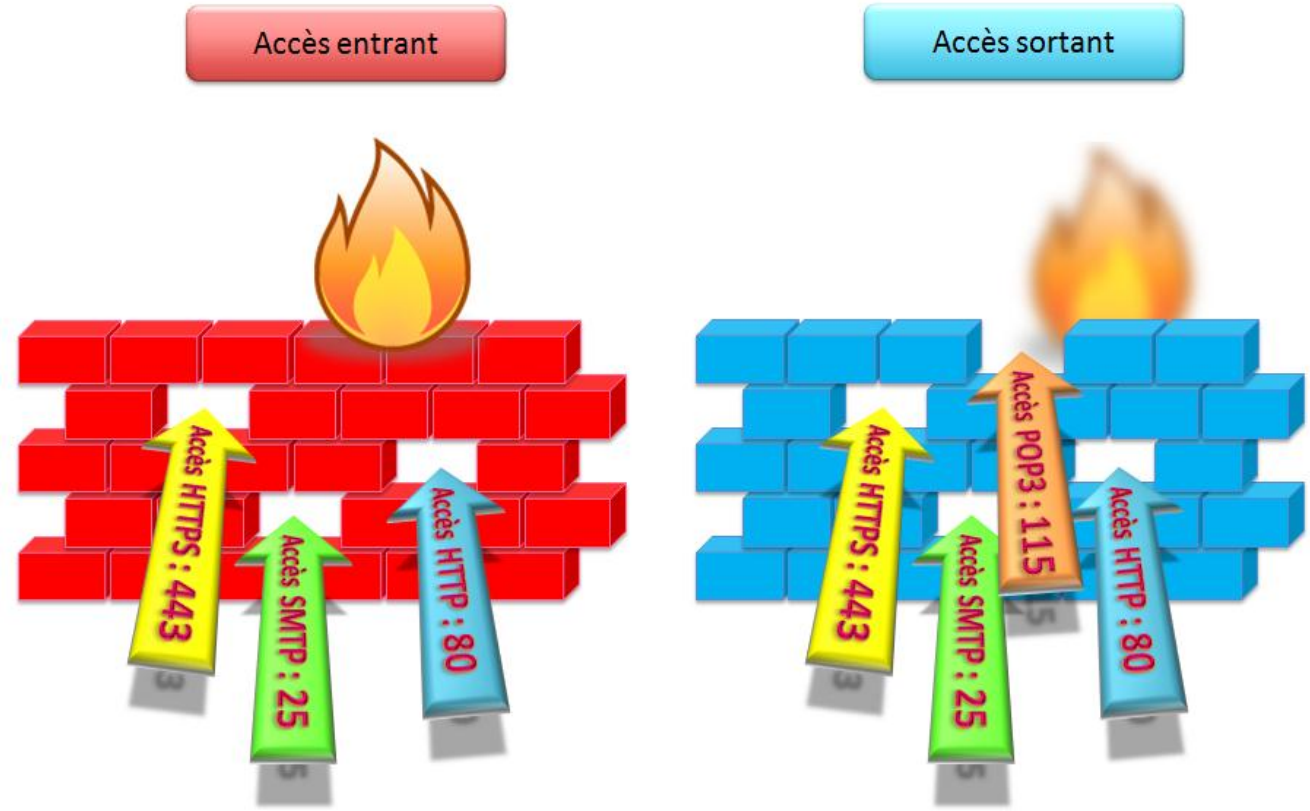
Le but ultime est de **fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance,** grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.

Le filtrage se fait selon divers critères, les plus courants sont :

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ;
- les options contenues dans les données (fragmentation, validité, etc.) ;

- les données elles-mêmes (taille, correspondance à un motif, etc.) ;
- les utilisateurs pour les plus récents.

On s'aperçoit donc que le pare-feu permet d'autoriser ou bloquer divers flux réseaux entrants comme sortants :



En plus de cela un bon pare-feu se doit d'avoir une pile TCP/IP robuste et fiable, idéalement exempt de failles de sécurités. La plupart des pare-feu savent se prémunir des malformations de paquets IP et autres joyeuseries énumérées précédemment.

… et ne fait pas.

En regardant le schéma précédent il est aisé de comprendre que si nous lançons **une attaque (**via l'accès entrant **SMTP qui est ouvert**) visant le serveur de messagerie (ou relais) de l'entreprise **nous ne nous attaquons pas directement au pare-feu aussi bien configuré ou performant soit-il** mais bel et bien à la machine accessible par le port TCP 25 …
Donc pare-feu ou pas **ce sera la robustesse du relais mail qui sera mise à l'épreuve, pas celle du pare-feu**.

Allons plus loin. Vous ne souhaitez pas que vos utilisateurs du réseau interne puissent prendre la main à distance sur leur PC personnel, chez eux.
Alors vous décidez de **mettre en place un proxy, vous configurez votre pare-feu en conséquence**.
Dommage mais des produits comme TeamViewer vont permettent **d'encapsuler le protocole** de déport d'affichage à distance **dans des paquets HTTP(S)** … donc de passer outre votre pare-feu
Le bureau à distance de Microsoft usant du protocole RDP peut également être encapsulé dans du HTTPS, RD HTTP Gateway : même punition, le flux passe sans souci votre pare-feu.
On voit donc que le rôle du pare-feu n'est plus suffisant dans ces quelques cas de figure, or il en existe une multitude.

Types de pare-feu

Par technologies

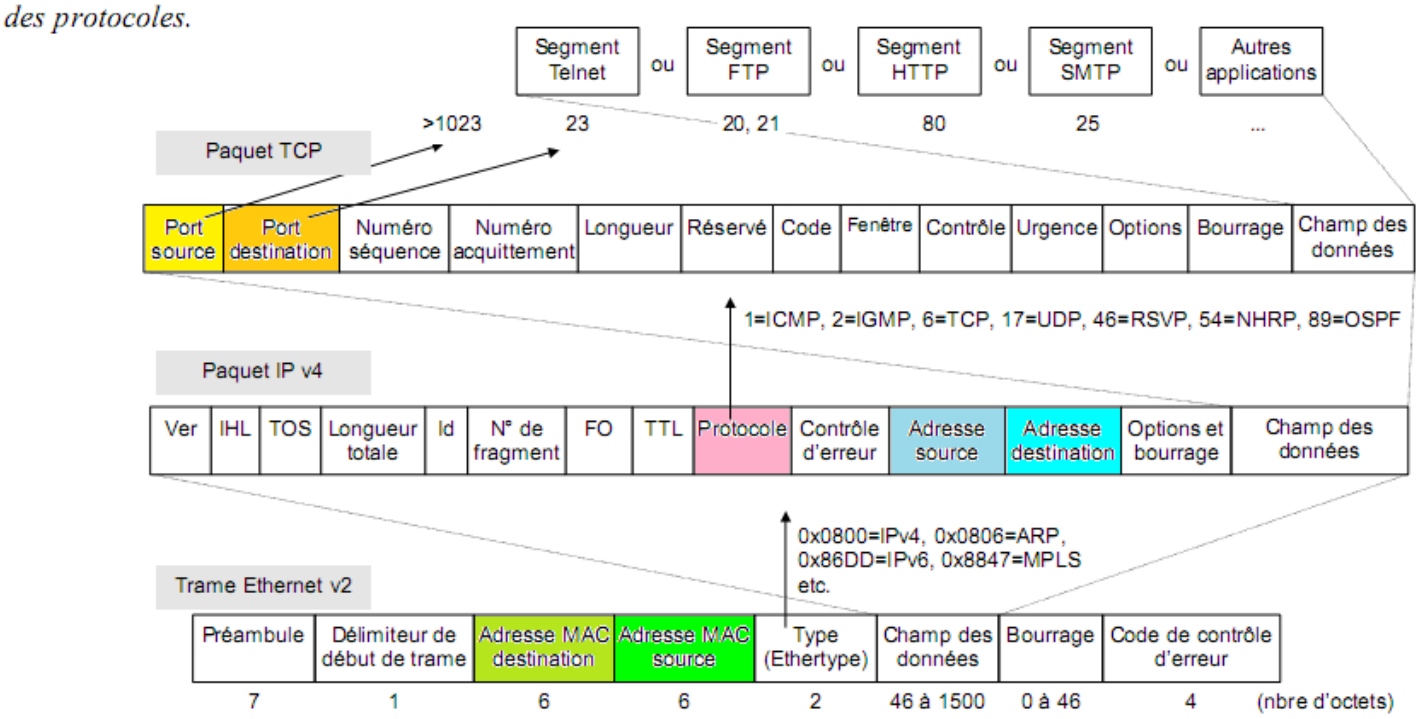
Filtre de paquets

La protection la plus évidente et la plus ancienne consiste à placer, entre un sous-réseau à protéger et ses attaquants potentiels, un filtre de paquets. Un tel système peut prendre notamment la forme d'un routeur filtrant (via les ACL) ou d'un pare-feu dédié. Ce système est capable d'autoriser, ou au contraire d'interdire, le passage de paquets en s'appuyant, dans la majorité des cas, sur des critères comme suit :

- Les adresses IP sources/destinations d'un paquet IP,
- Le type de paquet (UDP, TCP …),
- Les ports TCP/UDP sources/destinations d'un segment TCP ou d'un paquet UDP.

Rappel :

Le principe de l'encapsulation des protocoles.



Cette solution est notamment utilisée pour empêcher l'accès à certains services depuis l'extérieur ou vers l'extérieur du réseau. Elle contribue également à la prévention des attaques contre les applications fondant entièrement leur authentification sur l'adresse IP de l'émetteur de chaque requête, qui s'avère, dans certaines situations, aisément falsifiable.
Ainsi, il n'est pas normal, au niveau du routeur reliant un réseau à Internet, de transmettre un paquet IP émis depuis Internet à destination de ce réseau, mais ayant néanmoins une adresse IP source appartenant à ce même réseau.

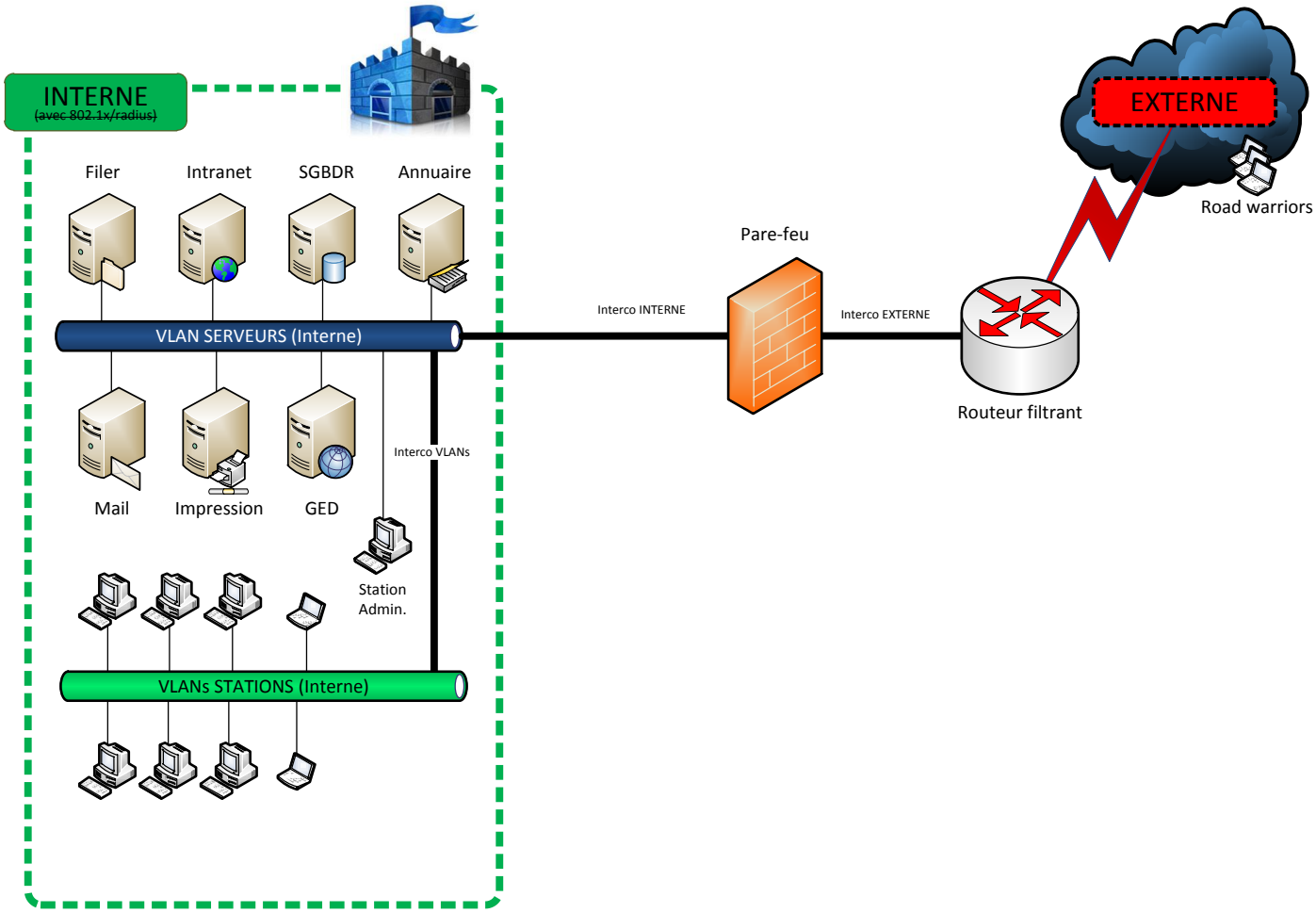
Un pratique usuelle consiste à ne pas transmettre les paquets « destinés à » ou « émis » par des adresses de broadcasts ou multicasts afin de se protéger des DoS (Denial of Service), ou servir de relais à ces types d'attaques.

De plus si cette approche offre une défense simple et efficace, elle manque de souplesse pour que sa mise en place en protection d'un réseau, dans la majorité des cas, ne s'avère pas bloquante pour le bon fonctionnement des systèmes de réseau concernés.

Vous l'aurez compris ce genre de protection est nécessaire mais pas suffisante, on veillera donc à mettre en œuvre ce genre de filtrage, qui doit rester simple (le FTP est trop délicat à gérer avec ce genre de filtrage basique), en amont, sur le routeur du site à protéger (avant le pare-feu donc).

Généralement votre prestataire de lien réseau distant (WAN) doit vous fournir cet équipement.

Exemple de routeur filtrant :



“Stateful Packet Inspection” : filtre à état

La technologie·’’Stateful Packet Inspection’’ repose sur deux principes fondamentaux :

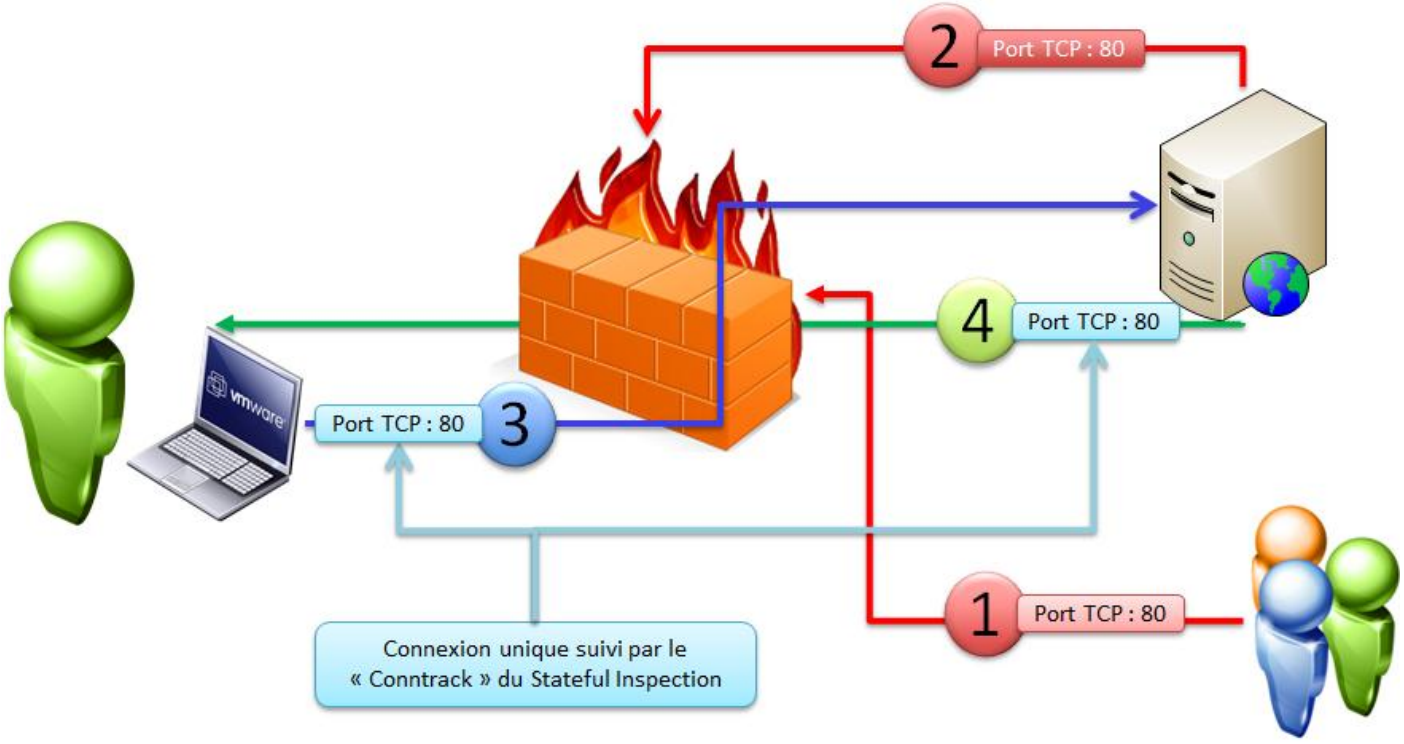
- Le premier est l’analyse complète du paquet avant son arrivée dans la couche réseau du système hébergeant le firewall (PREROUTING sur Netfilter),
- Le second est la définition et le maintien de tables des connexions autorisées (table « Conntrack » pouvant supporter un nombre défini de suivi de connexions, sessions simultanées d’un pare-feu).

L'intérêt d'une analyse effectuée en aval de l‘entrée en couche 3 (indispensable pour les opérations de routage) est de s’affranchir des risques d'intrusion liés aux potentielles vulnérabilités ou attaques sur la stack IP du firewall … ~~tant que cette attaque est perpétrée via un paquet rejeté, compte tenu de la politique de sécurité.~~

Cette analyse est également intéressante dans la mesure où elle est effectuée sur l'ensemble du paquet, ce qui permet d’implémenter quelques fonctions de filtrage intéressantes au niveau de certains protocoles (à la proxy), de gérer les tables de connexion (voir ci-dessous) et surtout de gérer les protocoles « complexes » du type FTP.

La gestion des tables de connexion (table « Conntrack ») consiste à maintenir à jour une liste des connexions actives et autorisées Pour schématiser disons qu’une telle table précise qu'à l'instant *t* une connexion est autorisée entre la machine A, sur le port X, vers la machine B, sur le port Y.
Les numéros de séquence sont également pris en compte afin de restreindre les risques de « Spoofing » via prédiction de séquence. Les entrées sont initialisées à l'ouverture de la session **TCP** (pour une connexion autorisée) et supprimées à sa **fermeture ou à l'expiration d'un délai** spécifique.
La gestion de telles connexions en **UDP (mode non connecté)** est effectuée uniquement en considérant qu’une requête UDP est caractéristique d‘une ouverture de session. La connexion s'achève à l'issue d'un **délai prédéterminé**. Cette fonction présente l’avantage de gérer nativement les flux retours, et par conséquent, d'alléger les règles mises en place sur le pare-feu (chose inexistante sur IPchain et les kernel 2.2 Linux, cf. les configurations fastidieuses des premières FireBox I & II de WatchGuard).
En outre, elle limite considérablement les risques de « hijacking » de session.

SPI (**S**tateful **P**acket **I**nspection) en action :



Dans l'exemple ci-dessus il n'est pas nécessaire d'autoriser l'entrée de tout segment TCP ayant 80 pour port source (connexion initiée avec numéro 3 et retour sur numéro 4) : seul l'établissement de connexions TCP à la demande de système du réseau protégé doit être permis. Ensuite, la connexion étant légitimement autorisée, le pare-feu laissera passer les données retournées par le serveur distant sur le port 80, et cette autorisation prendra fin lors de la fermeture de la connexion TCP/80 par le client.

En revanche veuillez noter qu'une connexion initiée depuis l'extérieur vers le pare-feu est irrémédiablement stoppée par défaut.

Dans le meilleur des cas c'est ce type de pare-feu que vous parviendrez à mettre en œuvre un transformant une distribution GNU/Linux généraliste en pare-feu.
Donc pas vraiment satisfaisant, car votre pare-feu ne sera pas très intelligent face aux attaques présentes sur Internet.

Voici un autre exemple de table de suivi d'état d'une connexion avec Netfilter :

```
tcp      6 117 SYN_SENT src=192.168.1.6 dst=192.168.1.9 sport=32775 \
     dport=22 [UNREPLIED] src=192.168.1.9 dst=192.168.1.6 sport=22 \
     dport=32775 [ASSURED] use=2
```

Cet exemple contient toute l'information gérée par le module conntrack pour savoir dans quel état se trouve une connexion.
Tout d'abord, il y a le protocole, ici **tcp**. Ensuite, encore le protocole mais codé en décimal **6**.
Après cela, on voit combien de temps doit survivre cette entrée de conntrack. La valeur à cet instant est de **117 secondes**, elle est décrémentée régulièrement jusqu'à ce qu'on voit à nouveau du trafic pour cette connexion. Cette valeur est alors réinitialisée à la valeur par défaut pour l'état en question à cet instant donné. Ensuite vient l'état actuel de cette entrée

Dans le cas présenté ci-dessus, on visualise **une connexion qui est dans l'état *SYN_SENT***. La valeur interne d'une connexion est légèrement différente de celles utilisées en externe avec iptables. La valeur SYN_SENT indique que **cette connexion a seulement vu un paquet TCP SYN** dans une direction.

Puis, on voit l'adresse IP source, l'adresse IP destination, le port source et le port destination.

Arrivé à ce niveau, on voit un **mot-clé spécifique qui signale qu'aucun trafic n'a été observé en retour** (UNREPLIED) pour cette connexion.
Enfin, on voit **ce qui est attendu pour les paquets en réponse** (ASSURED). Entre autres, l'adresse IP source et l'adresse IP destination (qui sont inversées, puisque le paquet attendu doit être dirigé dans l'autre sens).
La même chose s'applique au port source et port destination de la connexion. Ces valeurs nous intéressent particulièrement.

Les entrées du traçage de connexion peuvent prendre un ensemble de valeurs différentes, toutes spécifiées dans les en-têtes de conntrack et disponibles dans les fichiers linux/include/netfilter-ipv4/ip_conntrack*.h.
Ces valeurs dépendent du sous-protocole IP qu'on utilise. Les protocoles TCP, UDP et ICMP correspondent à des valeurs fixées et spécifiées dans le fichier linux/include/netfilter-ipv4/ip_conntrack.h.

Passons à l'indispensable technologie qu'est le filtrage de flux : le proxy.

Filtrage applicatifs des flux (proxies)

Dans le premier cas, le firewall est doté **d'agents spécifiques à chaque protocole applicatif** (FTP, Telnet, SMTP;HTTP, etc,). Ces agents ont pour fonction de valider un certain nombre de critères : les adresses IP source et destination, les commandes passées (telles que GET ou POST pour HTTP), voire dans une certaine mesure le contenu. Cela présente l'avantage évident d'être à même d'effectuer un filtre très précis sur chacun des paquets émis, et d'être à même de comprendre les spécificités de chaque protocole.

Ainsi, dans le cas d'une communication en FTP, seule la communication sur le port défini par la commande PORT sera autorisée; et uniquement sur la durée du transfert.
De plus, la gestion au niveau applicatif impose le réassemblage des paquets et l'élimination de facto des attaques par fragmentation.

Cette approche présente cependant **deux inconvénients**.

Le premier est une question de **performances**. En dépit de tout ce qui peut être dit, il ne reste pas moins que le filtrage d'un paquet nécessite la "remontée" de toutes les couches jusqu'au niveau applicatif
C'est quand même beaucoup de travail. Quant au fait de proposer une solution fondée sur le filtrage du premier paquet (ou de la première commande) et le « forwarding » implicite des paquets suivants, bien... c'est un peu comme regarder le premier fragment d'un paquet et autoriser les suivants, si vous voyez ce que je veux dire.

Autre inconvénient, la **disponibilité des agents**. Certes, la quasi-totalité des protocoles standards est disponible. Cependant, on commence à rencontrer des problèmes dès qu'il s'agit de protocoles propriétaires ou exotiques. Dans ce cas, le firewall se comporte ni plus ni moins comme un routeur filtrant, faute d'agent adapté.

Nous verrons dans la partie architecture que cette technologie est reprise par les sondes de filtrage de flux, qui elles ne sont dédiées qu'à cela. Cela respecte de facto l'atomicité des fonctionnalités.
Les serveurs « Proxy », NIDS/HIDS (style Squid, Forefront, snort, samhain etc …) sont dédiés au filtrage de flux variés tel que HTTP(s), FTP, SMTP, POP3 etc. et viennent compléter cette panoplie d'éléments sécurisant un réseau.

Nous voyons bien que nous ouvrons une porte vers le concept du **DPI** (Deep Packet Inspection) mais ce n'est pas le propos de ce cours. (cf. http://fr.wikipedia.org/wiki/Deep_packet_inspection)

Par famille

De nos jours il est relativement difficile de classer les pare-feu car ces derniers regroupent l'ensemble ou une partie des technologies vues précédemment.

Si l'on considère, par exemple, un « firmware » comme un logiciel, ce qu'il est au demeurant, alors un « Appliance » est un pare-feu logiciel …
De ce il n'existerait pas de pare-feu matériels : nous savons qu'il n'en est rien.

Il se dégage tout de même 3 familles :

Logiciel :

A la base ce type de pare-feu est venu combler un manque sur des systèmes tel Windows 9X jusqu'à Windows 2000 (dans une moindre mesure XP). En effet le pare-feu logiciel vient se placer sur la pile IP du système qui en est dépourvu, ou bien se substitue au pare-feu déjà intégré.

Voici quelques exemples de pare-feu logiciel (principalement sur plate-forme Microsoft Windows) :

- ZoneAlarm,
- Ashampoo,
- comodo,
- PC Tools Firewall Plus,
- Sygate,
- module pare-feu des anti-virus du commerce,
- etc.

Et sous GNU/Linux, BSD (et dérivée), Mac OS X me direz-vous ?
De tels pare-feu n'existent heureusement pas sous des systèmes GNU/Linux ou BSD. En effet sur ces systèmes le **pare-feu logiciel** (IPchains-Linux, Netfilter-Linux, Packet Filter-OpenBSD, IPFilter-BSD/SOLARIS, IPFirewall-FreeBSD …) **est natif**.
Sur ces systèmes, la pile IP couplée au module de filtrage de paquets assure une base suffisamment solide, fiable et sécurisée pour couvrir 100% des usages allant d'un pare-feu basique à un pare-feu évolué.
Dans le cas où l'intégrateur (fabricant/développeur de pare-feu) souhaiterait modifier cette base, noyau + module de filtrage, il est aisé* de reprendre le code sources (libre) pour en ajuster le comportement à sa convenance ou durcir son comportement.

* : pour des experts en développements noyau et sécurité bien entendu ...

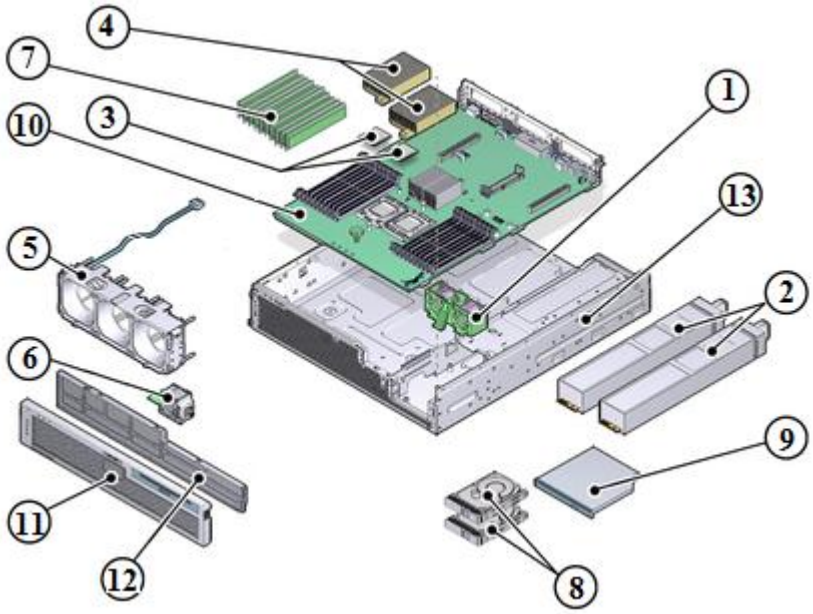
De plus, bien qu'il existe une multitude de distribution GNU/Linux ou BSD (et dérivées) dédiées ou non au « firewalling », il faut avoir connaissance que **la base commune de toutes ces distributions reste le « framework » Netfilter** (développé initialement par Rusty RUSSELL) et **Packet filter (voirIPF).**

Bien que **NetFilter soit un pare-feu logiciel**, nous verrons qu'il constitue la **base de beaucoup de pare-feu matériel**. Evidement un pare-feu comme le *WatchGuard XTM 505* (850€), bien que disposant également d'un noyau Linux et de NetFilter, implémente tout une montagne de modules propriétaires d'analyse comportementale des paquets etc.

Matériel :

Le pare-feu matériel est une solution pare-feu dédiée. Les couches logicielles implémentées sont soigneusement masquées et judicieusement intégrées par le fabricant du pare-feu pour s'adapter parfaitement au matériel choisi.
Un des avantages du pare-feu est matériel est qu'il ne nécessite pas un matériel haut de gamme. De ce fait les pare-feu matériel sont bien souvent dépourvu des éléments mécanique tournants, cause de la plupart des pannes.
Prenons l'exemple d'un intégrateur peu alerte qui aurait choisi un serveur ou pc comme socle matériel pour son pare-feu :

1) Ventilateur alimentation,
2) Alimentation redondante,
3) Processeurs,
4) Radiateur de processeur,
5) Ventilateurs processeur (ici x3),
6) Détail ventilateur processeur,
7) Modules mémoire,
8) Disques durs,
9) Lecteur CD/DVD-ROM,
10) Carte mère,
11) Cache face avant,
12) Filtre poussière,
13) Châssis xU.



Comme on peut le voir sur le schéma ci-dessus bâtir un pare-feu sur du matériel non dédié (serveur, pc, etc.) présente de nombreux points de faiblesse en vue de la haute disponibilité. Ventilateurs, disque durs, cd-rom et autres éléments mécaniques tournants sont beaucoup plus susceptibles de tomber en panne que du matériel dédiés.

Voyons un pare-feu qui limitera au maximum les soucis matériels :

- Une carte mère avec tous les composants intégrés en « fan less » (éventuellement un ASIC dédié crypto qui libérera le processeur central d'une charge parfois titanesque),
- Une alimentation externe (moins de risque de chauffe dans le boitier),
- Stockage de la partie logicielle sur carte « flash » ou SSD.

Bref vous voyez qu'avec un matériel présenté ci-dessous, les risques de casse sont limités au maximum :

Actuellement le pare-feu basique n'existe pratiquement plus, il est toujours couplé à d'autres fonctionnalités indispensables on parle alors d'UTM.

Note : l'UTM brise notre règle d'atomicité des fonctions mais hélas face à la rationalisation des moyens les acteurs du marché se mettent à proposer une gamme toujours plus conséquente de pare-feu de ce type.

Bien entendu les UTM, en fonction du nombre d'utilisateurs/sessions qu'ils seront amenés à gérer, auront parfois une architecture matérielle plus conséquente que celle présentée ci-dessus, c'est-à-dire des ventilateurs de boitiers et ASIC de cryptage en sus. Mais dans ce cas on parle d'équipements pour gros DataCenter ou le recours aux technologies pointues de refroidissement sont de la partie.

Sachez toutefois que pour un **pare-feu pouvant suivre 40 000 sessions en simultanées** on reste encore sur du **matériel « fan less ».** Au-delà les pare-feu sont équipés de dispositifs de refroidissement actifs.

Mais qu'est-ce qu'un UTM exactement ?

Parmi les fonctionnalités présentes dans un UTM, outre le pare-feu traditionnel, on trouve généralement :

- le filtrage anti-spam,
- un logiciel antivirus,
- un système de détection HIDS,
- prévention d'intrusion (NIDS),
- un filtrage de contenu applicatif (filtrage URL).

Toutes ces fonctionnalités sont regroupés dans un même boîtier, généralement appelé « Appliance ».

On trouve parmi les principaux éditeurs de solutions UTM :

- AhnLab : Appliance UTM 1000
- Arkoon : Appliance UTM FAST360
- Astaro : Appliance UTM Astaro (basée sur Suse Linux)
- Check Point : Safe@Office, VPN-1 UTM Edge, VPN-1 UTM (Logiciel), UTM-1
- Citypassenger : Appliance MobileIT
- Cyberoam : Appliances UTM basées sur l'identité
- Edenwall Technologies : EdenWall
- DrayTek : VigorPro
- Endian Firewall
- Fortinet : FortiGate
- funkwerk : packetalarm
- IBM : Proventia
- InfoSet : Leading world
- iWall : éditeur du système genWall
- Juniper Networks
- LokTek
- NetASQ : Appliance UTM NetASQ
- Secure Computing Corporation : SnapGear
- SonicWall : NSA E7500
- Symantec
- Untangle : Untangle Open source
- WatchGuard : Firebox
- Sysun Technologies : Sysun Secure
- Zyxel : ZyWALL USG

En plus il existe **des matériels qui eux sont dédiés pour chaque type de filtrage**, mais là on commence à s'écarter du rôle du pare-feu, mais on respecte à nouveau notre règles d'atomicité des fonctionnalités :

- **Le pare-feu de courrier indésirable**, Spam & Virus Firewall, est une solution matérielle et logicielle conçue pour protéger votre serveur de courriel contre les attaques de spam, de virus, d'hameçonnage (phishing), d'usurpation (spoofing) et de logiciels espions (spyware),
- **Le pare-feu de filtrage Web** est conçu pour renforcer les politiques d'utilisation d'Internet de l'organisation par le filtrage de contenus, le blocage des applications et la protection contre les logiciels espions,
- Le serveur VPN pour les télétravailleurs,

- Le chiffreur réseau,
- L'IDS, HIDS :

  IDS réseau (NIDS)

  Snort
  Bro
  Enterasys
  Checkpoint
  Tipping point

  IDS système (HIDS)
  AIDE
  Chkrootkit
  DarkSpy
  FCheck
  IceSword **(fr)**
  Integrit
  Nabou
  OSSEC
  Osiris
  Prelude LML
  Rkhunter
  Rootkit Unhooker
  Samhain
  Tripwire

- Etc.

Pour finir sur les pare-feu matériel voici comment décrypter une plaquette de pare-feu matériel type UTM :

Les caractéristiques importantes sur lesquelles nous reviendront plus en détail au moment du choix de votre pare-feu proprement dit :

- **Sessions simultanées** (nombre, et connexion/s),
- **Débits de filtrage** du pare-feu avec ou sans les filtrages de flux activé (Proxies, IDS etc.),
- Débits des tunnels VPN,
- Zones configurables,
- NAT disponibles,
- HA (redondance, mise en cluster, etc.),
- Agrégat de bande passante,
- VLAN.

Ensuite bien entendu il faudra toujours vous référez à la documentation technique.
Et plutôt que de lire la traditionnelle plaquette technique du produit, qui sera bien évidement flatteuse sur les fonctionnalités affichées du produit, attachez-vous plutôt à lire **le manuel technique de configuration** (souvent un PDF de quelques centaines de lignes), là vous aurez un **aperçu exhaustif des fonctionnalités et … de leurs limites d'implémentations sur le pare-feu que vous souhaitez acquérir**.



WatchGuard® Model	WatchGuard® XTM 810	WatchGuard® XTM 820	WatchGuard® XTM 830
Ideal For	Main offices/headquarters that need strong security and a solution that offers room for growth.	Main offices/headquarters looking for fast throughput and strong security that grows with changing needs.	Main offices/headquarters that need enterprise-grade performance & security
Hardware			
Model Upgradeable	✔	✔	N/A
Interfaces	10: 10/100/1000	10: 10/100/1000	10: 10/100/1000
DMZs	8	8	8
Security			
Application Proxies	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3, SIP, H.323, TFTP	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3, SIP, H.323, TFTP	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3, SIP, H.323, TFTP
Intrusion Prevention (DOS, DDOS, PAD, port scanning, spoofing attacks, address space probes, and more)	✔	✔	✔
Wireless Models Only	N/A	N/A	N/A
User Authentication with transparent Windows authentication	✔	✔	✔
Performance			
Firewall Throughput**	3 Gbps	4 Gbps	5 Gbps
VPN Throughput**	1 Gbps	1.4 Gbps	1.7 Gbps
XTM Throughput**	1 Gbps	1.3 Gbps	1.6 Gbps
Concurrent Sessions* (bi-directional)	500,000	750,000	1,000,000
VPN Tunnels			
Branch Office VPN Tunnels (Max.)	1,000	2,000	6,000
Mobile VPN with SSL Incl/Max	1,000/1,000	4,000/4,000	6,000/6,000
Mobile VPN with IPSec Client Licenses (Bundled)	600	700	800
Mobile VPN with IPSec Tunnels (Max.)	2,000	6,000	8,000
VPN Authentication	✔	✔	✔

Management			
Centralized (Multibox) Management. Optional licenses enable Drag and Drop VPN and one-touch appliance updates.	4-device WatchGuard System Manager license included with purchase. Appliances activated online receive an automatic 5-device bonus pack.	4-device WatchGuard System Manager license included with purchase. Appliances activated online receive an automatic 5-device bonus pack.	4-device WatchGuard System Manager license included with purchase. Appliances activated online receive an automatic 5-device bonus pack.
Networking Features			
Dynamic NAT	✔	✔	✔
Static NAT	✔	✔	✔
One to One NAT	✔	✔	✔
VLAN	200	300	400
Policy-Based Routing	✔	✔	✔
WAN Failover	✔	✔	✔
Multi-WAN Load Balancing	✔	✔	✔
Server Load Balancing	✔	✔	✔
Traffic Management/QoS	✔	✔	✔
High Availability Active/Active or Active/Passive	✔	✔	✔
Dynamic Routing	✔	✔	✔
VoIP (SIP and H.323) Support	✔	✔	✔
Additional Security Subscriptions			
Application Control	Optional	Optional	Optional
Reputation Enabled Defense	Optional	Optional	Optional
spamBlocker with Virus Outbreak Detection	Optional	Optional	Optional
Gateway AntiVirus/ Intrusion Prevention Service (IPS)	Optional	Optional	Optional
WebBlocker with HTTPS URL filtering	Optional	Optional	Optional
LiveSecurity® Service	1-year, 2-year, and 3-year subscriptions available	1-year, 2-year, and 3-year subscriptions available	1-year, 2-year, and 3-year subscriptions available

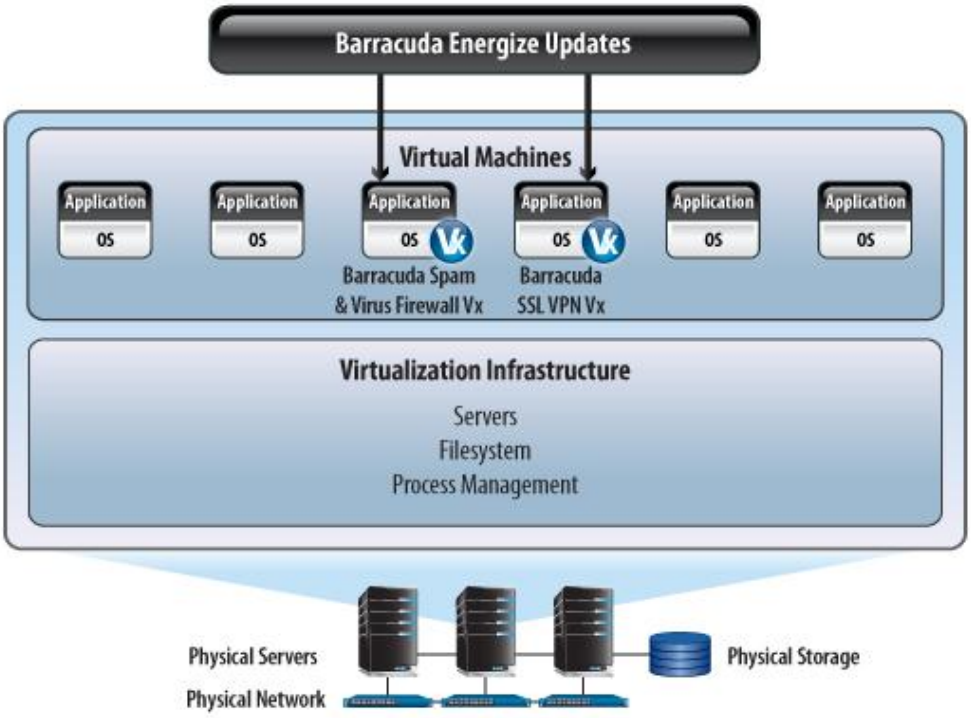
*Concurrent sessions here represent the number of bi-directional connections. Firebox e-Series products have previously published uni-directional concurrent sessions which we have converted here for comparison purposes. You can multiply this bi-directional number by 2 to calculate uni-directional data.

**Throughput rates will vary based on environment & configuration

Virtuel

Nous n'en parlerons pas ici mais sachez que la plupart des fabricants de pare-feu commencent à commercialiser le logiciel (firmware) contenu dans leur ***pare-feu matériel sous forme de machine virtuel*** pour les principales infrastructures virtualisées (ESXi, XENServer, PlateSpin, XEN, KVM, Hyper-v etc.).

De plus il est intéressant de considérer la virtualisation comme une nouvelle brique de sécurité à part entière avec ses avantages et ses inconvénients.



Le pare-feu dans votre réseau

Maintenant que vous avez pris connaissance des concepts de base concernant la sécurité informatique et ce qu'est un pare-feu nous allons voir comment envisagé son intégration dans votre réseau d'entreprise.
Tout d'abord nous allons présenter l'étude amont préalable au déploiement du pare-feu puis nous bâtirons une architecture sécurisée type.

Etude amont

Nul besoin de préciser que sécuriser un SI ne s'improvise pas sur un coin de table. Les techniques style « Extreme Programming » ne peuvent être envisagées en sécurité informatique.
En effet si vous installez votre pare-feu sur un coin de table de la salle informatique et le branchez de manière irréfléchie :

- dans le meilleur des cas vous bloquerez les accès de votre entreprise et provoquerez une belle pagaille sur le réseau,
- dans le pire des cas vous risquerez une compromission immédiate de votre SI.

Rappel : un poste sous Windows XP, sans pare-feu et directement connecté sur internet, a une durée de vie de l'ordre de la dizaine de minutes avant qu'un ver ou bot ne le compromette !)

Gardez bien à l'esprit qu'assainir un système d'information après un sinistre est une tâche ardue d'autant plus complexe que l'est votre SI.

Nous ne détaillerons pas l'étude à mener car cela relèverai de la conduite de projet orientée sécurité.
Cependant il y a des phases incontournables pour un tel projet.

Par conséquent prenez le temps:

- D'auditer l'existant (architecture réseau, système et flux applicatifs)
- Recueillir des besoins fonctionnels des différents corps de métiers impliqué dans la gestion du SI :
  - En général les architectes applicatifs, système et réseaux,
  - Sinon directement auprès des équipe réseau, système, de développement,
- Elaborer un inventaire aussi complet que possible des éléments du SI,
- Identifier tous les points d'entrée et de sortie à risque de votre SI (on passe du pare-feu en passant par la clef USB et le poste nomade bourré de Virus en retour de déplacement en clientèle !)
- Définir et chiffrer minutieusement la politique de sécurité que vous souhaitez mettre en œuvre, (la partie la plus longue)

  Note : Pour les impatients, dès cette étape vous pouvez avoir une idée très précise des règles qui seront codées dans votre pare-feu,

- Valider le modèle retenu avec vos clients et les équipes dirigeantes,
- Planifier votre déploiement,
- Et surtout communiquer sur vos futures interventions,
- Faire la recette, grâce à des tests de pénétrations (en mode black, grey, white box), votre pare-feu,
- Assurer la formation de l'équipe sécurité,
- Mettre en place l'exploitation et la surveillance de votre pare-feu.

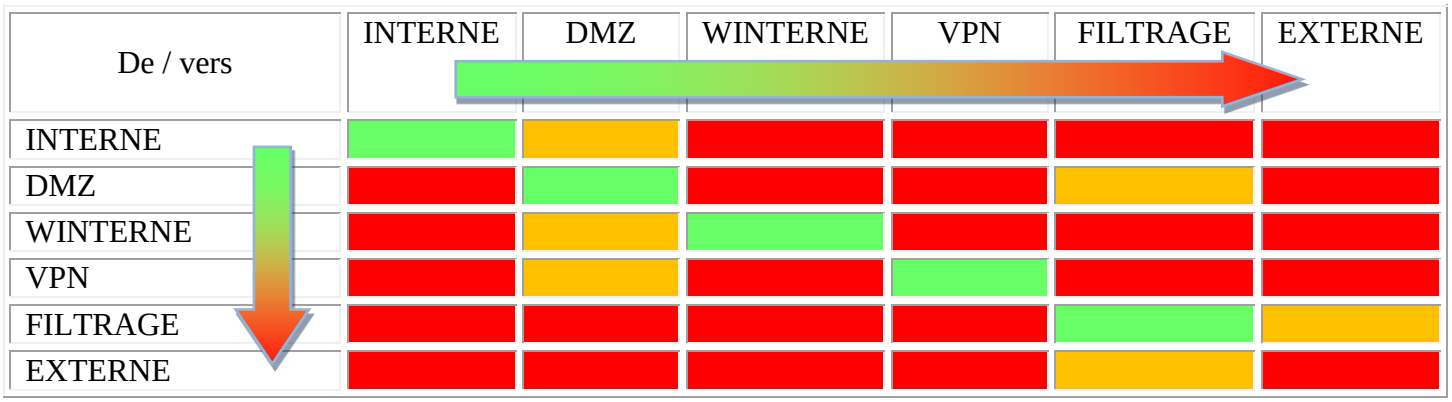
Après une étude amont menée par l'architecte sécurité, ce denier doit en générale vous remettre un ensemble de documents, concernant :

- Le comportement et le positionnement que doit avoir votre pare-feu au sein du réseau d'entreprise,
- La définition des zones de sécurité (en générale : LAN, WAN, DMZ …)
- La liste des utilisateurs avec leur niveau d'accréditations concernant les accès aux différentes zones,
- Les règles censées mettre en œuvre la politique de filtrage retenue (trafics autorisés en fonction des zones et utilisateurs),
- L'activation et le paramétrage des filtrages de flux (si disponible),
- L'activation et le paramétrage des modules IDS, AV etc. (si disponible),
- Le routage basique (cas le plus fréquent si l'architecture a été correctement pensée) ou avancé, le NAT (assez fréquent sur des pare-feu frontaux), bien évidemment un plan d'adressage IP,
- Intégration du type d'authentification en usage sur le site,
- Le niveau de disponibilité de votre pare-feu (cluster, répartition de charge, haut dispo. etc.),
- Le choix de la machine d'administration de votre pare-feu (machine sûre à accès exclusivement dédié à cette tâche),
- Mise en place d'un serveur de journaux (type syslog),

Exemple de diagramme des flux généraux (il faut ensuite détailler et affiner la politique de filtrage) :

Veuillez observer le classement des entêtes de « colonne/rangée », **du plus sécurisé au moins sécurisé** :

En cas de doute verrouiller l'accès, les journaux du pare-feu vous donnerons la raison d'un blocage suite à l'établissement de règles un peu trop restrictives.



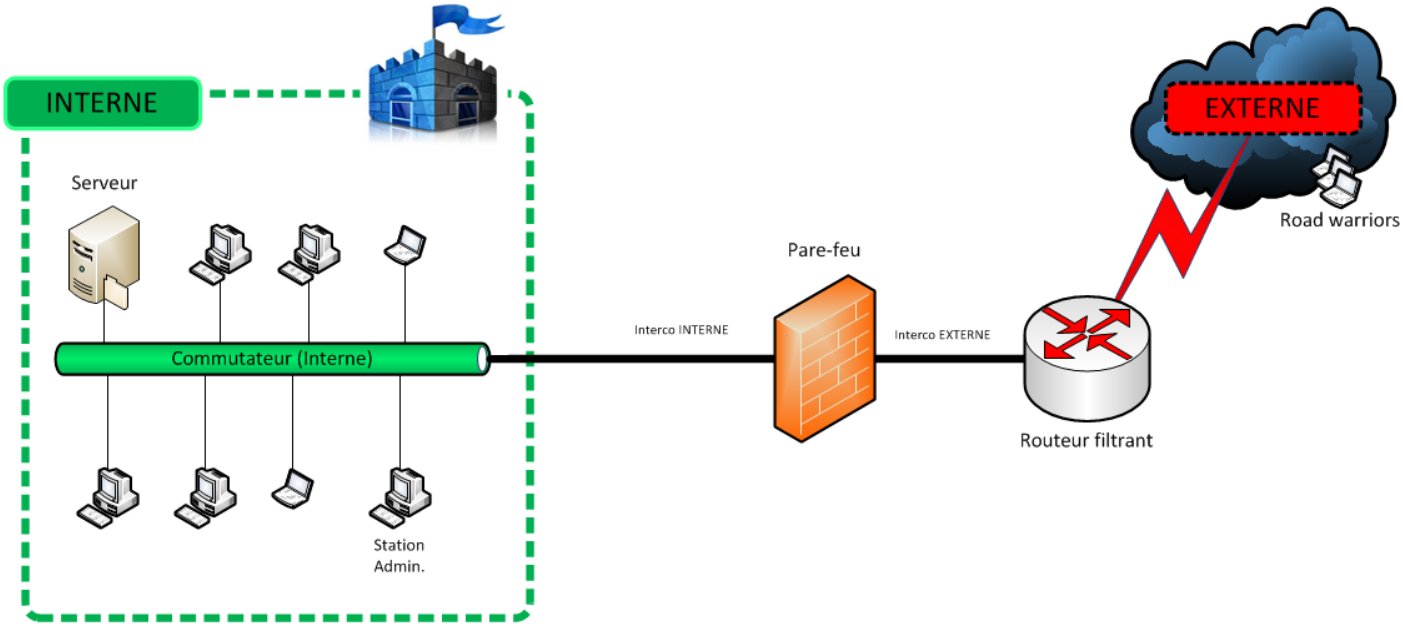
	Accès autorisé
	Accès autorisé sous certaines conditions très strictes
	Accès interdit

Important : Ne négligez pas le choix du placement au sein du réseau de votre pare-feu sinon au fil du temps il va vite devenir une passoire et deviendra ingérable.

Architectures usuelles

Maintenant nous allons tenter de passer en revue les architectures réseau sécurisées les plus courantes. Elles sont éprouvées et sont largement utilisées par de grands comptes.

En coupure simple



Cette architecture est la plus courante dans les TPE et PME : routeur filtrant, pare-feu, réseau commuté, En effet en présence de moyens limités en ressource humaine ou financière il s'agit d'une bonne option. Il faut bien garder à l'esprit que le stricte respect des fondamentaux en terme de sécurité induit un coût non négligeable.

Cependant si l'on se pose la question de ce qu'il y a sécurisé on peut supposer que le fait de n'avoir qu'un seul serveur ne justifie pas d'engager des moyens pharaoniques. Surtout si l'entreprise ne dispose pas de personnels qualifiés et aguerris aux métiers de la sécurité informatique pour gérer une solution beaucoup plus complexe.
Le risque dans ce cas peut avoir été évalué et jugé non critique, bien entendu cela est toujours à mettre en rapport avec le budget alloué à la sécurité informatique.

Si l'on choisit un pare-feu en coupure simple, généralement un UTM d'entrée de gamme, cela permet de proposer un bon niveau de sécurité tout en étant simple à mettre en œuvre et à maintenir pour des coûts inférieurs au demi-millier d'euros (or licences des anti-spam, anti-virus, blocage URL etc.)

\+ + + **Avantages** :

- Coût,
- Facilité de maintenance et d'administration,
- Diagnostic des pannes aisé.

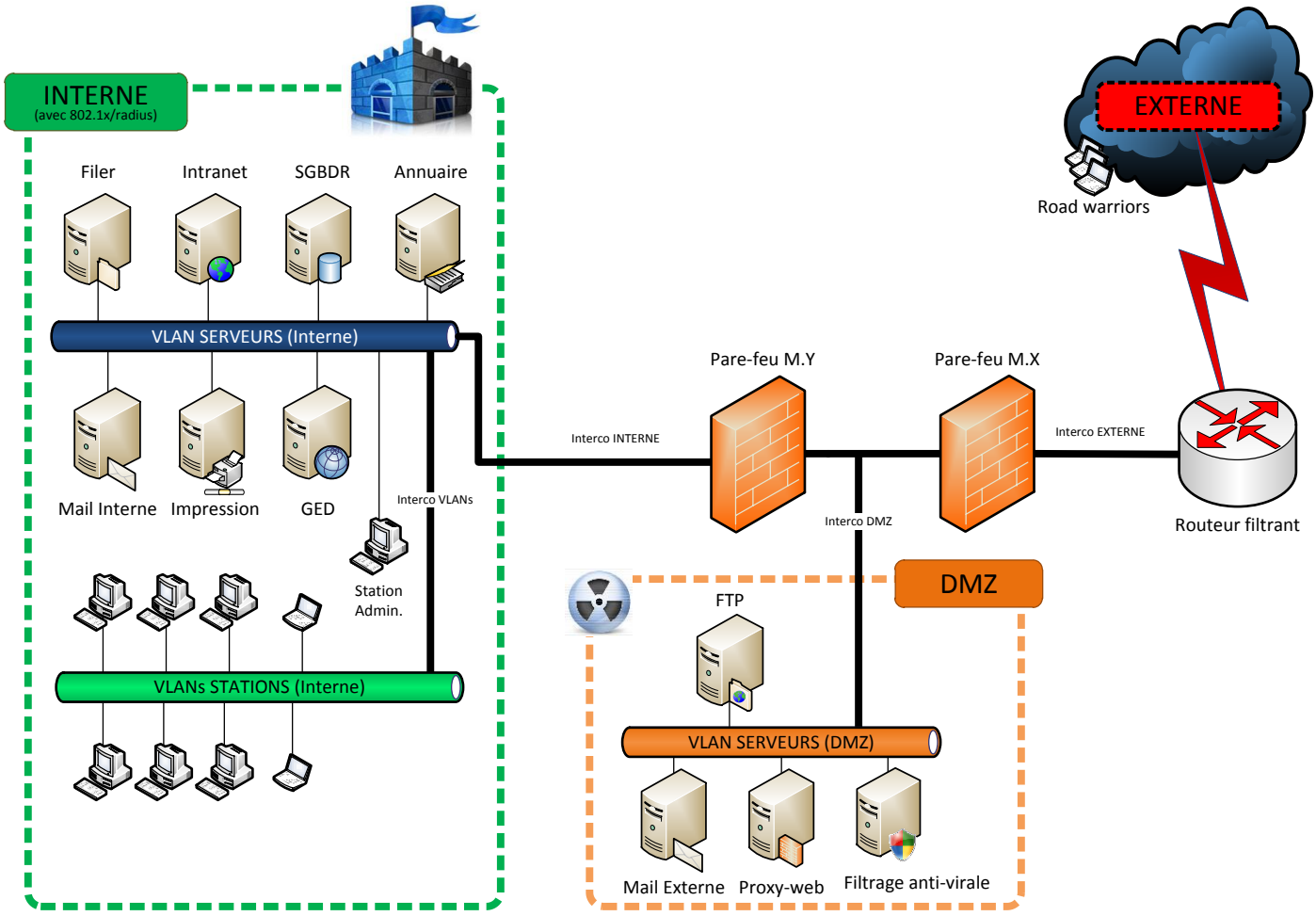
\- - - **Inconvénients** :

- Tolérance aux pannes,
- Non respects de certains fondamentaux en termes de sécurité (unicité des fonctions, zones de sécurité, mix des technologies, mises à jour délicate car 1 serveur/1 pare-feu si souci …),
- Niveau de sécurité faible.

Multizones

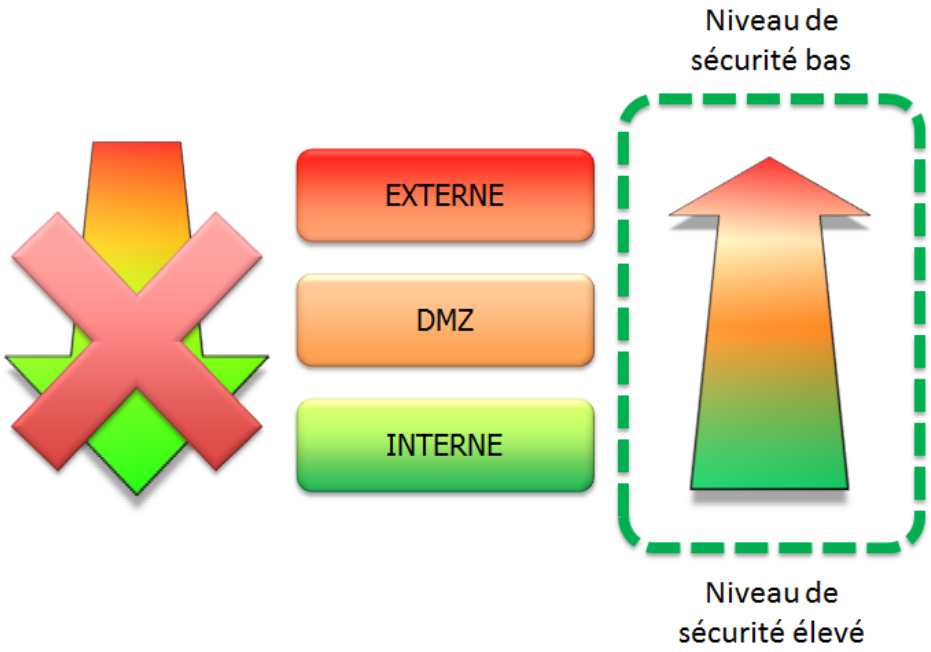
Dos à dos (double coupure)

Cas 1 :



Là nous commençons à disposer d'une solution qui propose un niveau de sécurité intéressant.
En effet :

- Des zones de sécurités sont clairement définies,
- La compromission d'un des 2 pare-feu préserve l'intégrité de la zone interne à sécuriser,
- La notion de mix des technologies est prise en compte au niveau des pare-feu,
- La zone à risque (DMZ) dispose de fusibles concernant les menaces externes (filtrage AV, proxy, relais mail),
- Les briques du SI respectent plus ou moins l'unicité des fonctions,
- Les zones ayant un niveau de sécurité bas n'ont pas accès à celles d'un niveau plus élevé,



- Les réseaux commutés sont sécurisés via VLAN et 802.1X,

Quelques mots concernant le 802.1X. Il s'agit d'une technologie qui opère au niveau 2 (commutation) et autorise ou interdit l'accès au média de transport en fonction de l'hôte qui tente de se raccorder au réseau. A ce stade on ne parle pas encore de système mais bien d'autorisation d'accès pour l'interface de connexion au réseau (carte réseau etc.). Il s'agit d'une sécurité réseau qui utilise également les serveurs RADIUS.

\+ + + **Avantages** :

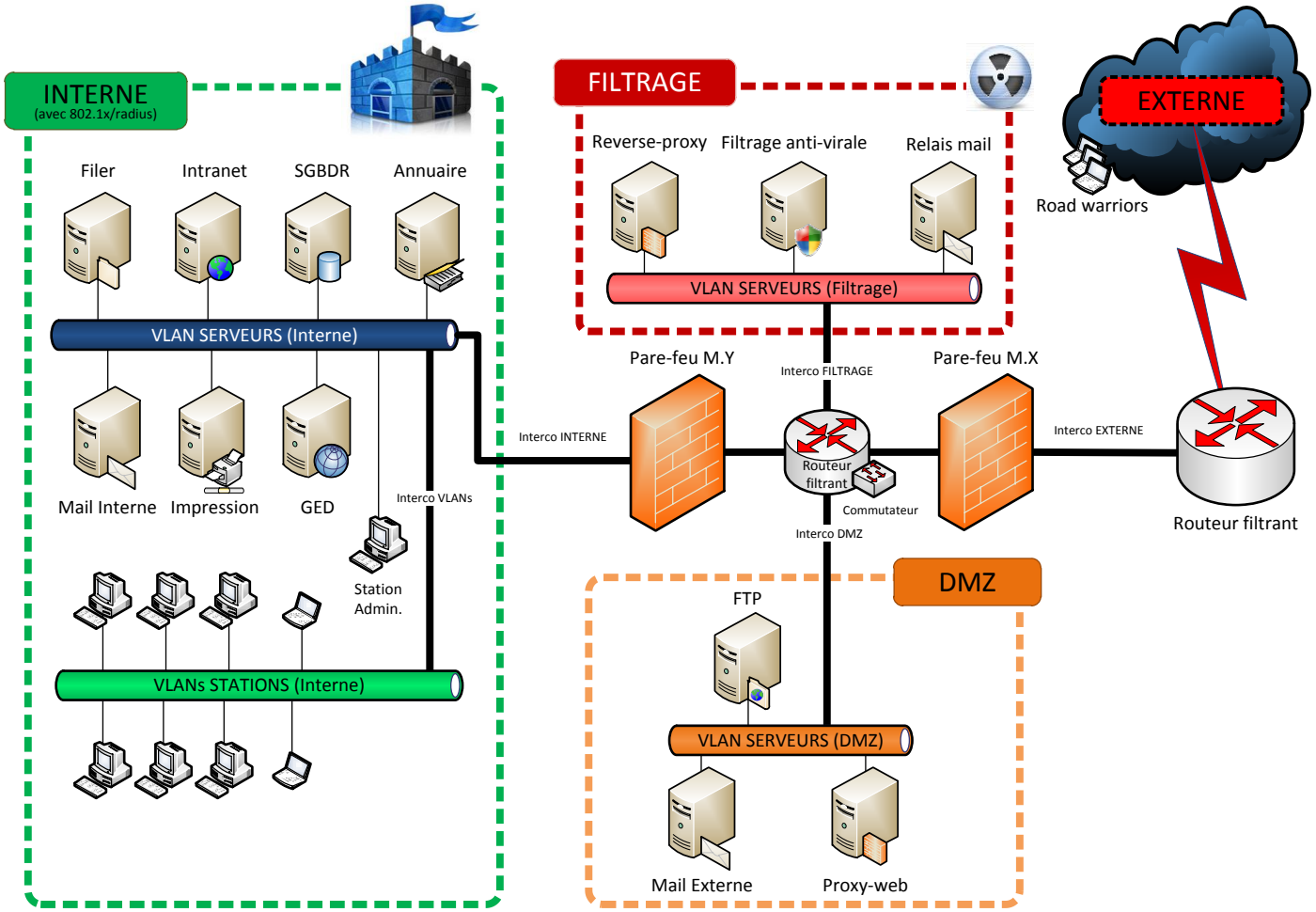
- Tolérances aux pannes prise en compte,
- Respects des principaux fondamentaux en termes de sécurité (unicité des fonctions, zones de sécurité, mix des technologies, facilité de mise à jour),
- Niveau de sécurité intéressant,
- Protection du réseau interne (accès non autorisé 802.1X, VLAN)

\- - - **Inconvénients** :

- Diagnostic des pannes,
- Présence d'un administrateur système/sécurité,
- Facilité de maintenance et d'administration,
- Coût.

Cas 2 :

Zone de périmètre : il s'agit d'une sorte de DMZ couplée à une zone de filtrage, les deux étant cloisonnée par un routeur filtrant.



Ce schéma d'architecture de pare-feu dos-à-dos constitue un bon cas d'école dans le sens où il **regroupe la plupart des « Best practices »** vu précédemment (cf. « Concepts de base ») et introduit également la notion de **zone de décontamination**, nommée pour plus de clarté **« FILTRAGE »**.

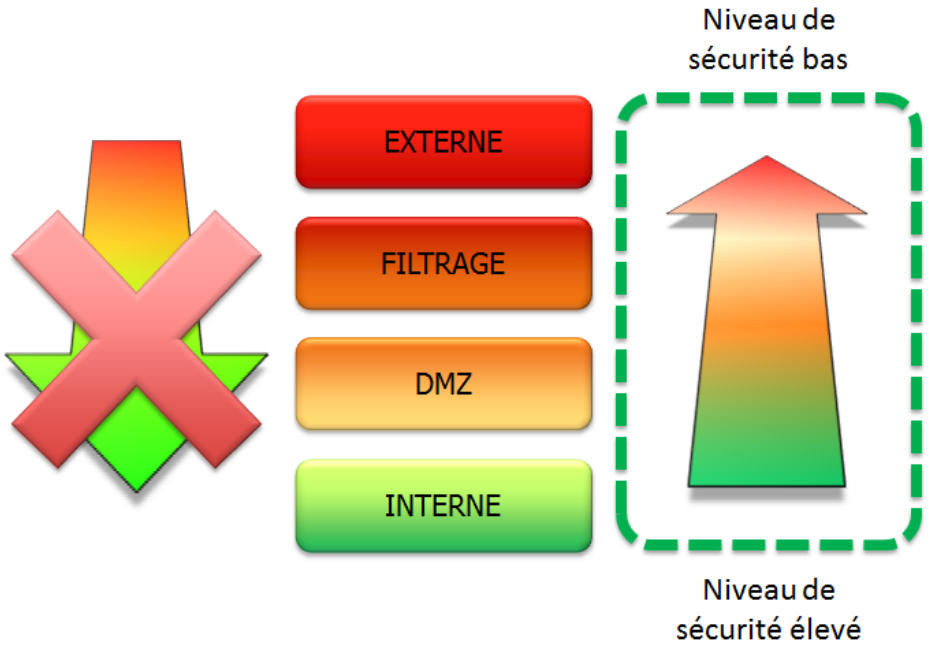
Cette architecture présente tous les avantages vu précédemment et ajoute une zone de sécurité supplémentaire. Il va sans dire que nous complexifions en conséquence l'administration de notre SI.
Vos règles de filtrage seront autrement plus lourdes à mettre en place et à gérer. Parfois la sécurité sera à ce prix.

Note : Veuillez remarquer que dans tous **ces schémas d'architecture nous ne parlons jamais de sonde d'analyse de menaces (NIDS, HIDS) pourtant essentielles** dès que l'on commence à envisager de telles solutions d'entreprise.

Sur ce schéma vous constatez que la zone la plus exposée, donc ayant un niveau de sécurité que nous aurons choisi de considéré comme basse (l'extérieur étant la plus basse), est la zone de « FILTRAGE ».

A propos des anti-virus en présences :
L'architecte sécurité aura pris soin de choisir des antivirus différents par zone de sécurité mise en place.
En ce sens il respectera le mix des technologies : si un produit laisse passer une menaces de type virale, vers, troyen etc. le second aura peut-être une chance de l'intercepter. Cela semble anodin mais pourtant terriblement efficace.

En fait si l'on veut énumérer les flux possibles on veillera à respecter autant que possible la règle des niveaux de sécurité (élevé vers bas OK) ci-dessous :



Plaçons-nous dans le cas concret du traitement d'un flux de courriel (SMTP).

Le serveur **de « Mail externe »** (placé en DMZ) n'initiera **jamais de connexion avec la zone interne** pour l'acheminement du courrier par exemple.
Ce sera le serveur de **« Mail interne » qui initiera la connexion avec le serveur de « Mail externe »** lequel obtiendra les courriels qu'il aura été **récupérer sur le « relais mail »** placé en zone de « FILTRAGE ».

Voici la politique précise concernant un flux de courriel type SMTP :

De / vers	INTERNE	DMZ			FILTRAGE			EXTERNE		
		SRC	DST	Proto.	SRC	DST	Proto.	SRC	DST	Proto.
INTERNE		Mail Interne	Mail Externe	SMTP 25						
DMZ					Mail Externe	Filtrage anti-virale	SMTP 25			
FILTRAGE								Filtrage anti-virale	ANY*	SMTP 25
EXTERNE					ANY*	Filtrage anti-virale	SMTP 25			

	Accès autorisé
	Accès autorisé sous certaines conditions très strictes
	Accès interdit

ANY* : vous pouvez établir des « Blacklist » de serveur SMTP et vérifier via les zones indirecte DNS les champs MX de vos potentiels « partenaires SMTP» etc.

Note : volontairement nous n'insérerons pas la notion d'authentification utilisateur pour simplifier le tableau ci-dessus. De plus il est acté que le « Filtrage anti-virale » et le « Relais mail » doivent travailler ensemble.
Souvent le « Relais mail » de la zone de « FILTRAGE » n'est rien d'autre que le module d'analyse anti-virale SMTP (SMTP Proxy) du pare-feu UTM.

Astuce : pour rendre la tâche plus gênante pour les attaquants n'hésitez pas à changer les numéros des ports standards que vous utilisez : un serveur SMTP qui écoute sur le port 61525 est beaucoup moins sujet à un « script Kiddie » qu'un autre écoutant sur le port 25.
Et surtout rendez vos serveurs (services système) le moins bavard possible … (« no information leak »).

\+ + + **Avantages** :

- Tolérances aux pannes prise en compte,
- Respects des principaux fondamentaux en termes de sécurité (unicité des fonctions, zones de sécurité, mix des technologies, facilité de mise à jour),
- Niveau de sécurité évolué,
- Isolation des menaces par zones très poussée,
- Protection du réseau interne (accès non autorisé 802.1X, VLAN)

\- - - **Inconvénients** :

- Mise en œuvre,
- Politique de sécurité clairement établie (règles, plan de reprise) incontournable,
- Diagnostic des pannes complexe,
- Présence d'une équipe chargée de la sécurité informatique,
- Facilité de maintenance et d'administration,
- Coût important.

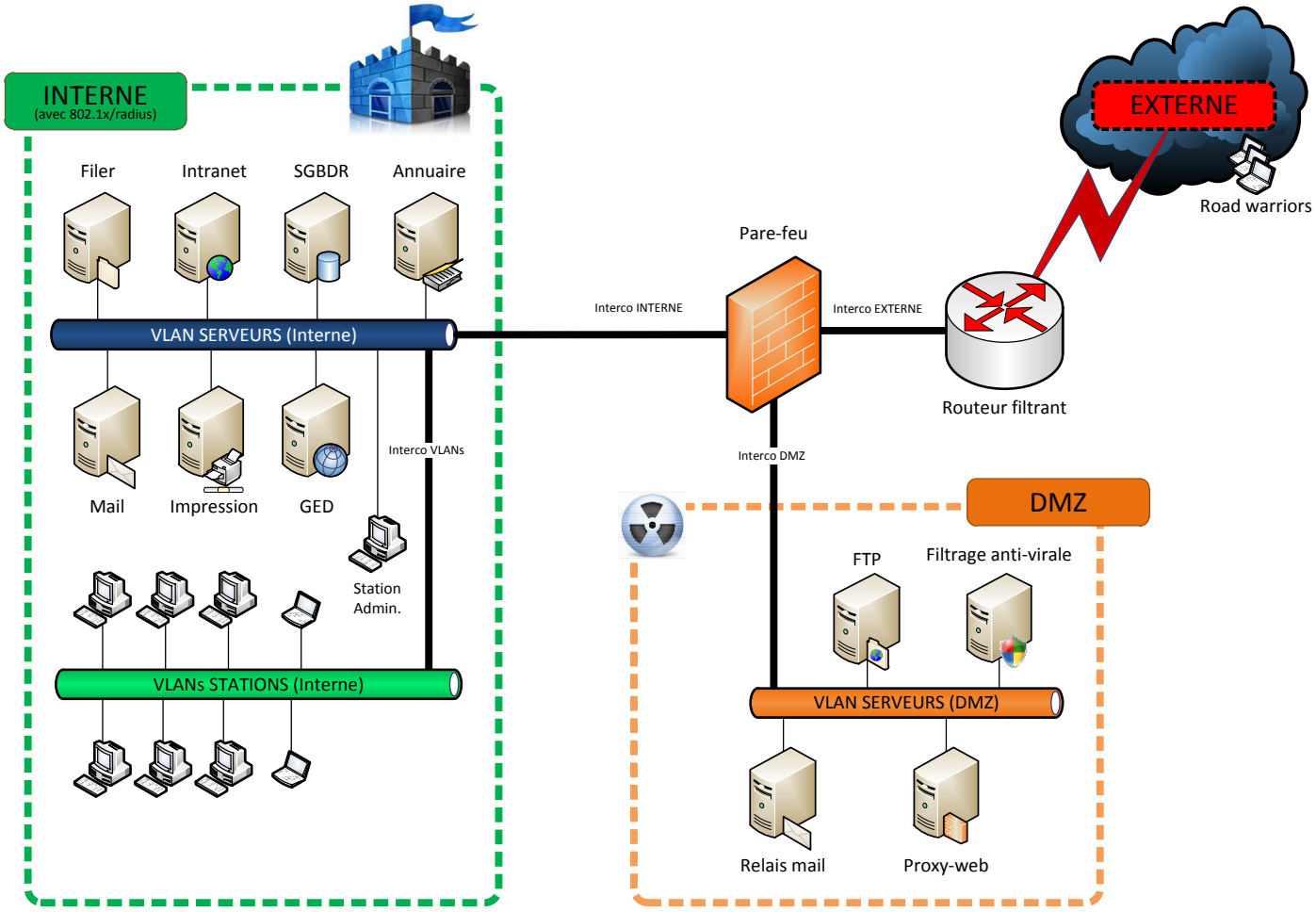
Quelques mots sur le « Reverse-proxy » et le « Proxy-cache »

Un « Reverse-proxy » est un mode de fonctionnement particulier d'un Proxy-cache. On utilise alors ce dernier à l'envers. Un « Reverse-proxy » se place en frontal d'un site Web hébergé en DMZ.
Il permet de traiter les requêtes (http par exemple) en envoyant au serveur Web uniquement les requêtes qui ne serait pas déjà dans son cache. Par conséquent il ne sollicite le serveur Web de DMZ que s'il ne dispose pas de la page demandée par le visiteur du site.
Il peut également faire de la répartition de charge sur une ferme de serveurs Web.
Mais surtout il permet de ne pas exposer le site lui-même (code, image, base etc.) à un visiteur un peu trop curieux ou/et malfaisant

Le « Proxy-cache » (Squid, ForeFront etc.) est le mandataire des clients du réseau INTERNE, il permet de :

- Contrôler les accès au Web (Blacklist etc.),
- Economiser la bande passante de la connexion EXTERNE via la mise en cache des sites Web déjà visités,
- Rendre la navigation Web nominative (Juridiction) et journalisée,
- Masquer le réseau INTERNE, donc hôtes, éléments actifs etc., du réseau EXTERNE,

Tri-résidents



Ici nous revenons dans une architecture classique largement déployée qui va assurer les **mêmes fonctionnalités que le pare-feu dos-à-dos du « Cas n°1 » étudié précédemment** avec quelques différences majeures :

- Un coût d'achat divisé par deux (pour la partie matériel),
- Une mise en œuvre simplifiée,
- En revanche une tolérance de panne inexistante ainsi qu'une compromission global du SI si le pare-feu venait à être compromis.

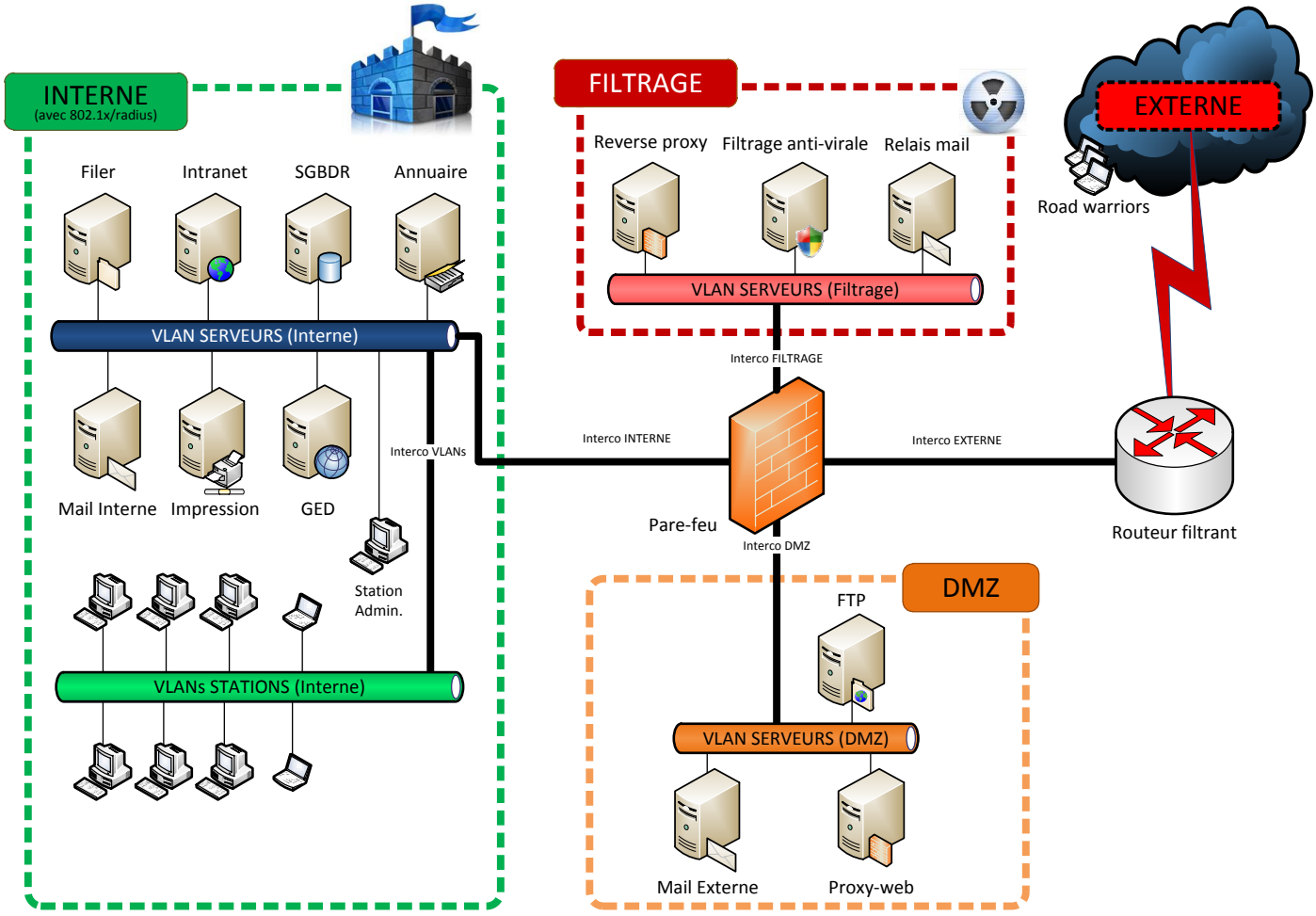
\+ + + **Avantages** :

- Coût équilibré/niveau de sécurité proposé,
- Respects des principaux fondamentaux en termes de sécurité (unicité des fonctions, zones de sécurité, mix des technologies, facilité de mise à jour),
- Niveau de sécurité intéressant,
- Protection du réseau interne (accès non autorisé 802.1X, VLAN).

\- - - **Inconvénients** :

- Tolérances aux pannes,
- Diagnostic des pannes,
- Présence d'un administrateur système/sécurité,
- Facilité de maintenance et d'administration.

Quadri-résidents



Comme avec l'architecture précédente nous revenons sur une architecture classique qui va assurer les **mêmes fonctionnalités que le pare-feu dos-à-dos du « Cas n°2 » étudié précédemment** avec quelques différences majeures :

- Un coût d'achat divisé par deux (pour la partie matériel),
- Une mise en œuvre simplifiée,
- En revanche une tolérance de panne inexistante ainsi qu'une compromission global du SI si le pare-feu venait à être compromis.

\+ + + **Avantages** :

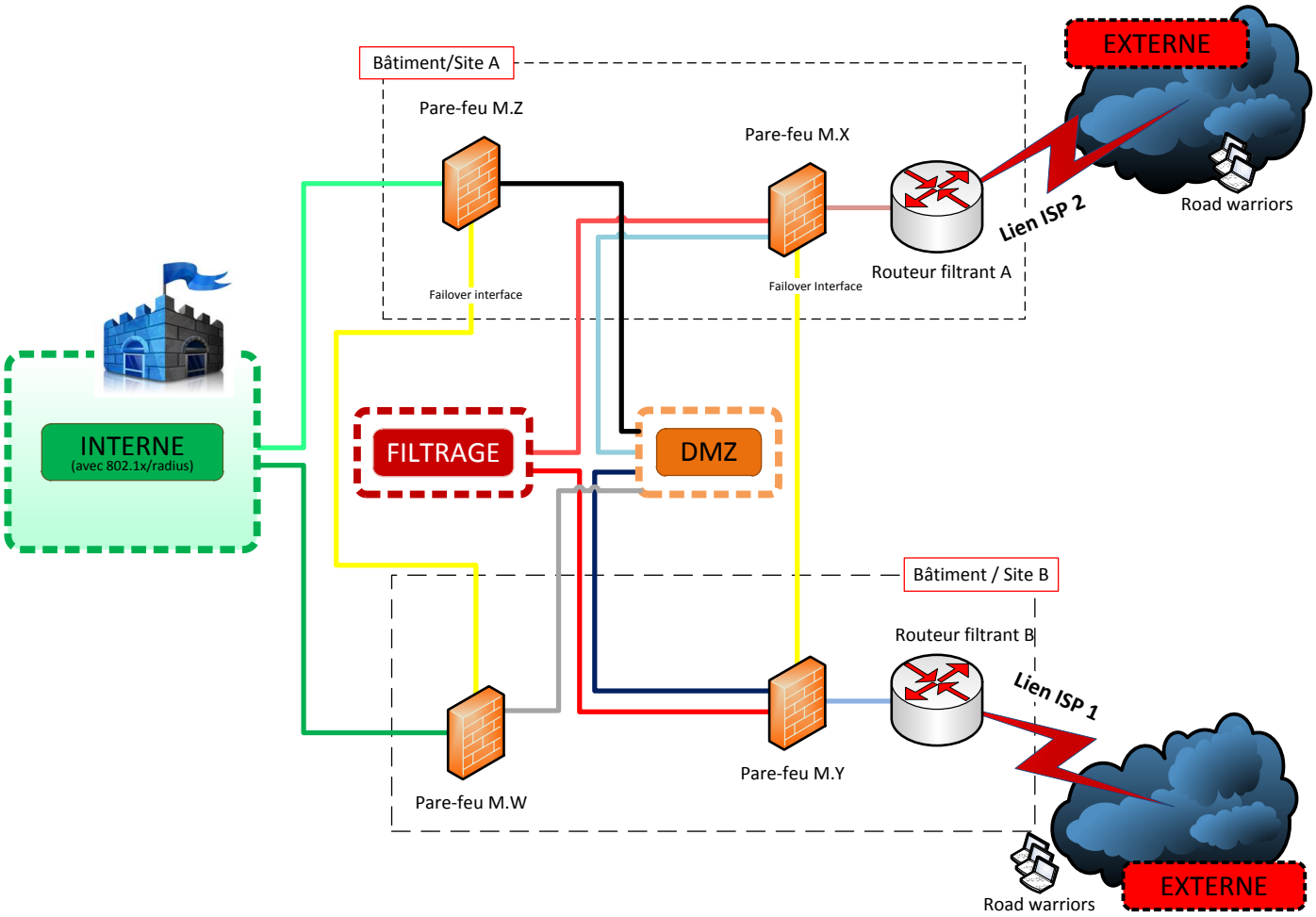
- Coût équilibré/niveau de sécurité proposé,
- Respects des principaux fondamentaux en termes de sécurité (unicité des fonctions, zones de sécurité, mix des technologies, facilité de mise à jour),
- *Niveau de sécurité évolué,*
- *Mise en œuvre,*
- *Isolation des menaces par zones très poussée,*
- Protection du réseau interne (accès non autorisé 802.1X, VLAN).

\- - - **Inconvénients** :

- Tolérances aux pannes,

- *Politique de sécurité clairement établie (règles, plan de reprise) incontournable,*
- *Diagnostic des pannes complexe,*
- *Présence d'une équipe chargée de la sécurité informatique,*
- Facilité de maintenance et d'administration.

Haute disponibilité



Ce genre d'architecture est quasi inexistant en TPE ou PME, seuls les grands comptes exigeants un taux de disponibilité proche des 100% peuvent se permettre d'acquérir de telles solutions.

Dans ce cas de figure le DSI a clairement mis dans la balance le coût d'une indisponibilité du SI, ne serait-ce qu'une journée ouvrée, face au budget alloué pour entrer dans le club fermé de la haut disponibilité.
Le ticket d'entrée est somme toute assez couteux.

Même si certains parviendront à mettre en œuvre ce genre de solution via des briques OpenSource, la maintenance et le suivi opérationnel d'une telle solution nécessitera une équipe conséquente complétement aguerrie aux concepts de la sécurité informatique. Le coût sera de toute façon en rapport avec l'architecture déployée.

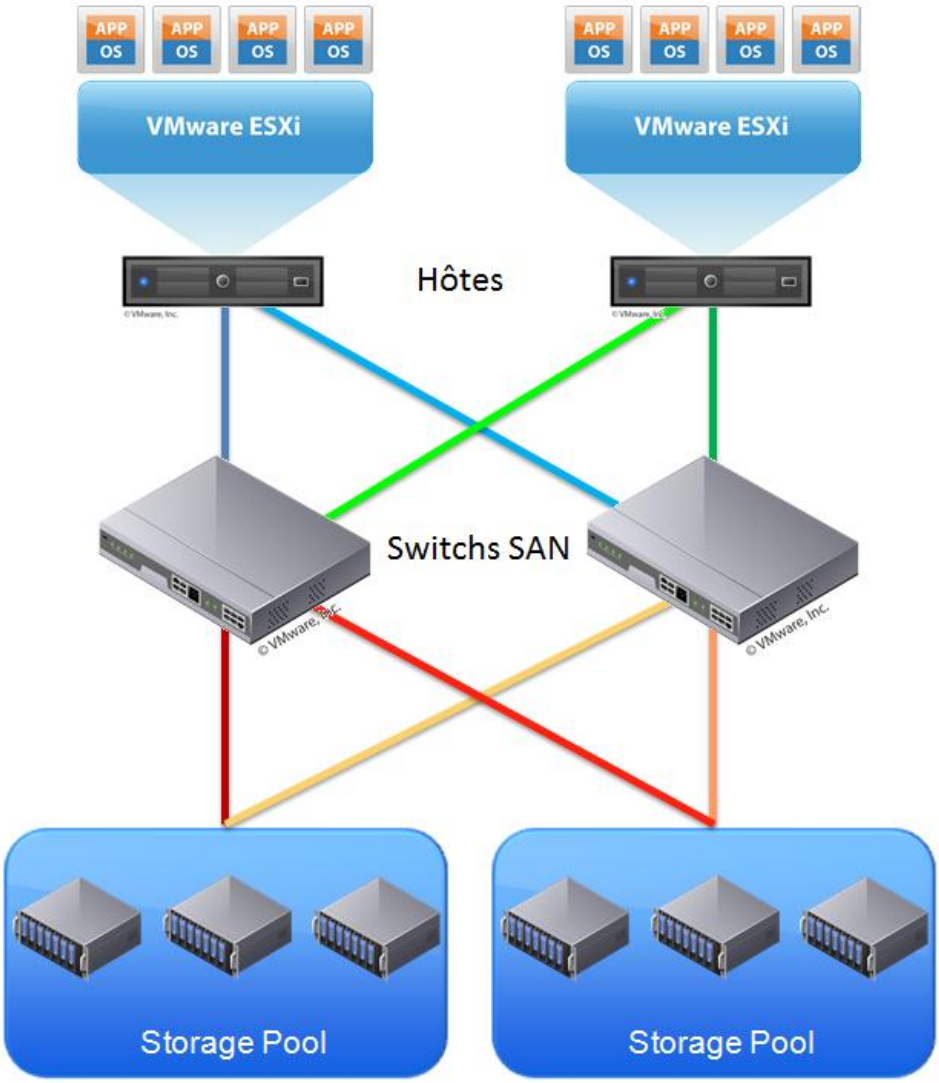
\+ + + **Avantages** :

- Haute disponibilité,
- Tolérances aux pannes prise en compte,
- Facilité de maintenance et d'administration.
- Respects des fondamentaux en termes de sécurité (unicité des fonctions, zones de sécurité, mix des technologies, facilité de mise à jour),
- Niveau de sécurité élevé,
- Isolation des menaces par zones très poussée,
- Protection du réseau interne (accès non autorisé 802.1X, VLAN).

- - - **Inconvénients** :

- Coût direct et indirect,
- Mise en œuvre,
- Politique de sécurité clairement établie (règles, plan de reprise) incontournable,
- Diagnostic des pannes complexe,
- Reprise après sinistre délicate,
- Présence d'une équipe spécialisée qui sera chargée de la sécurité informatique.

Note : En générale la haute disponibilité s'obtient par un maillage en croix des briques systèmes (ce genre de schéma peut également s'appliquer sur des Switchs réseau) :



Les « road warriors »

De nos jours, difficile de ne pas parler des accès possibles depuis l'extérieur vers le SI de l'entreprise. Dans certaines institutions cela n'est pas encore une réalité mais cela risque rapidement de le devenir, rationalisation oblige.

Mais qu'est-ce qu'un « **road warriors** » ?
Ce sont les pc nomades, les Smartphones … en fait toutes les machines accédant via WIFI ou VPN au réseau d'entreprise depuis l'extérieur de cette dernière.

Astuce : Les calculettes d'accès VPN doivent être de mise quand vous envisagez d'ouvrir votre SI aux télétravailleurs.

N'oubliez jamais qu'un portable (ou Smartphone etc.) de votre entreprise qui se connecte depuis un hôtel, un hot-spot, devient vite la brique du SI dont le niveau sécurité à l'instant t sera potentiellement le plus bas.
La compromission d'un ordinateur portable peut devenir catastrophique pour le SI de l'entreprise, envisagez dès la conception les possibles menaces et plan de reprise après sinistre pour ce type d'utilisateurs nomades.

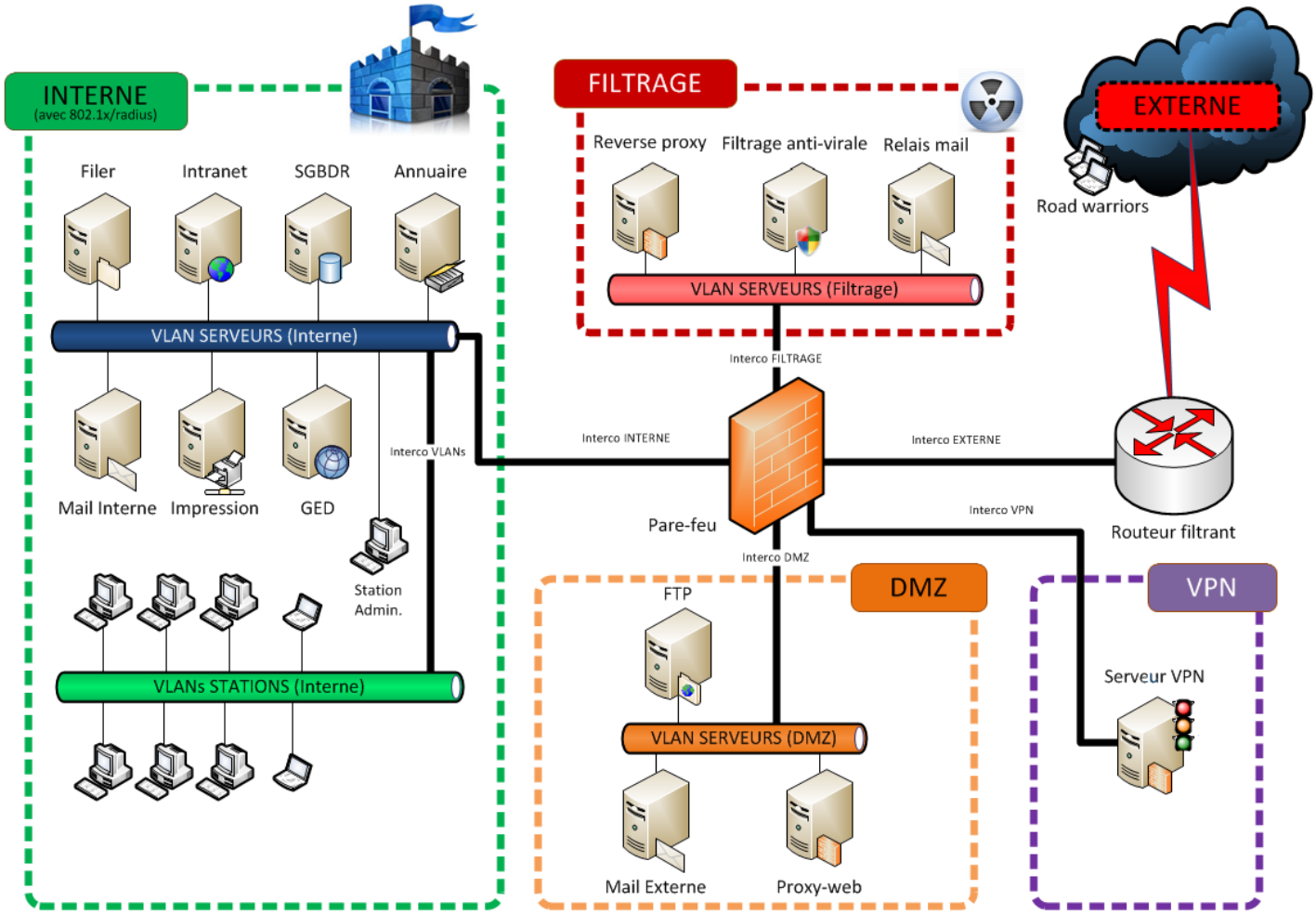
Ne perdez pas de vue qu'avec les débits (même Edge ou 3G) actuels un ver pourra corrompre un SI en quelques dizaines de minutes si vous avez mal envisagé l'aspect sécuritaire inhérent à la mise en œuvre d'un VPN. Les dégâts pourraient s'avérer catastrophiques pour la productivité de l'entreprise.

Attention un VPN est à double tranchant, il peut être uni ou bi directionnel et dans chaque cas vous devrez gérer cette zone de sécurité comme une autre, à savoir :

- Estimation des risques,
- Règles de pare-feu,
- Plan d'adressage,
- Filtrage des flux réseau comme applicatifs,
- Anti-virus,
- Etc.

Donc niveau architecture il va falloir remettre le couvert une nouvelle fois et envisager la création d'un autre zone de sécurité dite « Zone VPN » qui va s'intégrer dans votre politique de sécurité.

La zone des accès distants : « zone VPN »

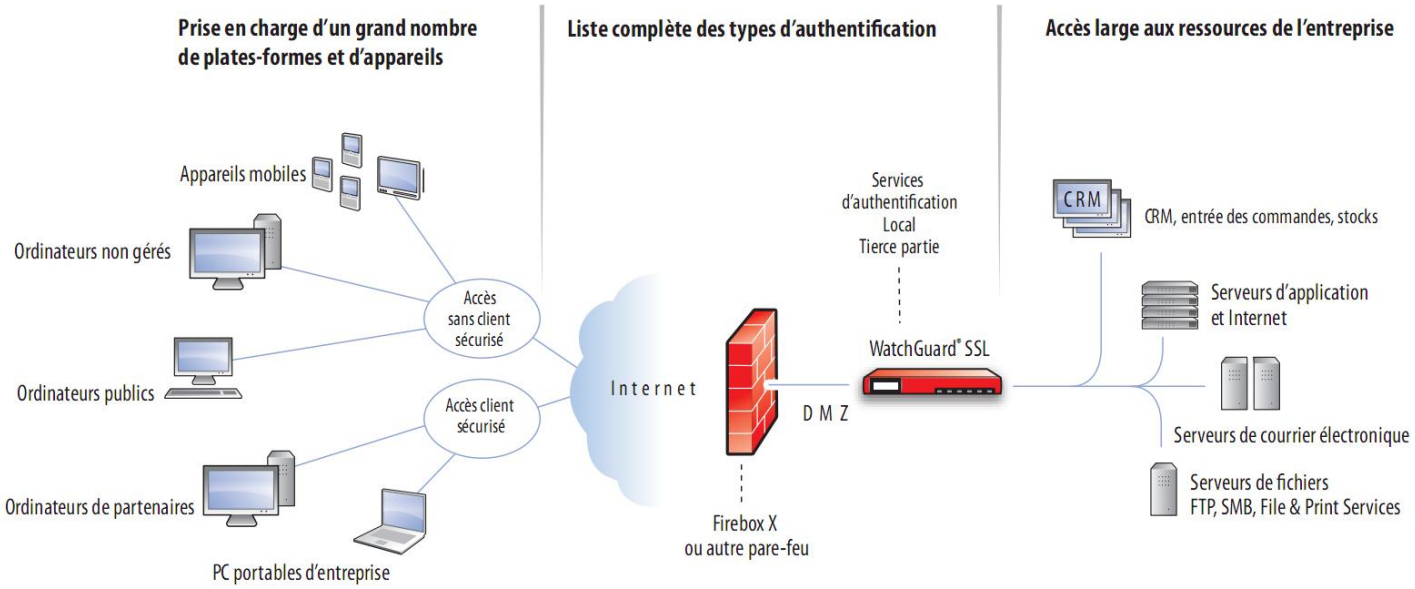


ATTENTION : Prenez soin de prendre un bon client VPN, ce dernier doit au minimum couper toutes les autres accès réseau.
En effet si vous êtes connecté à Internet via votre FAI vous disposez déjà d'un accès via une interface réseau si votre client VPN monte une seconde interface réseau (virtuelle cette fois) mais ne bloque pas l'accès direct à votre réseau local (routage etc.) votre ordinateur devient une passerelle entre Internet et votre entreprise sans la moindre protection …

Vous aurez compris que la mise en place d'un accès VPN, donc d'une zone de sécurité supplémentaire, pour les télétravailleurs rajoute une nouvelle zone à risque pour votre SI qu'il faudra surveiller et gérer de prés.

Ceci n'étant pas un cours sur les VPN je vous invite à largement vous documenter avant de vous lancer dans la mise en œuvre d'un VPN.

Prenez note que des « Appliance » sont vendus uniquement dans ce but comme ci-dessous :



~~La nouvelle approche : les zones dynamiques~~

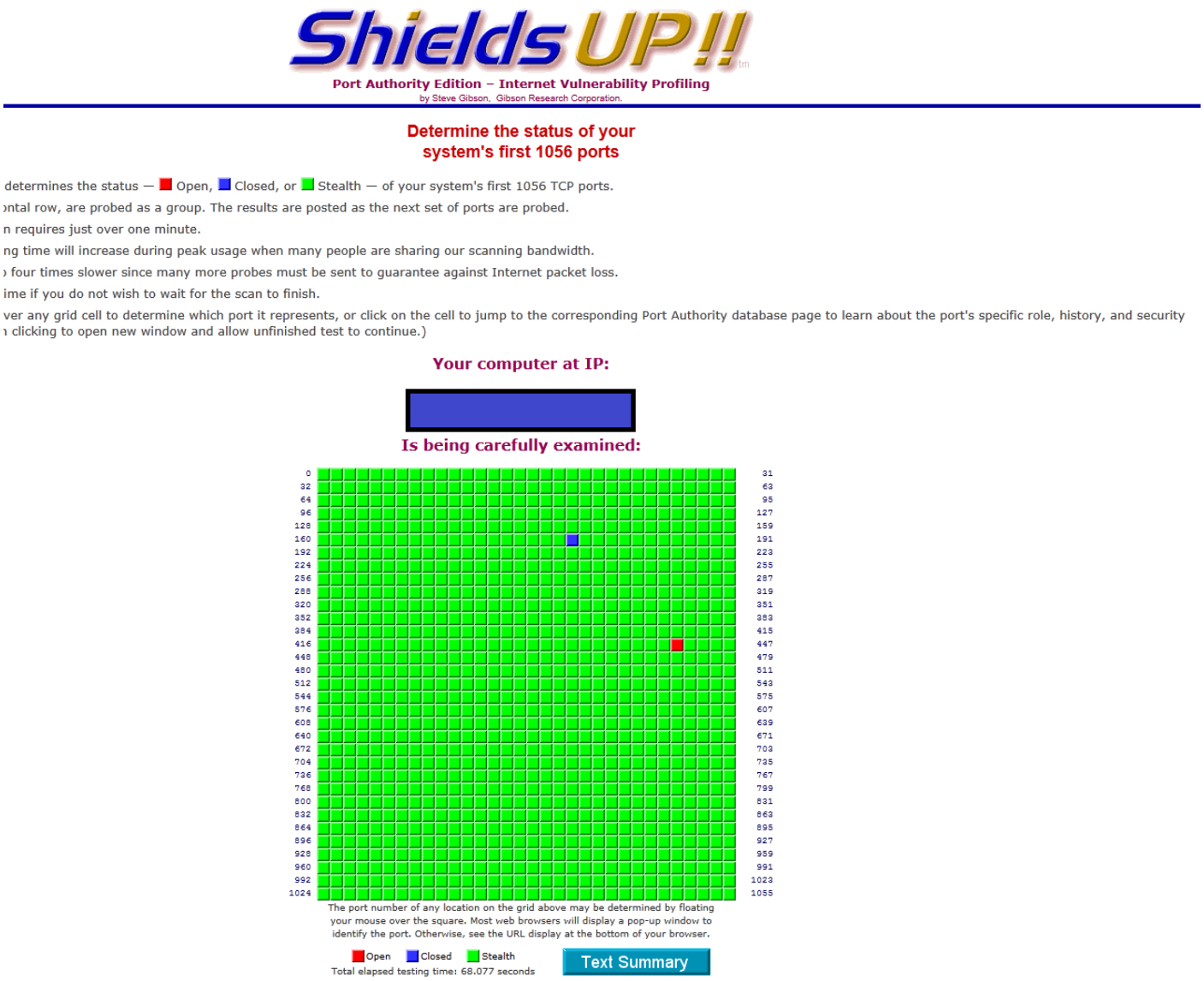
~~Il ne faut pas hésiter à user des technologies type NAP (Microsoft), NAC (CISCO) et avoir recours à la virtualisation (ESX, XEN, PLATESPIN…) etc.~~

Vérification installation

Une fois un pare-feu installé il faut impérativement lui faire subir une série de tests de pénétrations (PenTest) etc. et analyser méthodiquement au quotidien les journaux qu'il produit.

Dans un premier temps vous pouvez utiliser un test « Online » tel que celui proposé par « Gibson Research » : « Shield up !! » :

https://www.grc.com/x/ne.dll?bh0bkyd2



Sur le schéma ci-dessus on peut voir que seul le port 443 (HTTPS/SSL) est ouvert. Les autres ports sont dits « STEALTH » c'est-à-dire invisibles, dans les faits les paquets non autorisés sont détruits (DROP) sans prévenir l'émetteur de ces derniers.
On voit également que le port BGP (Bordure Gate Protocol) est ici interdit (REJECT) et l'on prévient l'émetteur du paquet que nous n'acceptons pas ce genre de paquet.

On peut bien évidement faire un scan complet avec des outils tel Nmap etc. Attention toutefois sur pare-feu professionnel un scan basique va très rapidement être détecté et bloquera votre ordinateur de test … (alors on évitera de faire les test de pénétration à partir de la console d'administration du pare-feu … ;-))

Et bien sûr il faudra passer en revue les attaques vues au chapitre « Les menaces ». Un bon ensemble d'outils de « Pentesting » est la distribution « BackTrack » : elle propose la plupart des outils dont nous avons discuté jusqu'ici.

Un audit extérieur n'est pas un luxe pour tester la robustesse de la solution une fois mise en place.

Choix et déploiement d'un pare-feu

Vous avez réussi à définir :

- Le comportement et le positionnement que doit avoir votre pare-feu au sein du réseau d'entreprise,
- La définition des zones de sécurité (en générale : LAN, WAN, DMZ …)
- La liste des utilisateurs et hôtes avec leur niveau d'accréditations concernant les accès aux différentes zones,
- Les règles censées mettre en œuvre la politique de filtrage retenue (trafics autorisés en fonction des zones et utilisateurs),
- Le filtrage des flux au sein de votre entreprise,
- Votre besoin en terme de module IDS, AV etc.,
- Le routage basique (cas le plus fréquent si l'architecture a été correctement pensée) ou avancé, le NAT (assez fréquent sur des pare-feu frontaux), bien évidemment un plan d'adressage IP,
- Intégration du type d'authentification en usage sur le site,
- Le niveau de disponibilité de votre pare-feu (cluster, répartition de charge, haut dispo. etc.),
- Le choix de la machine d'administration de votre pare-feu (machine sûre à accès exclusivement dédié à cette tâche),
- Quel serait votre système de journalisation,

Maintenant vous allez devoir choisir votre pare-feu parmi ceux énumérés au chapitre précédent.

Voici une check-list pour vous aider à faire ce choix.

L'heure du choix

Dimensionnement

Critères	Considérations	Petites organisation	Moy. et grandes organisations
Nombre d'adresse IP à protéger	**Licences?** (Oui ou Non) * Limité ou illimité nombre d'appareils agréés * Tous les produits ont des performances limites	Evolutif? Envisagez vos besoins de croissance.	Evolutif? Envisagez vos besoins de croissance.
Nombre de connexions simultanées	Varie # par modèle Firewall	Evolutif? Envisagez vos besoins de croissance.	Evolutif? Envisagez vos besoins de croissance.
Performance (débit , VPN , UTM / filtrage)	* Vérifiez les spécificités du pare-feu pour chaque fonction * Est-ce que le débit comprend TOUT le trafic à travers tous les ports * Envisagez le nombre : • d'utilisateurs, • de type de média, • de serveurs Web, • la vitesse de liaison. *** Les performances UTM peuvent être très inférieures à la performance du SPI.**	Evolutif? Envisagez vos besoins de croissance.	Evolutif? Envisagez vos besoins de croissance.
Configuration (nombre de ports, LAN, DMZ, WAN)	Vérifiez si les ports réseau sont assignés à des zones ou s'il sont configurables, et si le nombre fournis est suffisant	ICSA	ICSA , Common Criteria EAL4 +
Type d'accès VPN	* IPSEC **les plus courantes** soutenue * PPTP soutenue par certains, pare-feu seulement * SSL / VPN généralement un produit séparé, mais certains pare-feu comprennent l'accès SSL pour les petits nombre d'utilisateurs.	PPTP ou IPSEC peuvent être OK selon le niveau de sécurité requis. Les fonctionnalités Firewall + SSL / VPN peuvent être OK pour les petites nombre d'utilisateurs.	IPSEC est l'option la plus sûre. Peut-être prévoir l'achat de produits séparés pour la gestion SSL / VPN dans le but d'avoir des performances optimales pour certains pare-feu.

Niveau de sécurité

Critères	Considérations	Petites organisation	Moy. et grandes organisations
Certifications / Conformité	* **ICSA** est le niveau de certification de base * **Common Criteria** (EAL 4 + est souhaitable	ICSA	ICSA , Common Criteria EAL4 +
Avis du CERT (Vulnérabilités trouvées)	Les fournisseurs dont les produits ont peu de vulnérabilités et disposant de mécanismes de mise à jour rapide sont souhaitables	Plus petit nombre possible, rapidement fixés par téléchargements correctif éditeur	Aucune vulnérabilité souhaitable
Protection architecture * pare-feu Stateful sont requis + Stateful Proxy Firewall sont mieux * S'assurer d'avoir un OS sécurisé, robuste, de bonne conception, et jouissant d'une bonne réputation * IPS (basée sur la detection des signatures) * Unified Threat Management travaillant en couche 7	* Pare-feu Stateful est le minimum requis en entreprise (SPI) * Pare-feu avec des modules proxy pouvant fournir d'autres protections des réseaux internes * Evaluer la qualité et le type de filtrage de contenu de l'UTM	* Minimum: Stateful et à base de proxy antivirus et IPS en couche 7 * Désiré: UTM complet	* Minimum: Stateful Proxy + basée UTM complète + IPS + Protection contre les anomalies

Fiabilité, la redondance et de soutien

Critères	Considérations	Petites organisation	Moy. et grandes organisations
Architecture redondante * Double alimentation * Disk RAID ou Solid State * WAN Failover et loadbal. * Haute disponibles (une unité à l') basculement (2 unités)	* Mission Critical firewalls a besoin de certaines ou l'ensemble de ces caractéristiques * High Availability peut être actif-actif ou active-passive	Nice d'avoir. WAN basculement requises pour la mission Installations critiques	Obligatoires
Soutien * 8 heures x 5 jours par semaine * 24 heures x 7 jours par semaine	Choisir le niveau de soutien approprié	8 × 5, sauf Mission Critical	24 × 7
Garantie et temps de réponse * 1 ou 3 ans de garantie typiques * Dépôt de service (la poste) = plus lent * Sur place le jour ouvrable suivant = prochaine meilleure * 4 = Heure Onsite meilleurs	Choisir le niveau approprié de garantie de continuité d'activité	1 ou 3 ans. / Dépôt ou le bus suivant. réponse le jour	3 ans. + / Moins prochain bus. réponse le jour

Gestion & Reporting

Critères	Considérations	Petites organisation	Moy. et grandes organisations
* Network Management des outils et des journaux * Bande passante de surveillance * Le lissage du trafic * Journaux de base et de reporting	Certain nombre de balance des outils avec l'administrateur niveau de compétence. Peut être critique avec beaucoup de PC sur le réseau	Rapports de base	Niveau de l'entreprise des outils et des rapports requis

Prix

Critères	Considérations	Petites organisation	Moy. et grandes organisations
* Prix d'achat initial pour l'appareil * **Abonnements** supplémentaires pour Gateway, sécurité, etc * **Les frais de soutien, de garantie et de réparation Des frais d'installation ?***	Choisissez un appareil qui va grandir avec vous. Choisissez un fournisseur qui peut vous fournir d'autres solutions informatiques.	Trouver l'équilibre entre le coût à court et long terme, l'exposition de la sécurité, et soutenir la croissance	Focus sur le potentiel à long terme risque de perte d'actifs / revenus

D.I.Y. (Do It Yourself): Pare-feu “from scratch”

Littéralement D.I.Y. veut dire « bricolage ».

Pourquoi ce titre ironique ?
… et bien pour le simple fait qu’avoir la prétention de concevoir son propre pare-feu « from scratch » avec un simple PC pour protéger une entreprise en 2011, vu la quantité de menaces et surtout le niveau technique auxquelles la plupart se situent, revient à vouloir construire une cathédrale en 1 jour.

C’est impossible vous ne parviendrez pas à assembler un hardware fiable et robuste puis intégrer une pile logiciel robuste, testée, validée avec une équipe réduite.

De plus, quid de la maintenance, du suivi, des patches noyau à appliquer, des évolutions produit si votre guru GNU/Linux vous abandonne lâchement ?

Enfin il faut un très bon niveau en Scripting Bash pour tenter de mettre en place un ensemble de règles modulables ?

Il faut démystifier le pare-feu sous GNU/Linux (ou autre plateforme aussi robuste soit-elle) monté « from scratch ». Vouloir transformer une distribution Centos ou Debian en un pare-feu professionnel est à la portée de très peu de gens, et encore, en mettant combien de temps ?

Et pourtant … savoir monter un pare-feu basique sous GNU/Linux (ou OpenBSD) constitue en plusieurs points une connaissance fort intéressante pour appréhender de vrai pare-feu professionnel.

Alors pourquoi dédier une partie de ce cours à ce type de pare-feu (made in home) ?

Simple : comprendre le fonctionnement d’un filtre de paquet (ici NetFilter sera à l’honneur) et savoir le mettre en œuvre. Cela permet de comprendre, par la suite, le **comportement de beaucoup de moteurs de filtrage qui sont intégrés sur la plupart des pare-feu professionnel**.
En effet ces derniers s’appuient bien souvent sur les moteurs de filtrage de paquets libre :

- IPchains-Linux,
- Netfilter-Linux,
- Packet Filter-OpenBSD,
- IPFilter-BSD/SOLARIS – IPFW Mac OS X,
- IPFirewall-FreeBSD.

Note: Pourquoi ne pas choisir une base Windows pour monter un pare-feu « from scrtach » ?
Parce que Windows respecte très peu les « Best practices » vus précédemment et surtout parce qu’il n’est vraiment pas fait pour çà (ceux qui ont eu à gérer des ISA Serveur doivent comprendre ce que je veux dire).
Pour les curieux Microsoft propose une gamme « ForeFront » dédiée à la sécurisation du réseau … mais aucun de ces produits n’est intégré dans un « Appliance » : je vous laisse tirer vos conclusions !
Cependant avec les versions « Core » de ses serveurs Microsoft amorcent un virage … à suivre donc.

La première chose à faire est de choisir une distribution GNU/Linux que vous maîtrisez au mieux, ne vous lancez pas avec une « Gentoo » si vous ne savez pas ce qu’est « emerge ».
Bien sûr on évitera de préférence celles :

- orientées « desktop » (Ex. : Ubuntu à laquelle on préfèrera Debian)
- les laboratoires de test, instable (Ex. : « Fedora » à laquelle on préfèrera « Centos » ou « RedHat »).

Quoi qu’il en soit je ne conseille pas le déploiement d’une distribution généraliste en tant que pare-feu de production : vous l’aurez compris ;-) …….. Même à la maison !

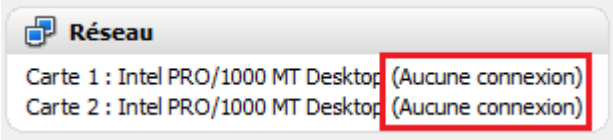
Pour la suite nous allons prendre une Centos comme base

Cependant une OpenBSD serait préférable mais peu de gens connaissent cette plate-forme alors soit … allons pour Centos (qui est une RedHat Enterprise).

Installation : faire les bons choix

1. La première chose à faire est de vous munir du média d'installation le plus à jour, en évitant les versions X.0, et SURTOUT de vérifier son intégrité physique.
   Les sommes (MD5, RSA) de contrôle disponibles sur le site de téléchargement sont là pour ça. Elles permettent deux choses essentielles en termes de sécurité :
   - Etre sure que le média n'est pas issue d'une ISO modifiée par malveillance,
   - Valider l'intégrité de la distribution que vous vous apprêtez à installer.

2. Procéder à une installation offline (pas de connexion réseau). Avec « Virtual Box » (logiciel de virtualisation gratuit d'Oracle) voici comment procéder :



3. Installer le minimum de paquetages (via la personnalisation des choix des paquetages à installer), vi suffira. Et surtout **pas de service serveur où d'interface graphique** (style Gnome, KDEetc.).
   Le plus simple étant de tout désélectionner les groupes de paquetages et garder un « système de base ». Ce dernier présentera une surface d'attaque réduite, mais que nous devrons encore réduire car par défaut nous avons déjà trop de programme s'exécutant en tâche de fonds.

   A l'invite choisissez un mot de passe fort (pas de mot du dictionnaire ou prénom, des caractères spéciaux et des chiffres) pour le compte « root ».

   Exemple sur une Centos 5.5 (on désélectionne tout sauf « Vi » et « Systèmes de base » / « Base ») :

4. Une fois l'installation effectuée, ôtez le média d'installation, au « First Boot » laissez les choix par défaut, il sera plus judicieux de monter ses propres règles (nous sommes « offline »).
   Il faut savoir que sur une distribution GNU/Linux, par défaut, les règles sont souvent trop permissives et surtout vous n'aurez pas une connaissance précise de ce que fait réellement votre pare-feu.
5. Veuillez créer un compte « admin » en simple utilisateur.

Votre pare-feu est installé mais en l'état actuel il ne vous protège pas beaucoup, surtout en ce qui concerne les attaques internes. Voyons comment sécuriser un peu mieux votre distribution.
Votre pare-feu s'appuie sur un filtrage de paquet performant : NetFilter. La suite va nous permettre de comprendre ses concepts et de le paramétrer.

Donc, retour à la théorie.

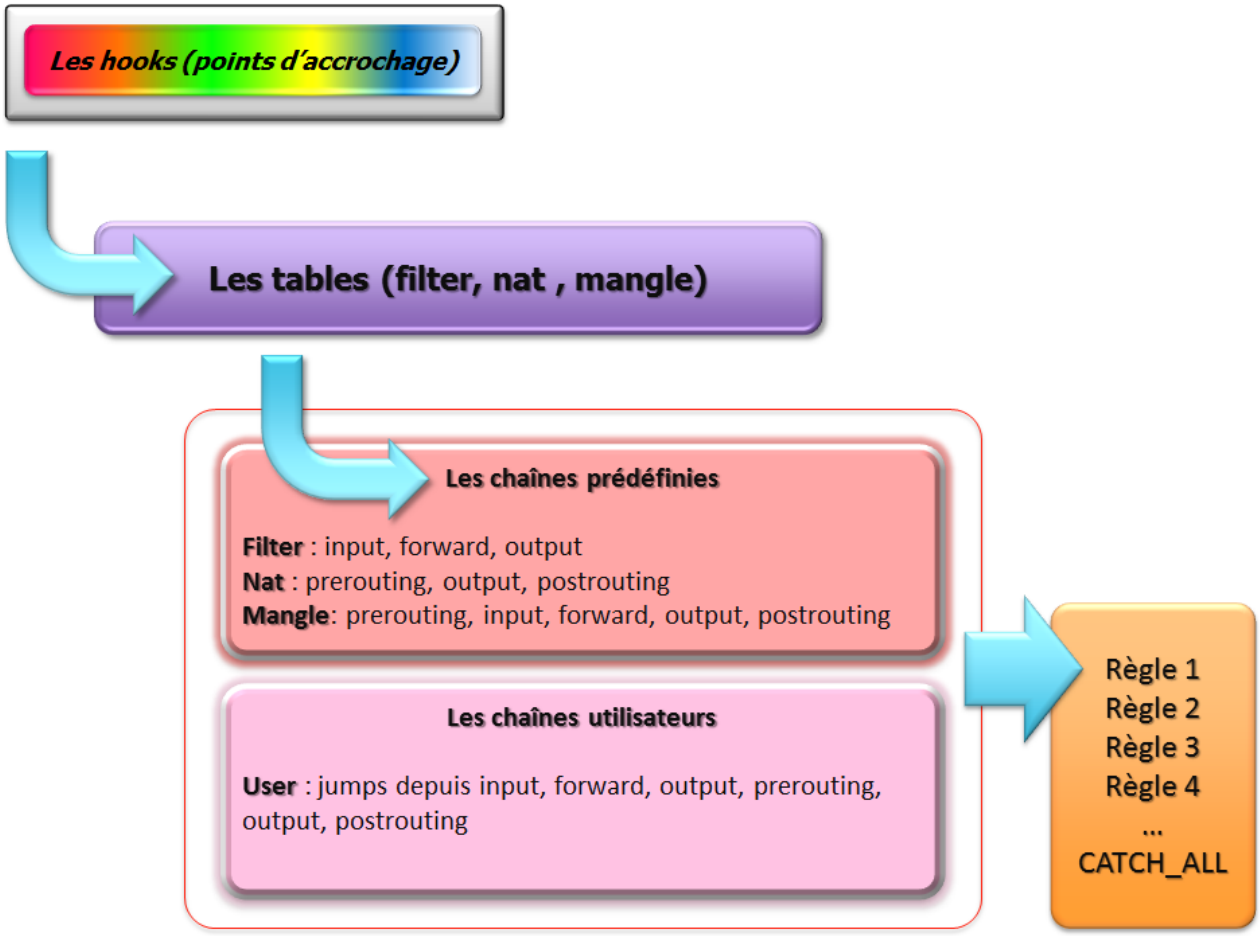
NetFilter c'est quoi ?

NetFilter est un Framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des points d'accrochage (**Hooks**) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau.

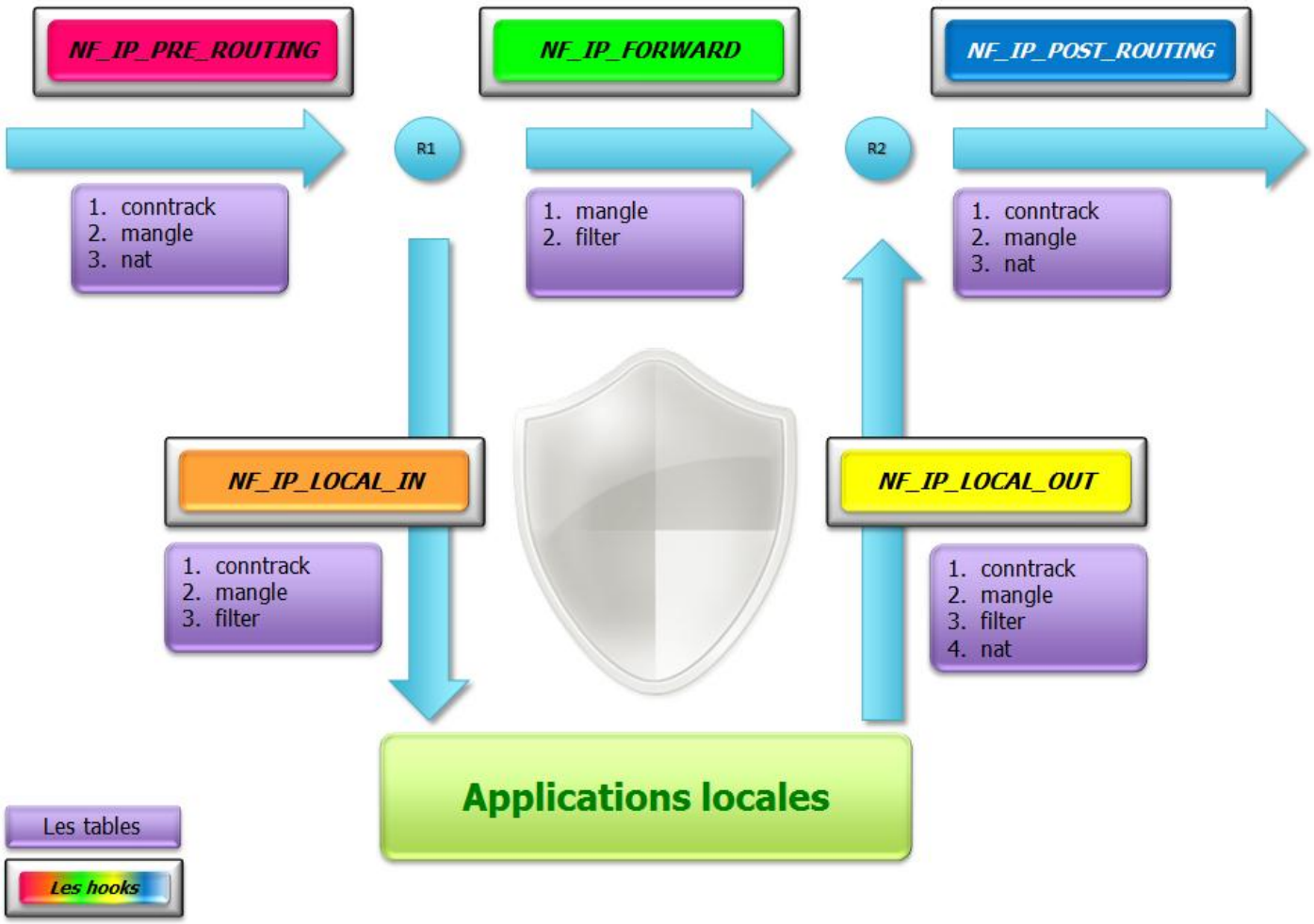
La version 1.4.2 a reçu un Certificat de Sécurité de Premier Niveau (CSPN) par l'Agence nationale de la sécurité des systèmes d'information

Le projet NetFilter/iptables a été lancé en 1998 par **Rusty Russell** (ci-contre), qui était aussi l'auteur du programme précédent, « ipchains ».

NetFilter est constitué ***de 5 points d'accrochage (Hooks)*** sur lesquels viennent se greffer les ***tables Filter, Nat et mangle.*** Dans chacune de ces tables prédéfinies il y a des ***chaînes dans lesquelles nous pourront créer nos règles de filtrage***. Il sera également possible de créer ses propres chaines : ***les chaînes utilisateurs***.



Voici comment nous pouvons schématiser les possibilités de passage d'un paquet IP dans le Framework NetFilter :



Veuillez noter les ***5 Hooks deNetFilter (NF_)*** :

- NF_IP_PRE_ROUTING,
- NF_IP_FORWARD,
- NF_IP_LOCAL_IN,
- NF_IP_LOCAL_OUT,
- NF_IP_POST_ROUTING.

Les 3 tables pouvant être accrochées sur ces certains de ces ***Hooks*** :

- Conntrack,
- Filter,
- Nat,
- Mangle.

« Conntrack » est à part, il s'agit de la table du module SPI assurant le suivi des connexions, les paquets qui se trouvent dedans peuvent être :

- ***NEW*** : le paquet ne correspond à un aucun flux connu dans la table « conntrack » et, s'il est accepté, donnera lieu à la création d'un nouvelle entrée dans cette table.

- ***ESTABLISHED*** : le paquet correspond à une entrée dans la table « conntrack », et fait donc partie d'une session existante.

- ***RELATED*** : le paquet est attendu par le moteur qui gère la table « conntrack » comme relatif à un flux existant, donc faisant partie d'une session en cours.
- ***INVALID*** : paquets pouvant être détruits pour plusieurs raisons.

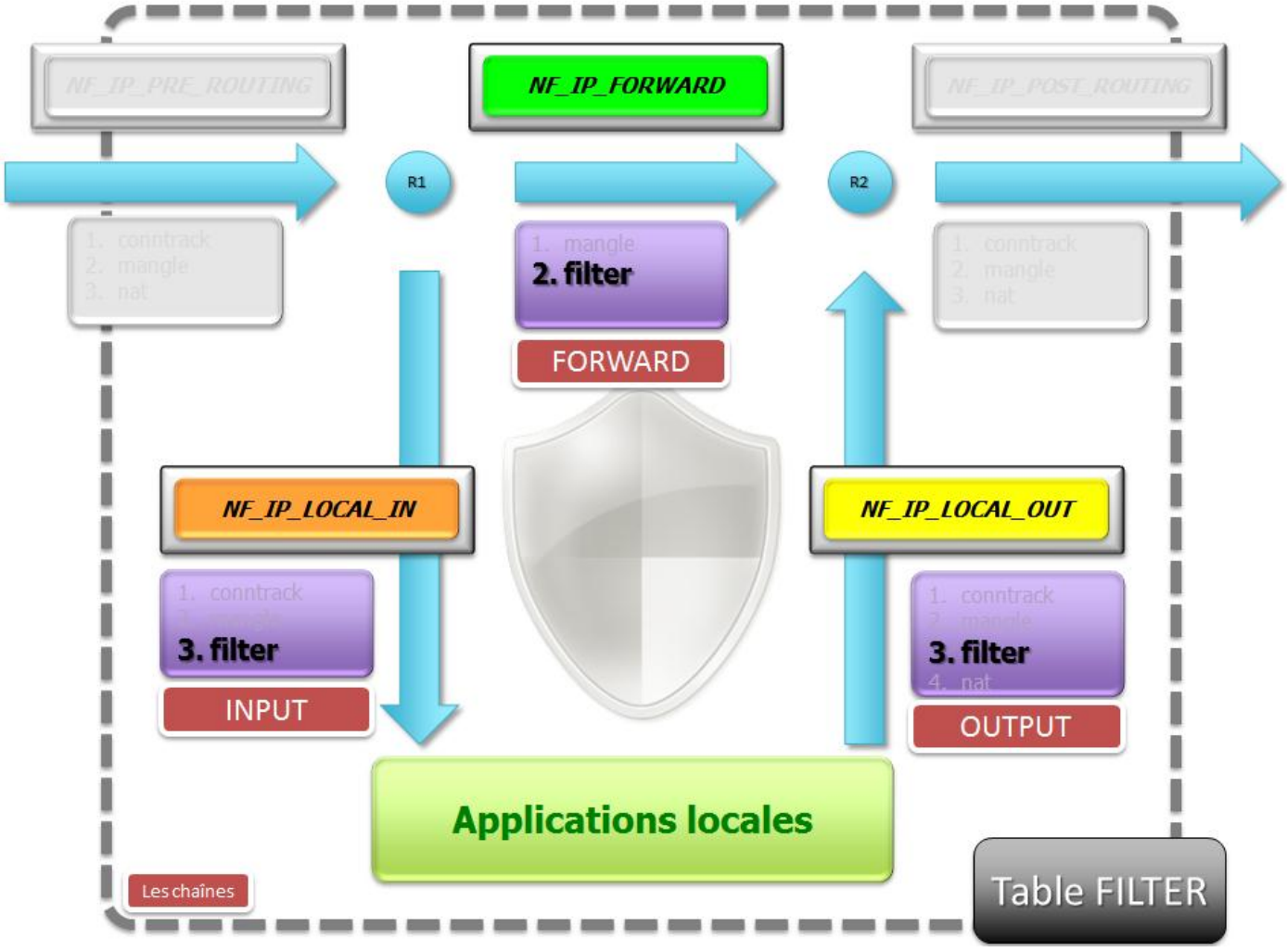
Maintenant focalisons nous sur la table « ***Filter »***. Il s'agit de la plus utilisée quand vous désirez construire un pare-feu avec «NetFilter ». « **IPTables** » est le logiciel qui permet d'utiliser le filtrage de paquet.

Cette table est présente sur les hooks :

- NF_IP_FORWARD,
- NF_IP_LOCAL_IN,
- NF_IP_LOCAL_OUT

Cela signifie simplement que vous pourrez **ajouter des règles de filtrage de paquets sur** :

- Les paquets destinés **<u>à traverser</u>** le pare-feu (chaines prédéfinie FORWARD), après la décision de routage (R1), il s'agit de la chaine la plus utilisée sur un pare-feu,
- Les paquets destinés **<u>à entrer dans</u>** votre pare-feu (chaines prédéfinie INPUT), après la décision de routage (R1),
- Les paquets destinés **<u>à sortir de</u>** votre pare-feu (chaines prédéfinie OUTPUT).

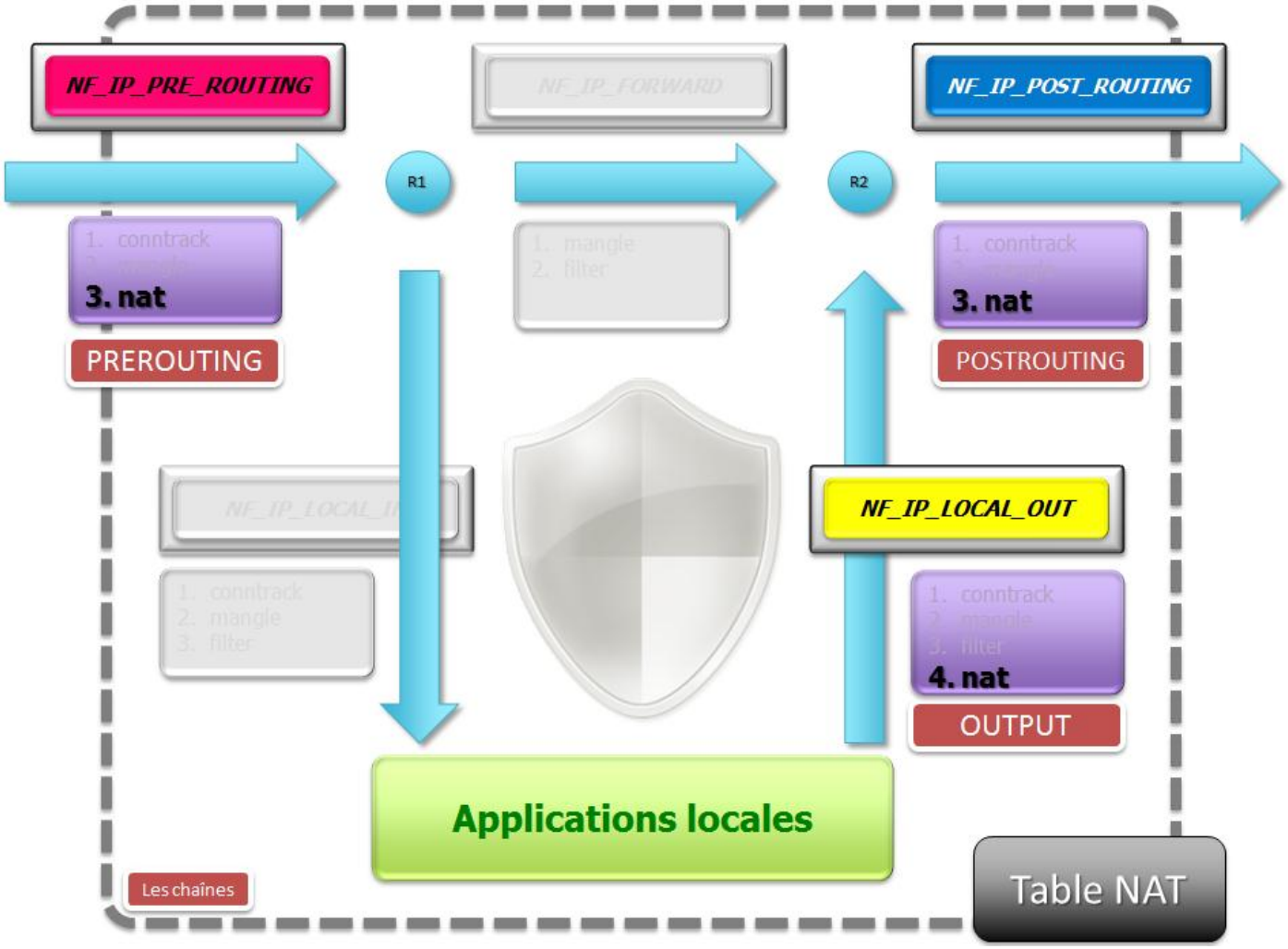


Voyons maintenant la table ***« nat »***.

Comme expliqué dans les chapitres précédents le « Nat » est un mécanisme qui permet de modifier à la volé les entêtes des paquets IP, TCP/IP, UDP etc. que ce soit en entrée ou en sortie.

En effet un **paquet arrivant** sur le hook ***NF_IP_PRE_ROUTING*** va pouvoir être modifié grâce à des règles placées dans la chaine prédéfinie « ***PREROUTING*** ».

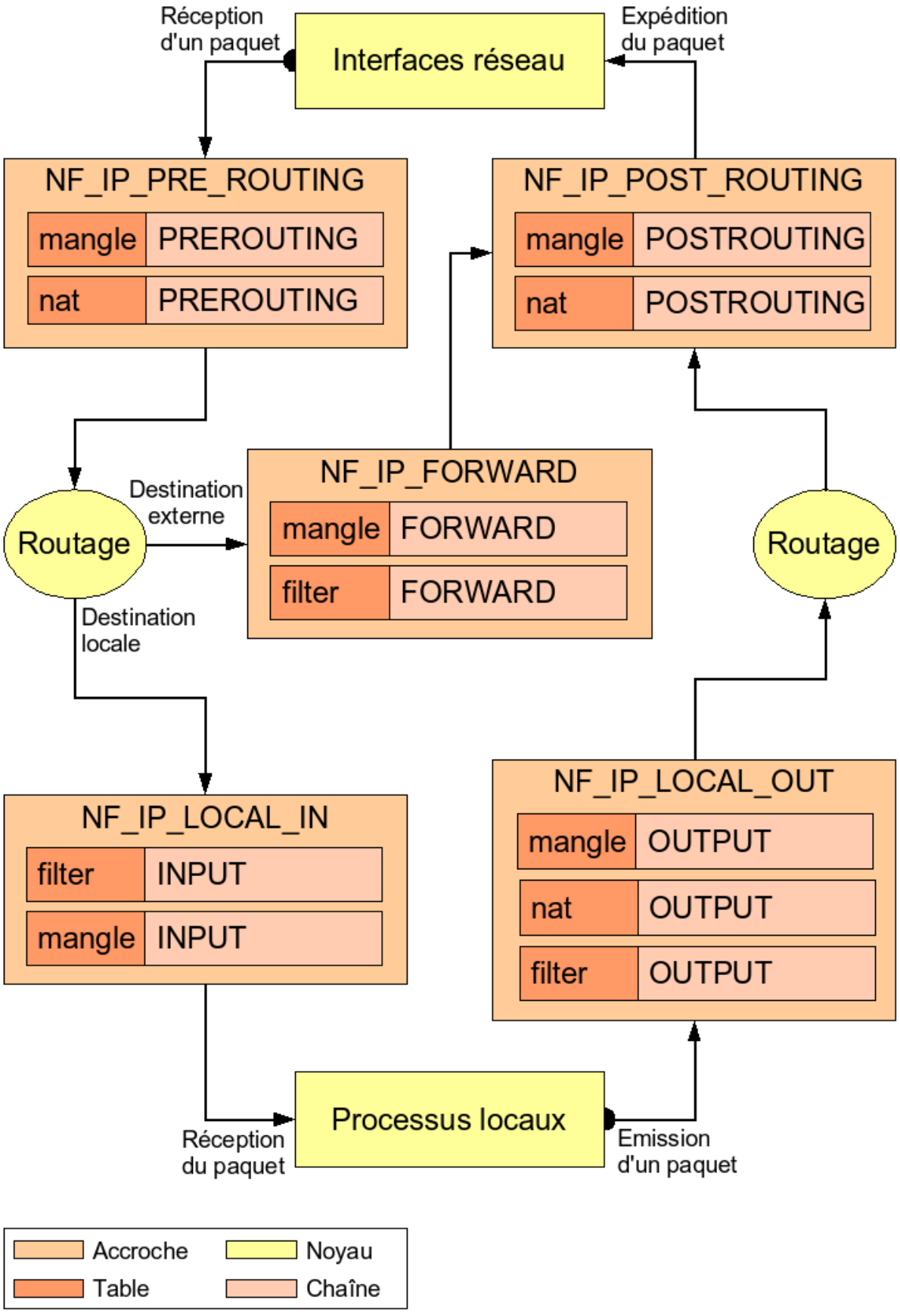
De même un paquet sortant de votre pare-fou pourra être modifié grâce à des règles placées dans les chaines prédéfinies « ***OUTPUT »*** *(avant la décision de routage en sortie R2) et* ***« POSTROUTING »*** *(après la décision de routage en sortie R2).* C'est souvent ici que l'on utilise la **cible MASQUERADE** (Masquage d'adresse)



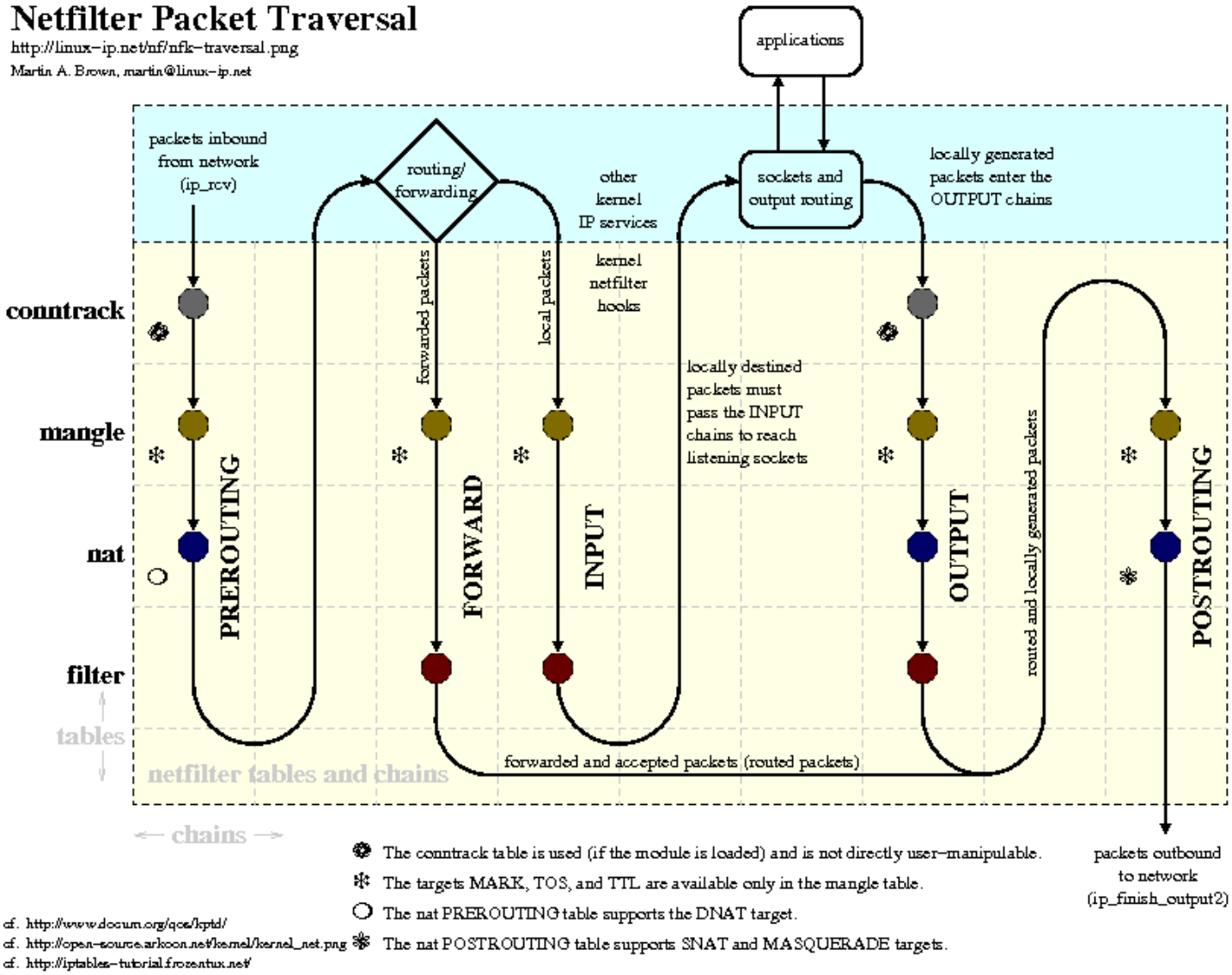
Nous verrons la pratique dans l'exemple qui va suivre ce rapide rappel des concepts de Netfilter.

Note : sachez qu'il existe également une table « mangle » qui permet de marquer les paquets, cela dépasserai le cadre de ce cours.

Synthèse 1


Réception d'un paquet
Interfaces réseau
Expédition du paquet
NF_IP_PRE_ROUTING
mangle PREROUTING
nat PREROUTING
NF_IP_POST_ROUTING
mangle POSTROUTING
nat POSTROUTING
Routage
Destination externe
NF_IP_FORWARD
mangle FORWARD
filter FORWARD
Routage
Destination locale
NF_IP_LOCAL_IN
filter INPUT
mangle INPUT
NF_IP_LOCAL_OUT
mangle OUTPUT
nat OUTPUT
filter OUTPUT
Réception du paquet
Processus locaux
Emission d'un paquet
Accroche
Noyau
Table
Chaîne

Synthèse 2



Sinon voici un très bon site qui explique le fonctionnement de NetFilter :

http://irp.nain-t.net/doku.php/130netfilter:start (Par Christian CALECA)

Maintenant que vous en connaissez un peu plus sur NetFilter voyons comment le paramétrer, de façon simple, pour transformer votre GNU/linux en mini pare-feu.

Mise en œuvre

Faisons un état des lieux du pare-feu installé et paramétré par défaut au chapitre précédent.

```
# Generated by iptables-save v1.3.5 on Sun Sep 11 12:28:07 2011
*mangle
:PREROUTING ACCEPT [469:49574]
:INPUT ACCEPT [469:49574]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [246:31196]
:POSTROUTING ACCEPT [246:31196]
COMMIT
# Completed on Sun Sep 11 12:28:07 2011
# Generated by iptables-save v1.3.5 on Sun Sep 11 12:28:07 2011
*nat
:PREROUTING ACCEPT [83:10484]
:POSTROUTING ACCEPT [2:140]
:OUTPUT ACCEPT [2:140]
COMMIT
# Completed on Sun Sep 11 12:28:07 2011
# Generated by iptables-save v1.3.5 on Sun Sep 11 12:28:07 2011
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [476:60500]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p esp -j ACCEPT
-A RH-Firewall-1-INPUT -p ah -j ACCEPT
-A RH-Firewall-1-INPUT -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Sun Sep 11 12:28:07 2011
```

Premier constat le routage n'est pas activé par défaut (ip_forward=0), le SNAT, bien que demandé, non plus.
On voit que sur une Centos 5.5 il y a une **chaîne utilisateur** créée dès l'installation : ***RH-Firewall-1-INPUT***.
Cette chaîne reçoit les paquets IP des chaînes par défauts : **INPUT** et **FORWARD** (OUTPUT laisse tout sortir du pare-feu : intéressant)

Par défaut tout peut rentrer depuis le LAN (eth1).
La politique par défaut de la chaîne utilisateur (accessible via les jump (-j) des chaines « FORWARD », « INPUT » de la table « filter ») est à « ACCEPT »
De plus cette chaîne finit par un REJECT.

Nous allons sécuriser tout cela.

Nous sommes sur un pare-feu à monter soi-même, alors c'est parti on va mettre les mains dans le cambouis …
Commencez par créer un fichier qui va nous permettre de sauvegarder votre politique de filtrage et configurer votre pare-feu.

```
vim firewall-simple.sh
```

Puis passez en mode édition (i):

Nous prendrons soin d'appliquer la première règle pour un pare-feu: on ferme complètement notre pare-feu.
« Tout ce qui n'est pas explicitement autorisé et par définition interdit ».

RAPPEL :
Voici la syntaxe de base de l'outil permettant de gérer le NetFilter : « iptables »
IP Tables a les options suivantes pour gérer l'ensemble des tables et chaînes :

Option	Action
-t <table> -L <chaine>	Liste les règles d'une chaîne ou celles de toutes les chaînes présentes dans la table (si chaine est omis)
-t <table> -F <chaine>	Efface toutes les règles dans une chaîne ou celles de toutes les chaînes
-t <table> -X <chaine>	Efface les règles d'une chaîne utilisateur ou celles de toutes les chaînes utilisateurs présentes dans la table (si chaine est omis)
-t <table> -A <chaine>	Ajoute une règle à la suite
-t <table> -D <chaine>	Efface une règle précise dans la chaine
-t <table> -I <chaine>	Insère une règle à une place précise dans la chaîne
-t <table> -N <chaine>	Création d'une chaîne utilisateur
Etc.	

Pour plus d'information faites un :

```
man iptables
```

Mise en place des **variables de fonctionnement** en début de votre script :

```
#!/bin/bash
# Mise en place du pare-feu
Nom_PareFeu=`hostname`
echo "Configuration des regles de filtrage de $Nom_PareFeu !"

################################################################################
# Binaires utilises
IPT=/sbin/iptables

################################################################################
# Variables

# Variables :les interfaces reseaux du pare-feu
if_lo="lo"
if_wan="eth0"
if_lan="eth1"
#if_dmz="eth2"

# Variables :les reseaux geres par le pare-feu
net_wan="dhcp"
net_lan="10.0.10.0/24"
#net_dmz="192.168.254.0/24"

# Variables :les adresses IP du pare-feu
ad_parefeu_wan=`/sbin/ifconfig $if_wan | grep "inet adr" | awk -F: '{print $2}' | awk
{'print $1}'`
ad_parefeu_lan=`/sbin/ifconfig $if_lan | grep "inet adr" | awk -F: '{print $2}' | awk
{'print $1}'`
#ad parefeu dmz=`/sbin/ifconfig $if_dmz | grep "inet adr" | awk -F: '{print $2}' | awk
{'print $1}'`

# Variables :les adresses IP des hotes geres par le pare-feu
any="0.0.0.0/0"
station_admin="10.0.10.100/32"
serveur_fichier="10.0.10.1/32"
serveur_mail="10.0.10.2/32"
serveur_dns_interne="10.0.10.3/32"
serveur_dns_externe_1="212.27.40.240"
serveur_proxy="10.0.10.3/32"
#serveur_ntp="ntp"
# Etc.
```

Ensuite nous allons **verrouiller TOUS les accès**, appliquer la politique restrictive et préparer la journalisation locale :

```
###############################################################################
# Mise en place de la politque restrictive (on remet tout a zero et DROP tout paquets
IP)
# Et des chaines utilisateur

# Effacement de toutes les regles dans toutes les chaines (tables filter, nat et
mangle) : -F
$IPT -t filter -F
$IPT -t nat -F
$IPT -t mangle -F
# Effacement de toutes les regles dans toutes les chaines utilisateurs (tables filter,
nat et mangle) : -X
$IPT -t filter -X
$IPT -t nat -X
$IPT -t mangle -X

# Definition de la politique de filtrage par defaut (-P) des chaines de la table
"filter"
# on "DROP" tous les paquets.
$IPT -t filter -P FORWARD DROP
$IPT -t filter -P INPUT DROP
$IPT -t filter -P OUTPUT DROP

# Definition de la politique de translation d'adresse par defaut des chaines de la
table "nat"
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT

# Definition de la politique de marquage des paquets par defaut des chaines de la table
"mangle"
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P FORWARD ACCEPT
$IPT -t mangle -P INPUT ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT
$IPT -t mangle -P POSTROUTING ACCEPT

# On cree la chaine utilisateur de journalisation des paquets rejetes
#$IPT -X LOG_DROP
$IPT -N LOG_DROP
$IPT -A LOG_DROP -j LOG --log-prefix 'NF PACKET DROP ==>' --log-level info # On
journalise le paquet indesirable
$IPT -A LOG_DROP -j DROP # On DROP le paquet apres l'avoir journalise

# Dans le même esprit on peut creer la chaine utilisateur de journalisation des paquets
acceptes
#$IPT -X LOG_ACCEPT
$IPT -N LOG_ACCEPT
$IPT -A LOG_ACCEPT -j LOG --log-prefix 'NF PACKET ACCEPT ==>' --log-level info # On
journalise le paquet desirable
$IPT -A LOG_ACCEPT -j ACCEPT # On ACCEPT le paquet apres l'avoir journalise
```

Maintenant que notre pare-feu ne laisse plus rien passer (en terme de filtrage de paquet) nous allons le rendre un minimum **communiquant** :

```
#############################################################################
# Mise en place de la politique de securité active

# Ajout de regle (-A : APPEND)
# Autorisation du trafic entrant et sortant (-i et -o) sur l'interface de "loopback"
(lo)
# Note : Quand on omet le parametre -t cela signifie que nous indiquons implicitement
la table "filter"
$IPT -t filter -A INPUT -p all -i $if_lo -j ACCEPT
$IPT -t filter -A OUTPUT -p all -o $if_lo -j ACCEPT

# Mise en place du SPI (Stateful_Packets_Inspection) pour tout protocoles : le suivi de
connexion TCP/IP
$IPT -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -t filter -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Ajout des regles par protocole

# Gestion ICMP
# ICMP en entree et en sortie sur le pare-feu
$IPT -t filter -A INPUT -p icmp -j ACCEPT
$IPT -t filter -A OUTPUT -p icmp -j ACCEPT
# ICMP vers le reseau exterieur
$IPT -t filter -A FORWARD -p icmp -j ACCEPT

# Administration du pare-feu via SSH pour la station admin depuis le LAN (tcp/udp)
$IPT -t filter -A INPUT -i $if_lan -s $station_admin -d $ad_parefeu_lan -p tcp --sport
1024:65535 --dport 22 -m state --state NEW -j ACCEPT
$IPT -t filter -A INPUT -i $if_lan -s $station_admin -d $ad_parefeu_lan -p udp --sport
1024:65535 --dport 22 -m state --state NEW -j ACCEPT

# Administration SSH pour la station_admin vers l'exterieur (tcp/udp)
#$IPT -t filter -A FORWARD -s $station_admin -d $any -p tcp --sport 1024:65535 --dport
22 -m state --state NEW -j ACCEPT
#$IPT -t filter -A FORWARD -s $station_admin -d $any -p udp --sport 1024:65535 --dport
22 -m state --state NEW -j ACCEPT

# Autorisation des demandes DNS vers l'exterieur (udp)
$IPT -t filter -A FORWARD -s $net_lan -d $serveur_dns_externe_1 -p udp --dport 53 -j
ACCEPT

# Navigation Web pour le poste du LAN : station_admin
$IPT -t filter -A FORWARD -s $station_admin -d $any -p tcp --sport 1024:65535 --dport
80 -m state --state NEW -j ACCEPT

# Autorisation des requetes DNS du pare-feu vers l'exterieur
#$IPT -t filter -A OUTPUT -o $if_wan -d $serveur_dns_externe_1 -p udp --dport 53 -j
ACCEPT

# TABLE NAT
# une fois proteger, nous allons mettre en place la translation d'adresse : SNAT
# ... afin de permettre aux stations de la zone "LAN" de pouvoir sortir en se faisant
passer pour le pare-feu
$IPT -t nat -A POSTROUTING -o $if_wan -j MASQUERADE
# Note : en general seul le serveur proxy est SNATter, pas les stations clientes,
# mais comme nous ne montons pas de PROXY

# Translation d'adresse pour autoriser l'administration a distance du pare-feu
#$IPT -t nat -A PREROUTING -i $if_wan -p all --dport 22  -j DNAT --to-destination
$ad_parefeu_wan
```

```
# ACTIVATION DU ROUTAGE
# Note: Activation du routage (ip_forward)
echo 1 > /proc/sys/net/ipv4/ip_forward
# Sur centos : dans le fichier /etc/sysctl
```

Enfin nous allons journaliser et s'assurer qu'aucun paquet non désiré puisse passer : la cible DROP sera notre dernier mot.

```
#############################################################################
# FIN DU SCRIPT
#
# On logue les paquets indésirables, avec l'indication de la chaine qui a DROPé.
$IPT -t filter -A FORWARD -j LOG --log-prefix 'FORWARD_PKTS_DROP ==> ' --log-level info
$IPT -t filter -A INPUT -j LOG --log-prefix 'INPUT_PKTS_DROP ==> ' --log-level info
$IPT -t filter -A OUTPUT -j LOG --log-prefix 'OUTPUT_PKTS_DROP ==> ' --log-level info
# ... avec chaine utilisateur LOG_DROP + /etc/syslog.conf ==>kern.=info
#/var/log/iptables.log + service syslogd restart
#$IPT -t filter -A FORWARD -j LOG_DROP
#$IPT -t filter -A INPUT -j LOG_DROP
#$IPT -t filter -A OUTPUT -j LOG_DROP

# CATCH-ALL", au cas ou l'on n'utilise pas la chaine utilisateur "LOG_DROP"
# on "DROP" tous les paquets.
$IPT -t filter -A FORWARD -j DROP
$IPT -t filter -A INPUT -j DROP
$IPT -t filter -A OUTPUT -j DROP
```

Sur une Centos voici les commandes pour mettre en production de façon permanente votre script de pare-feu :

```
chmod +x <votre_script.sh>
sh ./<votre_script.sh>
service iptables save
```

Vérification :

```
iptables-save ou service iptables status
```

Attention : votre service « iptables » doit être lancé au runlevel par défaut.

Note : avec ce type de journalisation on débugue aisément le comportement du pare-feu à l'aide d'un tail -f /var/log/messages ou tail -f /var/log/iptables.log

Voici un résumé des règles que nous avons misent en place :

```
# Generated by iptables-save v1.3.5 on Sun Sep 11 12:22:09 2011
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:LOG_ACCEPT - [0:0]
:LOG_DROP - [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -s 10.0.10.100 -d 10.0.10.254 -i eth1 -p tcp -m tcp --sport 1024:65535 --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -s 10.0.10.100 -d 10.0.10.254 -i eth1 -p udp -m udp --sport 1024:65535 --dport 22 -m state --state NEW -j ACCEPT
-A INPUT -j LOG --log-prefix "INPUT_PKTS_DROP ==> " --log-level 6
-A INPUT -j DROP
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -s 10.0.10.0/255.255.255.0 -d 212.27.40.240 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -s 10.0.10.100 -p tcp -m tcp --sport 1024:65535 --dport 80 -m state --state NEW -j ACCEPT
-A FORWARD -j LOG --log-prefix "FORWARD_PKTS_DROP ==> " --log-level 6
-A FORWARD -j DROP
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -j LOG --log-prefix "OUTPUT_PKTS_DROP ==> " --log-level 6
-A OUTPUT -j DROP
-A LOG_ACCEPT -j LOG --log-prefix "NF PACKET ACCEPT ==>" --log-level 6
-A LOG_ACCEPT -j ACCEPT
-A LOG_DROP -j LOG --log-prefix "NF PACKET DROP ==>" --log-level 6
-A LOG_DROP -j DROP
COMMIT
# Completed on Sun Sep 11 12:22:09 2011
# Generated by iptables-save v1.3.5 on Sun Sep 11 12:22:09 2011
*nat
:PREROUTING ACCEPT [69:18691]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [28:1960]
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Sun Sep 11 12:22:09 2011
# Generated by iptables-save v1.3.5 on Sun Sep 11 12:22:09 2011
*mangle
:PREROUTING ACCEPT [255:30619]
:INPUT ACCEPT [255:30619]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [178:24608]
:POSTROUTING ACCEPT [150:22648]
COMMIT
# Completed on Sun Sep 11 12:22:09 2011
```

Note : observez qu'à chaque fin de chaîne nous faisons un DROP systématique des paquets en plus de la politique par défaut qui est à DROP.

En annexe vous est proposé un exemple de script « iptables » se rapprochant de la philosophie d'un pare-feu multizones professionnel en production. Il use massivement des chaines utilisateurs et respecte minutieusement la gestion de plusieurs zones de sécurité. Cependant il ne code pas les attaques basiques sur une pile IP.

Pour un script beaucoup plus aboutit vous pouvez vous tourner vers des scripts comme :

- Arno's IPTables Firewall,
- Shorewall.

« Hardening » basique

Ce qu'il reste à faire :

- Codage des contre-mesures pour les attaques basiques (IP_spoofing, etc.)
- Epuration des services superflus ou inutiles pour un pare-feu,
- Mise à jour automatique,
- Durcissement de la couche système avec des outils tels : samhain, arpwtachdog, chkrootkit, selinux Firewall Watchdog, AppArmor, Smack, TOMOYO, etc…
- il existe également des paquets spéciaux qui permettent de sécuriser plus sérieusement une distribution existante. Les deux variantes les plus connues sont Hardened Gentoo et Hardened Debian,
- Préparation à la Redirection des journaux vers un serveur « syslog » dédié et protégé,
- Penser à la mise en place d'un script plus élaboré comme celui fournis en annexe.

La cible ULOG (vs LOG)

Plutôt que d'utiliser « syslog », cette cible permet d'envoyer les paquets à un démon spécialisé : ulogd. Ce démon permet d'obtenir des logs plus présentables, voire stockés dans une base de données comme MySQL (déportée).

Question : disposons-nous d'une solution professionnelle ?
De nos jours ce n'est plus suffisant : Proof of concept, supervision, gestion centralisée etc

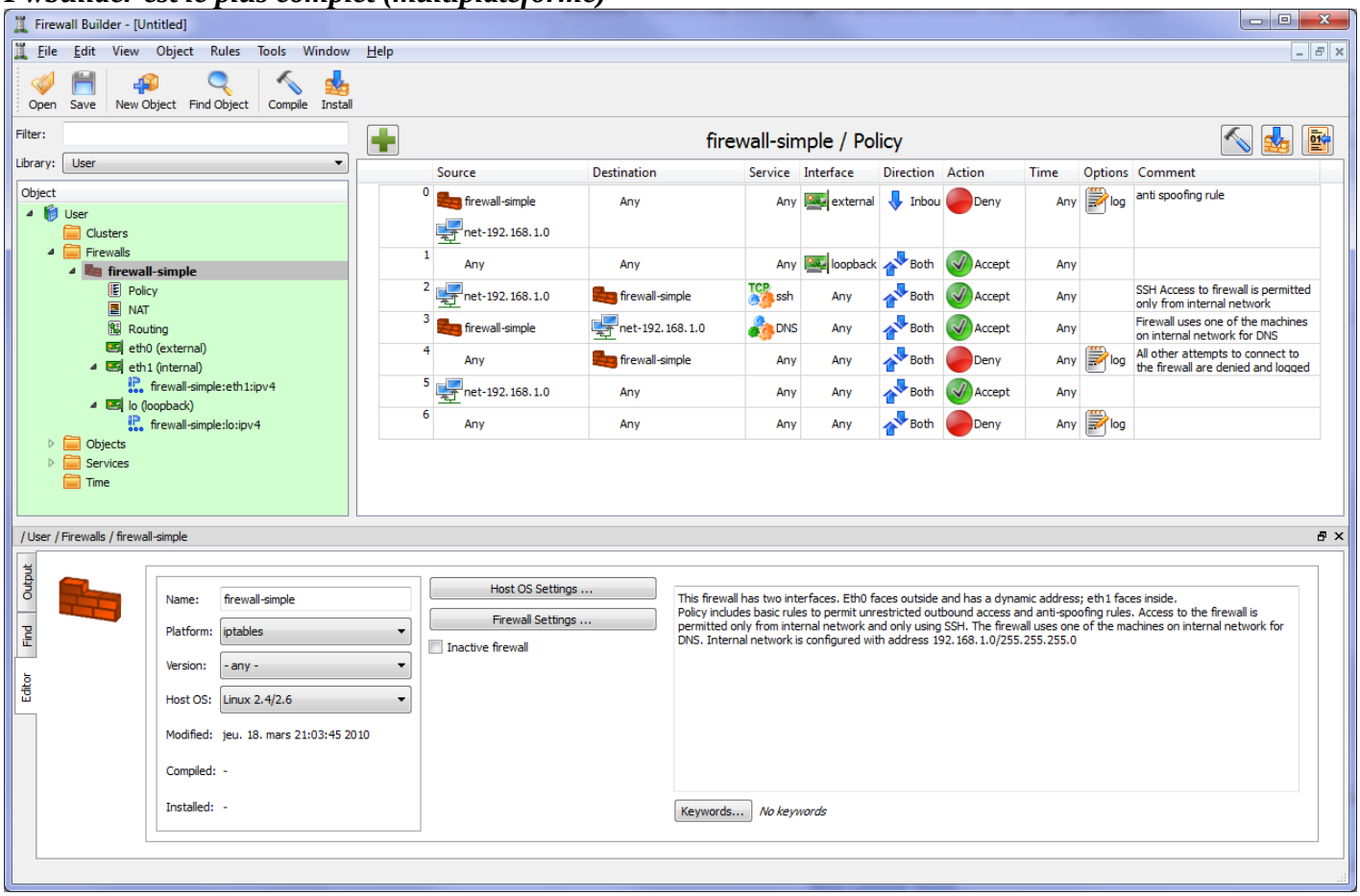
Autre piste de pare-feu à faire soit même, OpenBSD = un très bon choix (discussion)

Les GUI pour NetFilter

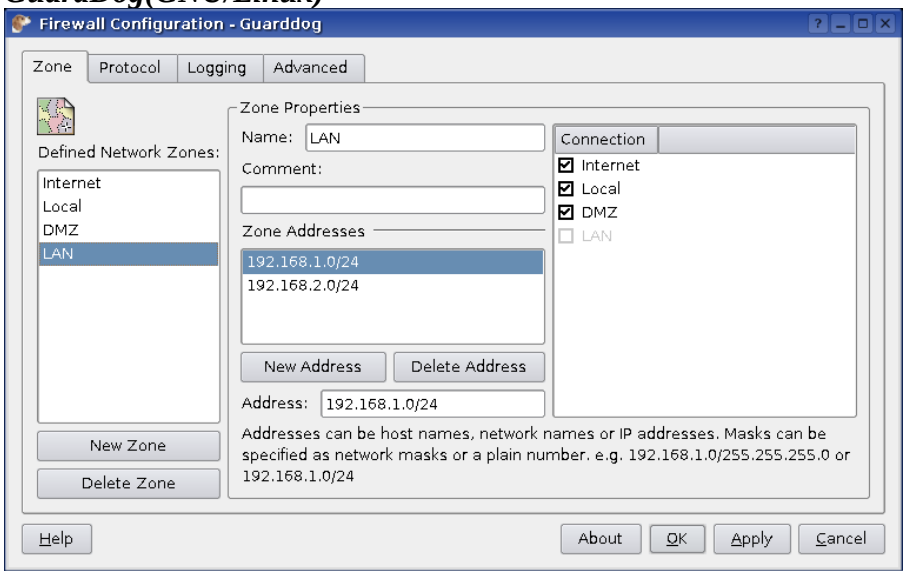
Nous avons généré nous-même nos règles « iptables » mais il faut savoir qu'il existe quelques frontaux graphiques pour la commande « iptables »
Ces derniers vont vous permettre de vous concentrer sur l'essentiel : votre politique de filtrage des flux.

En voici quelques-uns :

Fwbuilder est le plus complet (multiplateforme)

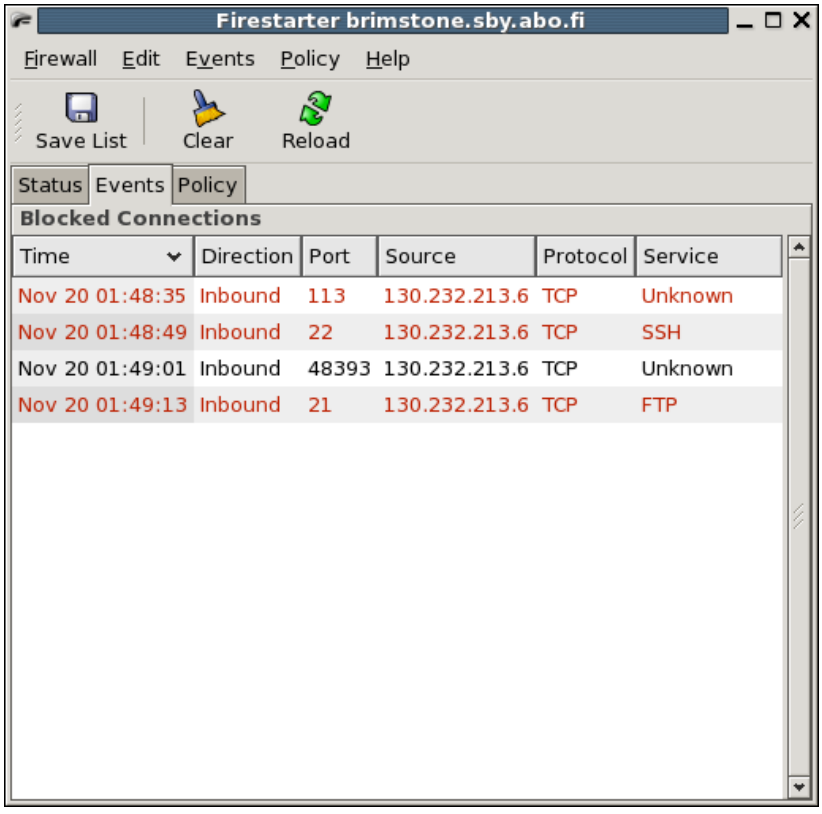


GuardDog(GNU/Linux)



GuFW (Ubuntu/Gnome)

FireStarter



Ces frontaux graphiques vont vous permettre de **coder des règles simples**, essentiellement en se basant sur la table « Filter ». Ici pas d'utilisation de la table « mangle » … encore moins question de « hardenning » de votre base système

Pour cela il va falloir nous tourner vers les distributions spécialisées en sécurité.
Des distributions où l'expert en sécurité va pouvoir se concentrer sur l'essentiel de son métier : la mise en place d'une politique de sécurité globale en s'appuyant sur des spécificités bien précises pour assurer la fonctionnalité qui est celle d'un pare-feu au sein d'un SI sécurisé.

La raison : les distributions spécialisées « Pare-feu »

Comme vous avez pu vous en apercevoir dans le chapitre précèdent transformer une distribution GNU/linux en un pare-feu digne de ce nom est un travail de longue haleine sans garantie que les résultats soient à la hauteur d'un produit exploitable en production.
A la maison cela peut passer, et encore vu le niveau des attaques actuels j'ai des doutes, mais vouloir déployer ce genre de pare-feu en milieu professionnel relève de la pure inconscience.

L'argument du budget pour défendre ce genre de mise en place n'en n'est pas un : il existe de très bonne distribution dédiée à la sécurité qui pourront tenir une place honorable au sein de petites ou moyennes entreprises.

Sachez qu'en installant une distribution dédiée sécurité vous n'échapperez pas au travail d'intégration de cette dernière sur le matériel que vous aurez judicieusement choisi.
Le simple PC à recyclé peut convenir, néanmoins je vous suggère pour une ou deux centaines d'euro de vous munir d'un boitier dédié à ce genre d'usage (attention à la compatibilité de la distribution sur certaines architecture matériel : Geode, Arm, VIA etc., le mieux étant les cartes ITx à base de 3 connecteur RJ45 réseaux et d'un cpu intel).

De façon générale une distribution dédiée sécurité est une distribution GNU/Linux, FreeBSD, BSD etc. basée sur un système épuré voir « From Scratch », faisant office de pare-feu.

Elle vise à fournir un moyen simple mais puissant pour configurer un pare-feu sur une architecture de type PC. Elle peut protéger sur une telle architecture un réseau familial ou de petites ou moyennes entreprises, elle offre la classique Zone démilitarisée, interne, externe ainsi que les tunnels réseau privé virtuel (acronyme VPN en anglais).

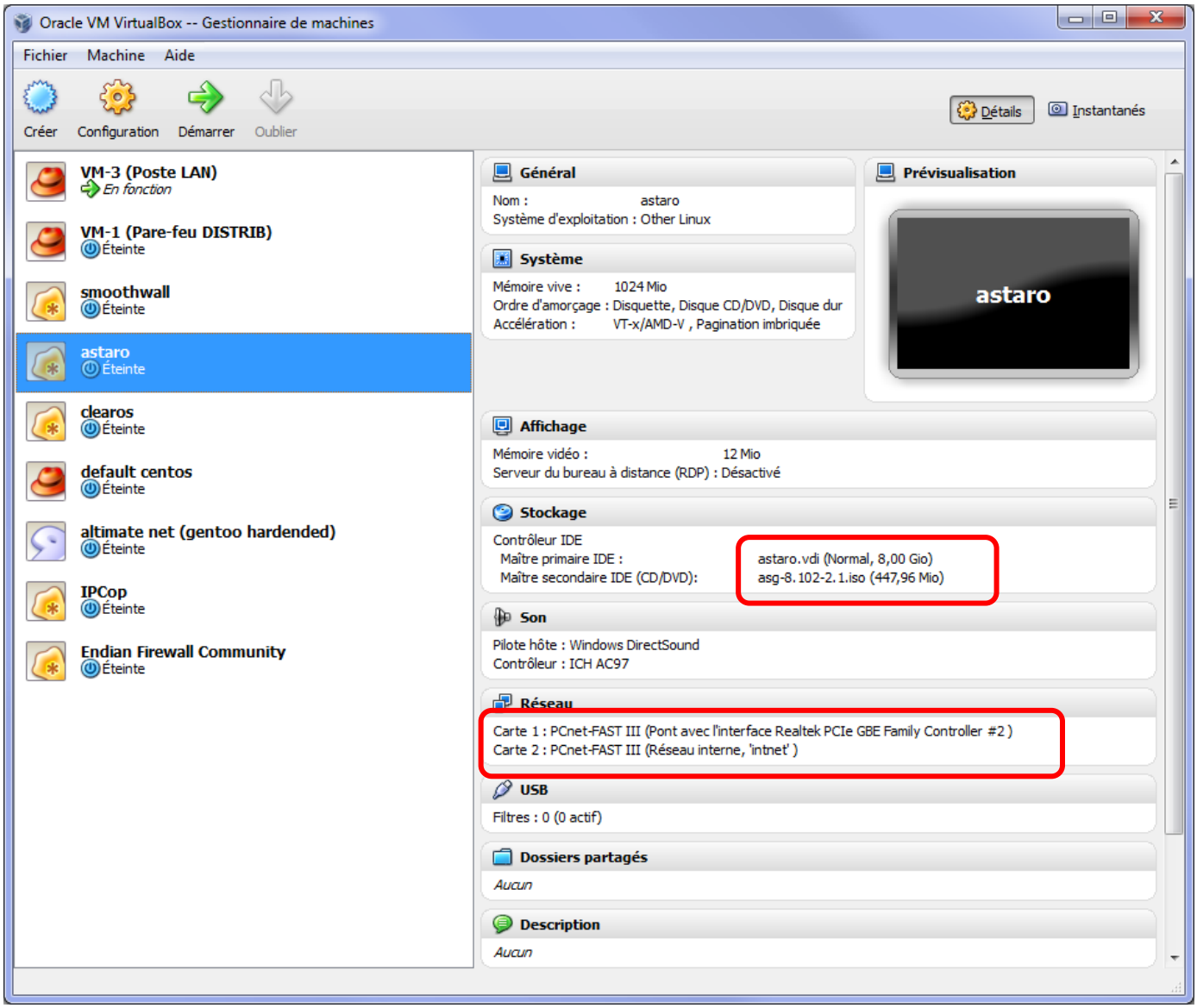
Elle peut éventuellement servir de serveur mandataire (proxy), serveur fournissant des adresses IP dynamique (DHCP), de relais DNS, de serveur de temps (NTP), et en installant des greffons ou modules, de bien d'autres choses (contrôle de contenu, liste noire, liste d'accès, DNS dynamique, contrôle de trafic, etc...). Le support des clients sans fil est aussi prévu par le biais d'une zone dédiée.

Les images ISO des CD-ROM d'installation (moins de 50Mo à la taille d'un CD) sont généralement disponibles via un réseau de sites miroirs.

Ces distributions sont le fruit de plusieurs années de développement par des équipes ou communautés de spécialistes reconnus (Rusty RUSSEL, McHARDY etc…) en système et sécurité : ils ont déjà fait 75 % du travail d'intégration et de « hardenning »sur ces distributions. Les autre 25% étant souvent réservés aux produits commerciaux…..

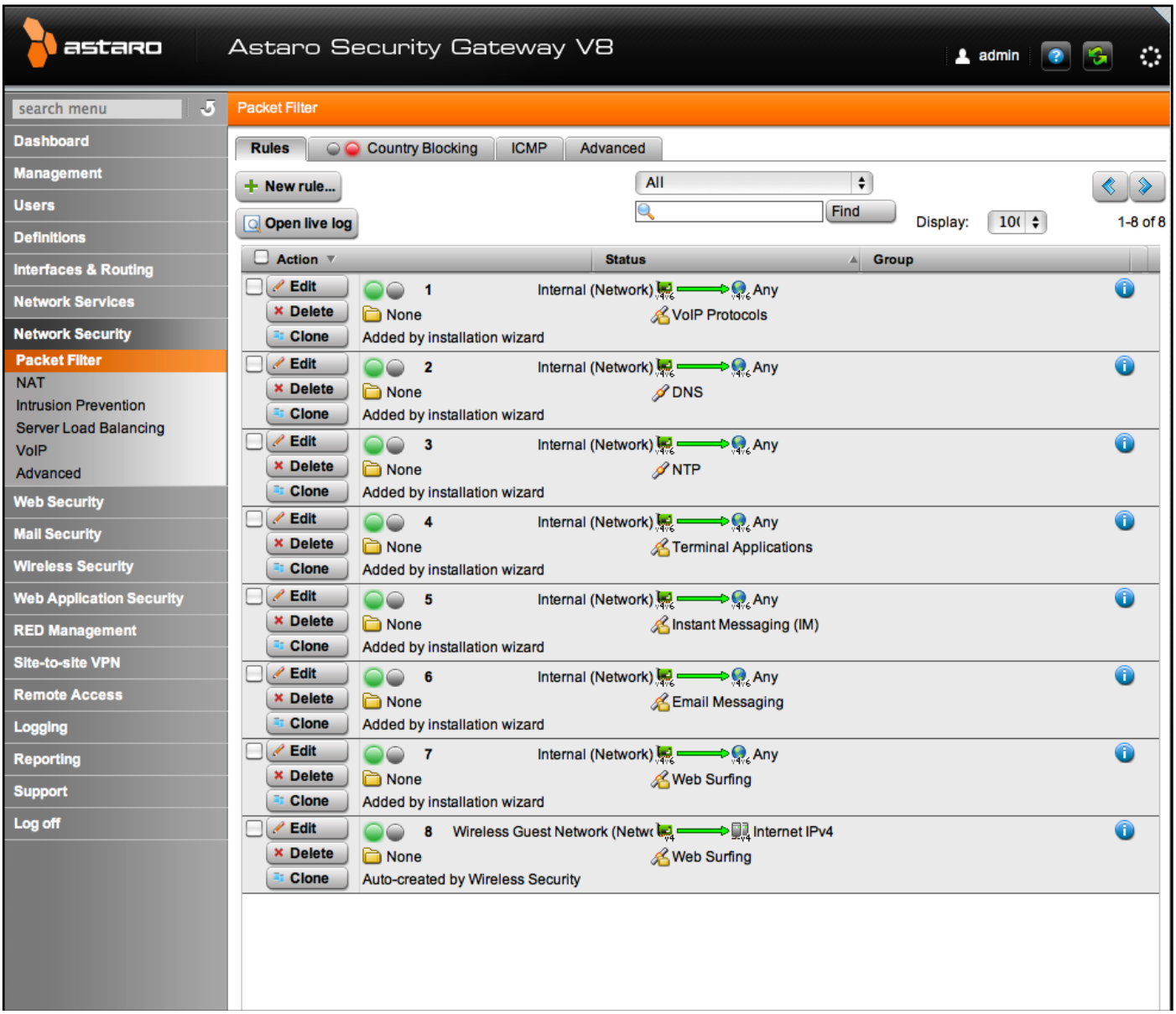
Distributions basées sur GNU/Linux:

Vous pouvez vous forger un avis sur chacune d'entre elle en vous servant d'un outil de virtualisation :



Astaro

Astaro Network Security comprend des fonctions entièrement intégrées telles qu'un pare-feu configurable associé à un système de protection contre les intrusions, le déni de service, les transferts de trafic, des outils NAT. Astaro est une société allemande qui propose cette version gratuite et compte dans son effectif quelques membres de la Core team de NetFilter (via sponsorisation à plein temps).



Cette distribution contient en autre les modules suivants :

Intrusion Prevention
En scrutant le trafic approuvé du réseau, le système IPS peut séparer le trafic légitime du trafic dangereux et protéger ainsi votre réseau contre les attaques extérieures.

DoS Protection
Les logiciels malveillants les plus basiques peuvent aisément détecter les connexions Internet et les utiliser de façon mal intentionnée. La prévention de déni de service de cette distribution GN/Linux permet de sécuriser vos ressources pendant ces attaques afin qu'elles ne subissent aucun dommage.

Bandwidth Control

La bande passante Internet limite souvent la rapidité de fonctionnement des réseaux. Ce module permet de garantir une certaine qualité de service pour vos utilisateurs.

Branch Office VPN
L'établissement de liaisons entre des sites distants et un bureau principal permet aux utilisateurs d'envoyer et de recevoir des informations via une connexion sécurisée. Avec le module VPN, les utilisateurs peuvent relier des centaines de sites sans expérience en configuration de réseaux VPN.

SSL Remote Access
Les voyageurs et le personnel de terrain se trouvent fréquemment en dehors de leur bureau ou de leur bureau à domicile ; ils ont donc besoin d'une connexion stable et sécurisée pouvant fonctionner à n'importe quel endroit. L'application SSL Remote Access de cette distribution permet de résoudre ce problème.

IPSec Remote Access
Pour que les travailleurs sur le terrain, puissent mener leurs activités il s'avère souvent nécessaire de pouvoir accéder aux ressources du réseau d'entreprise. A l'aide d'un client spécial, les utilisateurs peuvent accéder aux ressources qui se trouvent derrière cette distribution.

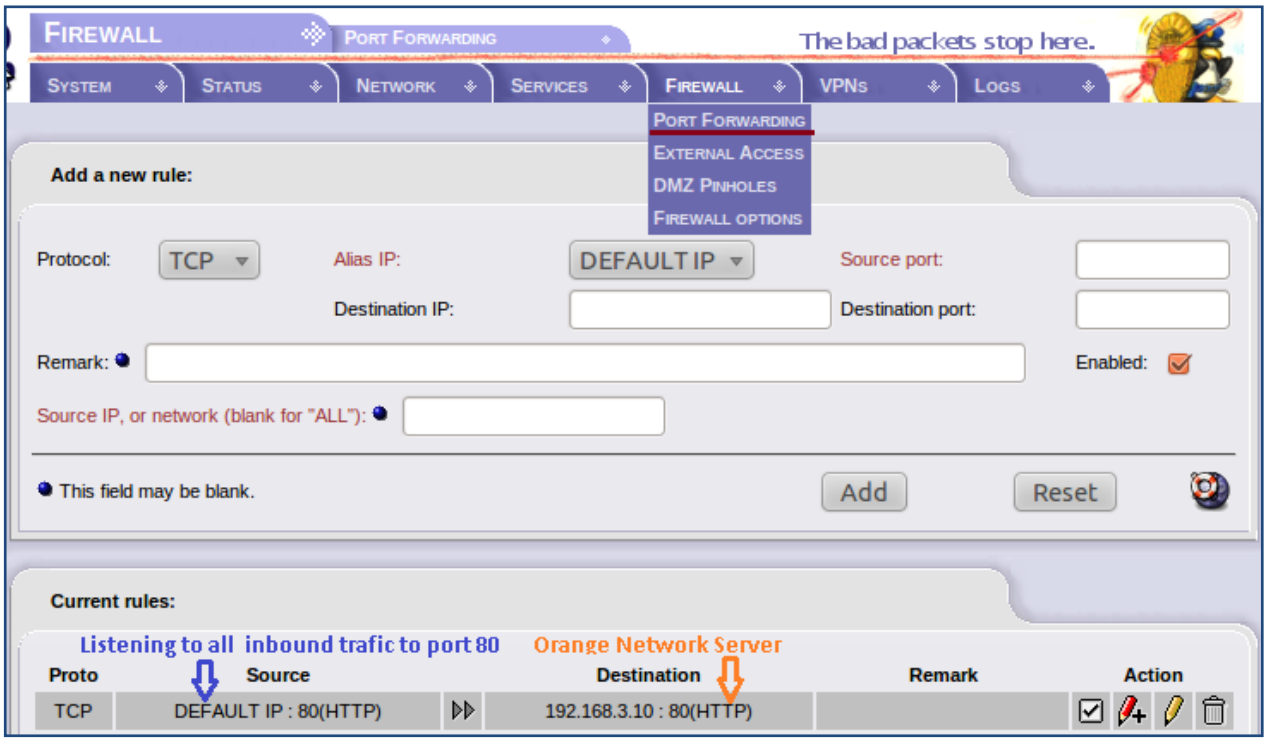
Native Windows Remote Access
Windows intègre des options permettant de connecter en toute sécurité un client à un point de terminaison distant. En tant que technologie d'accès distant ce module peut agir en tant que récepteur pour cette fonction afin que les utilisateurs Windows puissent créer des tunnels rapidement.

Directory Authentication
L'application Directory Authentication s'interface avec des bases de données externes afin de se servir de leurs utilisateurs et de leur groupes dans votre configuration de sécurité. Une façon simple de permettre aux utilisateurs de se connecter à leur accès VPN à l'aide de leurs informations d'identification existantes.

UserPortal
Le portail utilisateur Astaro UserPortal est un concentrateur d'auto-gestion dans lequel les utilisateurs autorisés peuvent utiliser leurs e-mails et des technologies d'accès distant préconfigurées sans requérir l'aide d'un administrateur.

Démonstration online :
http://demo03.astaro.com/

IPCop



v1.4

IPCop est une distribution Linux basée sur Linux From Scratch, faisant office de pare-feu. Elle jouit d'une assez bonne réputation.

Elle vise à fournir un moyen simple mais puissant pour configurer un pare-feu sur une architecture de type PC. Elle peut protéger sur une telle architecture un réseau familial ou de petites ou moyennes entreprises, elle offre la classique Zone démilitarisée (DMZ) ainsi que les tunnels réseau privé virtuel (acronyme VPN en anglais).

IPCop peut également servir de serveur mandataire (proxy), serveur fournissant des adresses IP dynamique (DHCP), de relais DNS, de serveur de temps (NTP), et en installant des greffons ou modules, de bien d'autres choses (contrôle de contenu, liste noire, liste d'accès, DNS dynamique, contrôle de trafic, etc...). Le support des clients sans fil est aussi prévu par le biais d'une zone dédiée.

À l'origine, IPCop était un fork de la distribution Linux « Smoothwall », depuis ces deux projets se sont développés indépendamment, et maintenant divergent de manière importante.

IPCop est sous licence GPL, en open source.

Les images ISO des CD-ROM d'installation (moins de 50Mo en janvier 2007) sont disponibles via un réseau de sites miroirs. Le support est disponible en langue anglaise, française, allemande et hollandaise. L'interface utilisateur d'IPCop est disponible dans 24 langues différentes.

Une machine très bas de gamme permet de le mettre en œuvre, voici un exemple d'une telle configuration :

- 2 interfaces réseau minimum (Ethernet 10/100 ou modem ADSL tout type)
- Microprocesseur à 200Mhz
- Mémoire vive 64Mo
- Disque dur 800Mo
- Lecteur CD-ROM

Optionnellement :

- 2 autres interfaces Ethernet pour la DMZ et le wifi
- Clé USB (installation) et disquette, clé USB (pour la sauvegarde).
- clavier, écran pour l'installation

Cette configuration minimale convient pour une utilisation domestique ou de petites entreprises jusqu'à 5 postes. Elle permet déjà d'utiliser la fonctionnalité de proxy et le système de détection d'intrusion (tous deux gourmand en ressource mémoire et en calcul processeur). Prévoir une configuration plus musclée pour le processeur et la mémoire vive pour une utilisation professionnelle.

IPCop peut fonctionner avec les fonctionnalités de base sur une architecture de type Intel 386 muni de 32Mo de mémoire vive seulement.

IPCOP, dans ses récentes versions, défini 4 ports Ethernets (donc 4 réseaux indépendants) :

- 1 Réseau ROUGE, relié à internet (réseau obligatoire),
- 1 Réseau VERT, relié au réseau local utilisateur, très sécurisé,
- 1 Réseau ORANGE, relié à la D.M.Z. (zone "demilitarized" ou démilitarisée), facultative. Cette zone est reliée, par exemple à des serveurs WEB, à des caméras I.P. ou autre dispositifs Ethernets accessibles (potentiellement !) depuis internet,
- 1 Réseaux BLEU, relié à des dispositifs "Wi-Fi" ou pouvant servir de seconde D.M.Z.

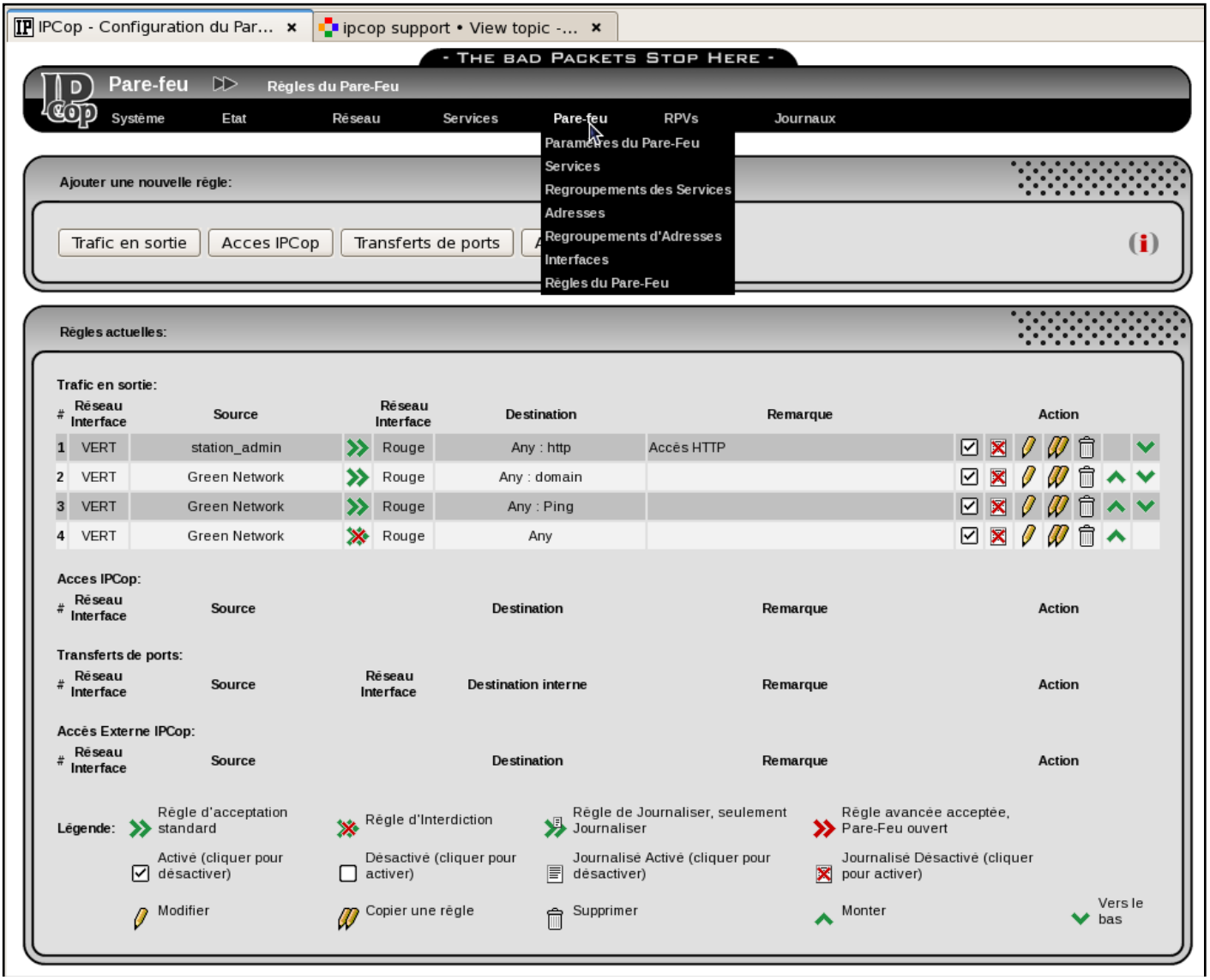
Cette zone est spécialisée par le paramétrage possible de l'adresse MAC ou IP des périphériques autorisés à s'y connecter (selon la configuration de IPCOP, bien sûr).

Le paramétrage général d'IPCOP (réalisé en mode serveur WEB par exemple) permet de gérer les flux autorisés entre ces différentes zones/réseaux, et les exceptions.
L'installation par défaut d'IPCOP fournit un paramétrage standard, bien souvent suffisant et totalement fonctionnel. Il faut noter que les versions initiales d'IPCOP ne géraient que les réseaux ROUGE et VERT.

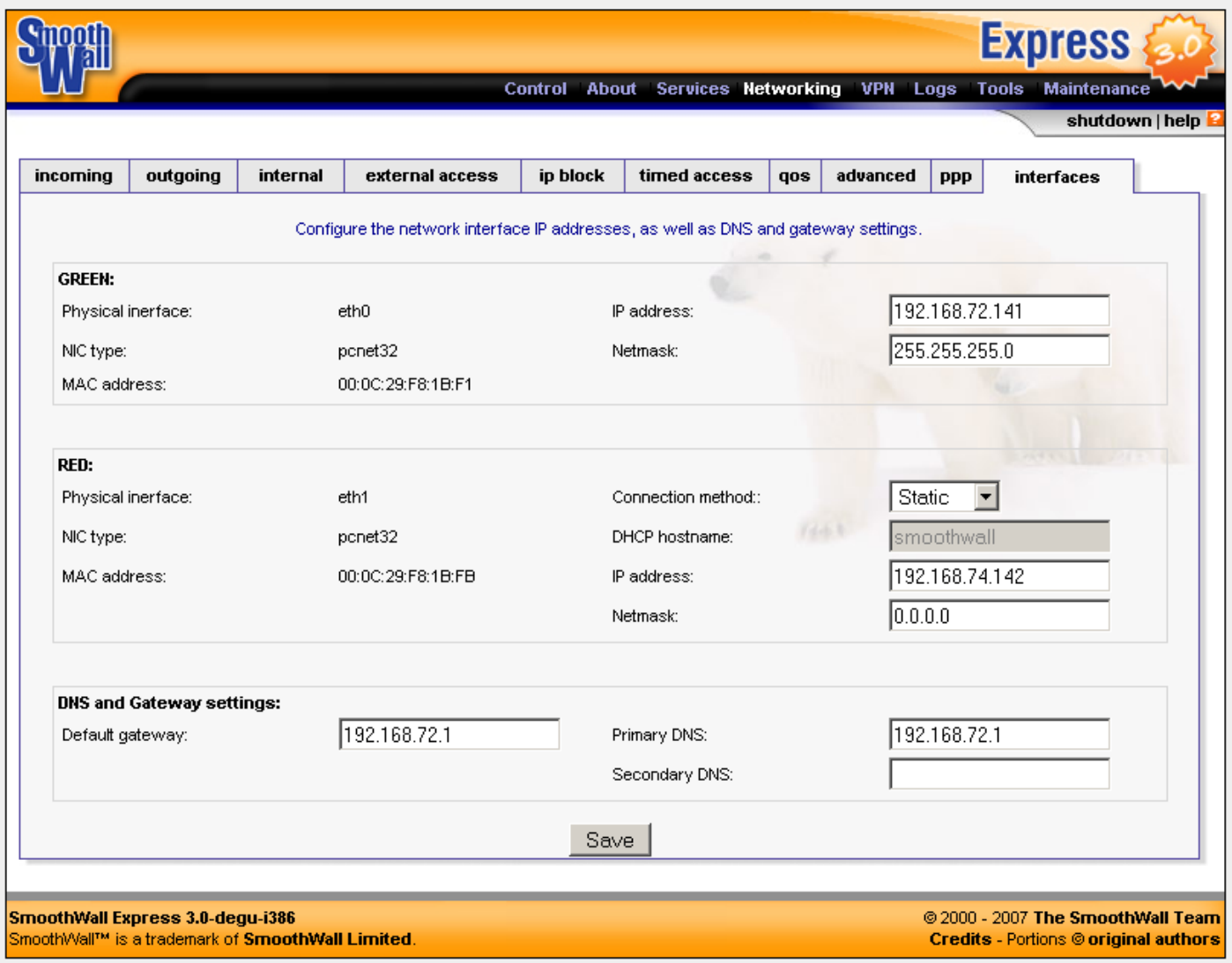
Du fait de la grande communauté qui gravite autour d'IPCOP, cette dernière dispose d'une quantité importante d'add-ons pouvant ajouter des fonctionnalités.
Cependant, tout comme pour les CMS, il est important de comprendre que l'ajout d'add-ons entame sérieusement la stabilité de votre distribution dédiée à la sécurité, parfois sa sécurité.

En sécurité il faut savoir rester sur des briques simples, fiables et robuste qui ne font uniquement ce qu'on leur le demande, mais qui le font bien.

Voici un avant-goût de la future version 2.0 (V1.9 RC1), qui tourne sous Kernel 2.6.X.
Elle n'a plus besoin du module BoT (BlockOutgoingTraffic) car il est natif.


IPCop - Configuration du Par...
ipcop support • View topic -...
- THE BAD PACKETS STOP HERE -
Pare-feu
Règles du Pare-Feu
Système
Etat
Réseau
Services
Pare-feu
RPVs
Journaux
Paramètres du Pare-Feu
Services
Regroupements des Services
Adresses
Regroupements d'Adresses
Interfaces
Règles du Pare-Feu
Ajouter une nouvelle règle:
Trafic en sortie
Acces IPCop
Transferts de ports
Règles actuelles:
Trafic en sortie:
Réseau Interface Source Réseau Interface Destination Remarque Action
1 VERT station_admin Rouge Any : http Accès HTTP
2 VERT Green Network Rouge Any : domain
3 VERT Green Network Rouge Any : Ping
4 VERT Green Network Rouge Any
Acces IPCop:
Réseau Interface Source Destination Remarque Action
Transferts de ports:
Réseau Interface Source Réseau Interface Destination interne Remarque Action
Accès Externe IPCop:
Réseau Interface Source Destination Remarque Action
Légende:
Règle d'acceptation standard
Règle d'Interdiction
Règle de Journaliser, seulement Journaliser
Règle avancée acceptée, Pare-Feu ouvert
Activé (cliquer pour désactiver)
Désactivé (cliquer pour activer)
Journalisé Activé (cliquer pour désactiver)
Journalisé Désactivé (cliquer pour activer)
Modifier
Copier une règle
Supprimer
Monter
Vers le bas

SmoothWall



SmoothWall est un pare-feu distribué sous licence GNU/GPL, avec son code source.
Cette distribution permet via une interface web de gérer à distance (en https) :

- Les règles de filtrage,
- les fichiers de log,
- le NAT,
- le DNS,
- le Proxy,
- les VPN,
- SSH,
- etc.

Il existe aussi une version commerciale professionnelle de SmoothWall, avec plus d'options et un support professionnel, disponible auprès de SmoothWall Ltd.

A noter : lors de sa première connexion, ce firewall enverra quelques informations non-personnelles comme le processeur utilisé, la taille de la RAM, la date et l'heure, la version de SmoothWall installée sur votre système aux auteurs. Les auteurs précisent que ce n'est pas un Spyware.

SmoothWall est gérable à distance, donc, une fois installé, il n'y a vraiment besoin que d'un PC, sans écran, sans souris, sans clavier...

SmoothWall supporte les cartes réseaux les plus courantes (3com, Realtek, NE 2000...) et les modes de connexion internet les plus courants (Modem, ISDN, ADSL, USB ADSL, Ethernet).

Note : une liste des cartes réseaux supportées (fichiers avec extensions .o) est disponible dans le fichier lib.tar.gz du cd-rom SmoothWall (il faut connaître le chipset équipant votre carte réseau : rlt8139.o est présent dans l'archive lib.tar.gz et indique que les cartes équipées d'un chipset Realtek 8139 sont supportées).

Il est possible de définir trois zones réseaux différentes :

- verte (Zone totalement sûre : votre réseau local),
- orange (Zone partiellement sûre : DMZ, De-Militarised Zone, c'est sur cette branche du réseau que sera branché votre serveur HTTP par exemple)
- rouge (Internet et ses pirates...).

Ceci veut dire que vous pouvez avoir jusqu'à trois cartes réseaux sur votre Firewall : une verte sur laquelle seront reliés votre réseau local et votre serveur local de fichier par exemple, une orange sur laquelle sera relié votre serveur web Apache, rouge sur laquelle sera relié votre modem Ethernet ADSL par exemple...

La configuration requise est vraiment minimale :

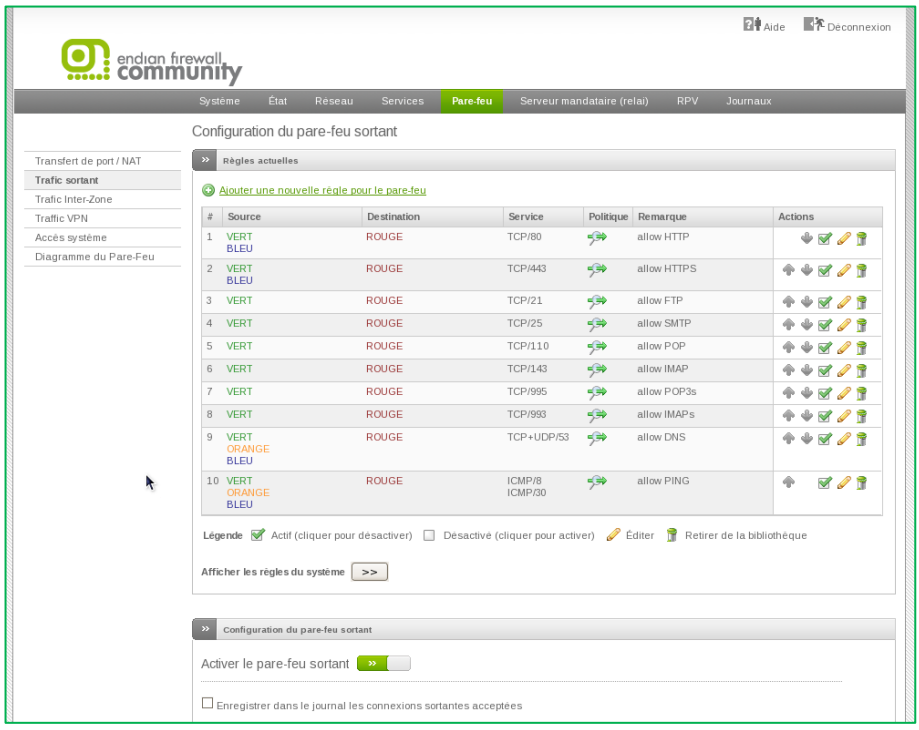
- Processeur 486DX4,
- 16 Mo de RAM,
- Disque dur de 200 Mo (SmoothWall n'occupe qu'environ 60 Mo),
- Carte réseau 10 Mb.

Ceci est le minimum pour faire fonctionner une connexion par Modem. Pour une configuration multi-utilisateurs (partage de connexion) et l'ADSL, il faudra étoffer un peu cette configuration...

Enfin, SmoothWall est basé sur un noyau Linux 2.2.19, et sa mascotte est un ours polaire du nom de Smoothie...

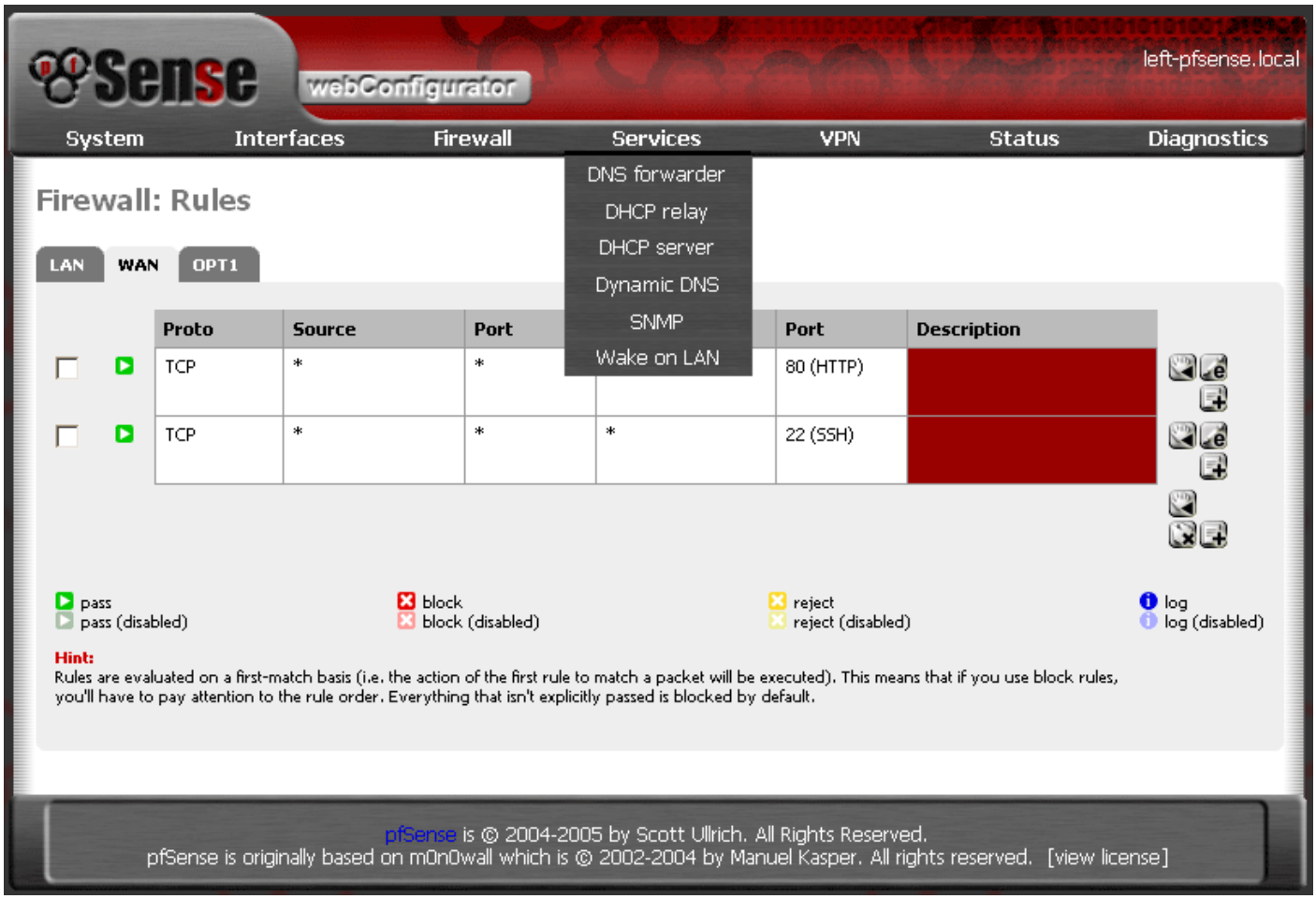
Et aussi :

- ***Endian UTM software Appliance,***
- OpenWall,
- Altimate gbmh NET,
- Etc.



Distribution basées sur BSD ou dérivée :

Pfsense/m0n0Wall



PfSense est une distribution libre, open source, **dérivée d'une version personnalisée de FreeBSD** qui a été adaptée pour une utilisation en tant que pare-feu et routeur.

En plus d'être un puissant pare-feu et une plate-forme flexible de routage, elle comprend une longue liste de fonctionnalités connexes et un système de modules permettant une évolutivité supplémentaires.

PfSense est un projet populaire avec plus de 1 million de téléchargements depuis son lancement. Cette distribution a été éprouvée dans d'innombrables installations allant de petits réseaux domestiques, la protection d'un PC, une Xbox, à de grandes sociétés, universités et autres organisations. Elle peut protéger des centaines de périphériques en réseau.

Ce projet a débuté en 2004 comme un fork du projet « m0n0wall ». Cette distribution est restée axée vers des installations type PC complet plutôt que sur des matériels embarqués (vs m0n0Wall).

PfSense offre également une image compacte pour les installations de base sur carte compact flash, cependant ce n'est pas son objectif principal.

OpenBSD

Avec une installation par défaut, sans démarrer le moindre service supplémentaire, cette distribution type BSD, un peu spéciale, n'est certes pas dédié à la sécurité mais par bien de ses comportements s'en rapproche.
Si vous vous contentez d'une installation de base sans ajouter ou démarrer de services réseau supplémentaires vous êtes en présence d'un système déjà bien sécurisé.
C'est pour cela que cette distribution un peu particulière, car orientée sécurité, ne figure pas avec les distributions à monter soi-même : elle a été créée dans l'optique de la sécurité.

Nous venons de voir quelques distributions dédiées à la sécurité.
En cas

Leurs principaux avantages sont :

- Leur compacité,
- Le niveau de sécurité proposé après installation sans modification profonde,
- Le savoir-faire des équipes l'ayant développé,
- La vitesse de déploiements,
- La facilité de mise à jour donc de maintenance.

Exercice TP N°2

⇨ Installation et paramétrage d'un pare-feu issue d'une distribution dédiée sécurité.

IPCop, Astaro ou Endian SoftwareUTM (Community)

Voir annexe.

La sagesse : les pare-feu matériels

Précédemment nous avons vu les pare-feu mis en œuvre à partir de distributions dédiées sécurité cependant il ne faut pas se leurrer ces dernières ne proposent pas toutes les fonctionnalités des pare-feu matériel qui eux bénéficient de moyens colossaux pour leur développement. Sans parler de l'expérience que certaines sociétés spécialisées dans la sécurité informatique, présentes depuis plus de 15 ans dans ce secteur d'activité, ont pu acquérir.
Bien évidement toute cette expérience se retrouvent concentrée dans « l'Appliance » qui est dédié à la sécurité.

Il en va de même pour le choix des composants électroniques qui constituent le pare-feu matériel.
Dans les cas étudiés précédemment ce sera une carte mère générique (processeurs non dédiés, ventilateurs, composants inutiles etc.) qui sera utilisée dans l'autre cas la carte mère sera pourvue d'ASIC (*Application-Specific Integrated Circuit*) dédié à la sécurité (chiffrement hardware etc.), de multiples optimisations matérielle (vitesse de démarrage), mise à jour par flashage du firmware etc. : la liste des avantages est très longues.

Vous l'aurez compris en milieu professionnel, et parce que nous sommes des professionnels, le pare-feu matériel est devenu incontournable, d'autant plus que le prix s'est littéralement effondré.
Un pare-feu matériel d'entrée de gamme avec filtrage de flux,IDS etc. revient à moins de 500 euros HT…
(Le prix d'un ordinateur de milieu de gamme !)

Parmi les pare-feu matériel on trouve 3 classes de produit (attention on ne parle pas du niveau de sécurité) :

- Les pare-feu à usage familiale,
- Les pare-feu SOHO (Small Office Home Office) plutôt pour les usages TPE et PME,
- Les pare-feu pour grand compte (voir grosses PME) pour protéger de grand réseaux, dense en utilisateurs, et parfois nécessitant de la haute disponibilité. Ici la majorité sont livrés au format rack 19''.

@Home : Basique

Ces pare-feu disposent des fonctionnalités de base pour :

- Le filtrage de paquets à état (SPI),
- La protection contre quelques attaques basiques (DoS, stack IP),
- Les services réseaux non évolués (DHCP, filtrage URL basique, NAT, journalisation, etc.)

Examinons la plaquette commerciale d'un de ces pare-feu :

- Switch 4 ports 10/100 intégrés
- Routeur compatible avec les offres ADSL 2+Support PPPoE/NAT/PAT
- Redirection de ports statiques (Port forwarding)
- Redirection de ports dynamiques (Port Triggering)
- Serveur DHCP (253 utilisateurs)
- Accès au Web contrôlé (heures de connexion, filtre d'URL par mots clés)
- Véritable Firewall avec SPI (Stateful packet Inspection), contrôle d'intrusion, DoS (Denial of Services), remontée d'alertes
- Configuration via agent WEB (demo ici : http://interface.netgear-forum.com/RP614v3/)
- Support VPN Pass Through
- Support UPnP

Premièrement on s'aperçoit que l'usage est clairement étudié pour les particuliers. Ici on ne parle pas de VLAN, 802.1x, Multizone, Gestion de bande passante avancée, politique de sécurité : tout peut sortir sans restriction, etc.

Et comme vous pouvez le constater ce genre de pare-feu propose en gros les mêmes caractéristiques, voire moins, qu'une distribution dédiée sécurité sans l'évolutivité et l'absence quasi systématique d'add-ons.
Ils présentent néanmoins l'avantage d'être très compacts et surtout très facilement maintenables par le commun des mortels.

Ce ne sont pas des pare-feu professionnel, ils sont donc à éviter en production car très vite ils montreront leur limites.

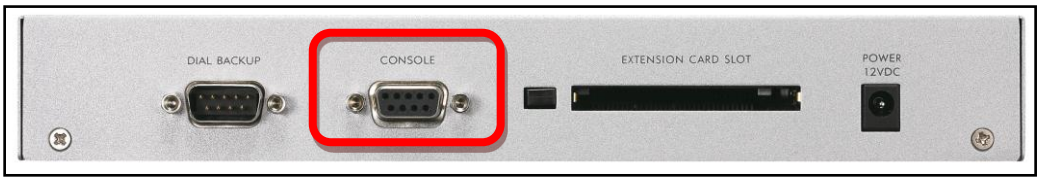
De plus ces pare-feu tendent à disparaître car les Box des fournisseurs d'accès Internet proposent à peu de chose près les mêmes fonctionnalités sans le moindre surcoût car fournies de base avec les offres haut débit.

@Office

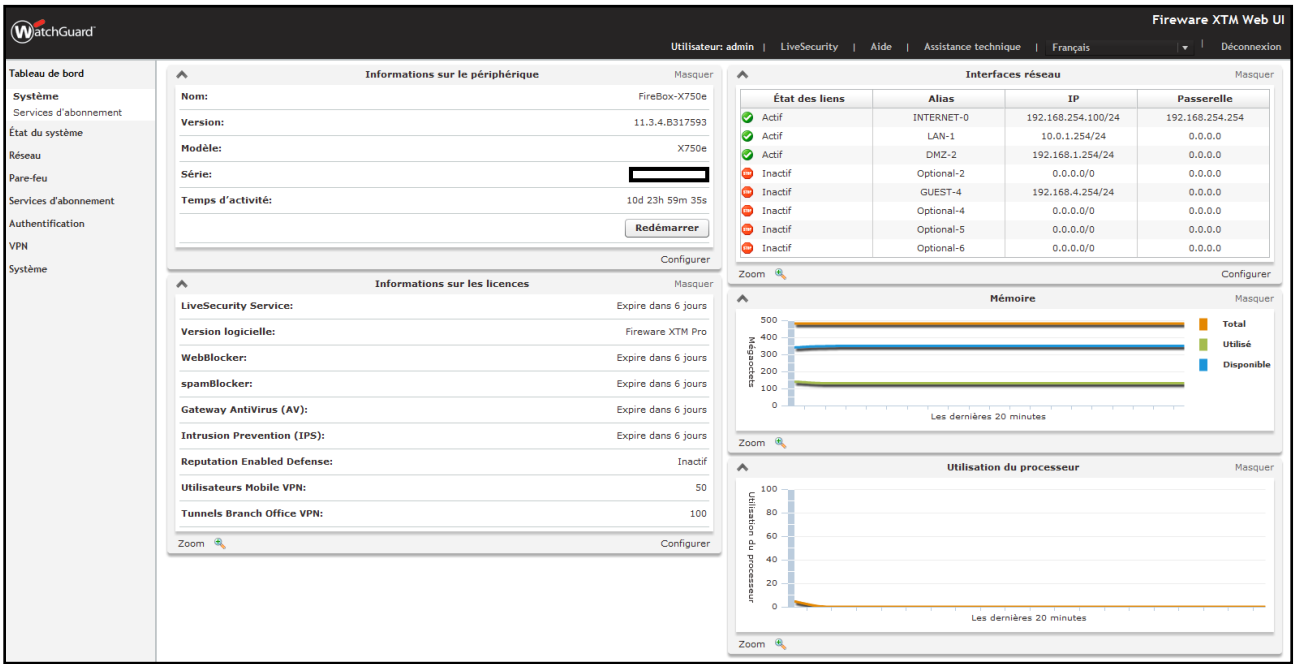
Maintenant attaquons nous au pare-feu matériel dit « SOHO ».
Ce sont des pare-feu étudiés pour les TPE et PME mais également pour les bureaux à la maison (Home Office) des télétravailleurs.
Ce sont de véritables pare-feu professionnels pourvus de l'ensemble des fonctionnalités d'un UTM.

Tout d'abord il faut savoir que ce type de pare-feu peut se gérer, généralement, de trois manières différentes :

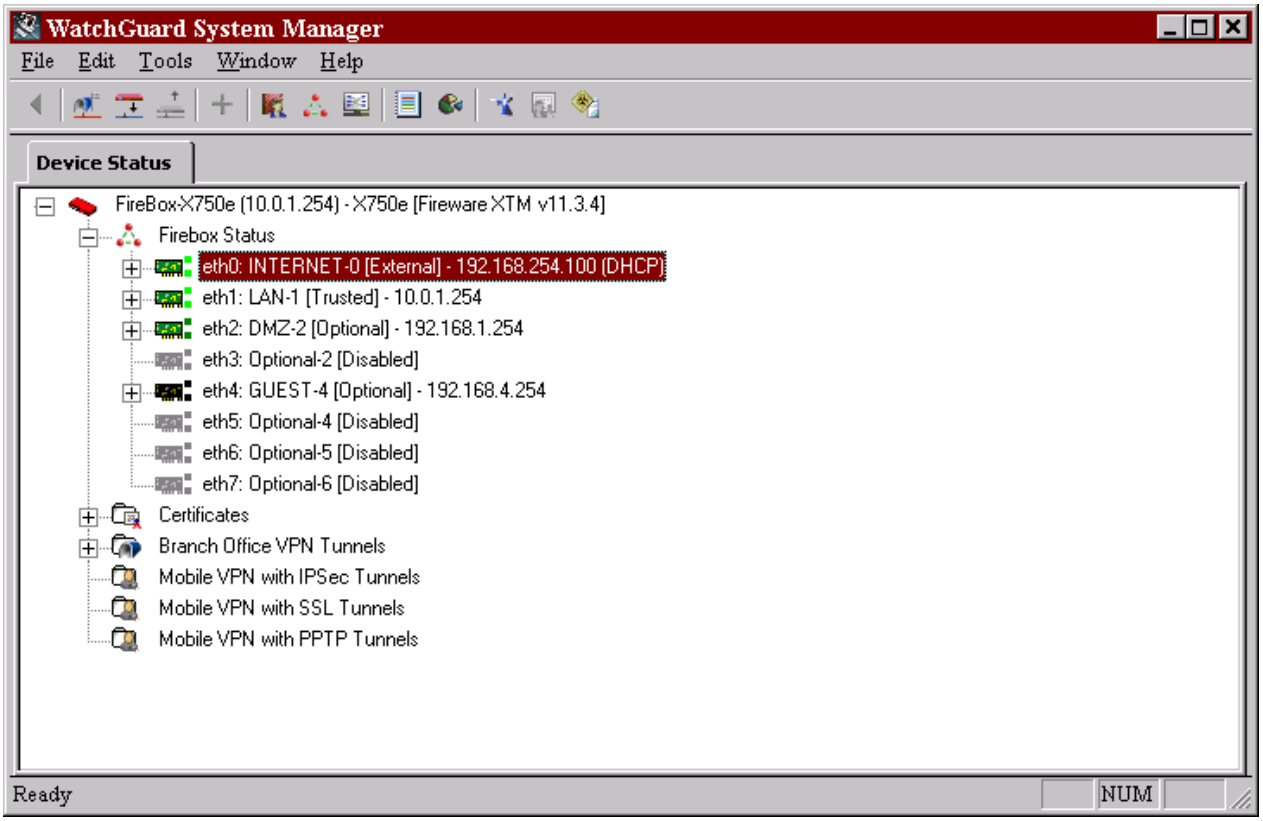
- Via un **port console (RS232) en ligne de commande** en vous servant d'un outil type HyperTerminal, vous accéder directement à la gestion de votre pare-feu tout comme un routeur/switch :



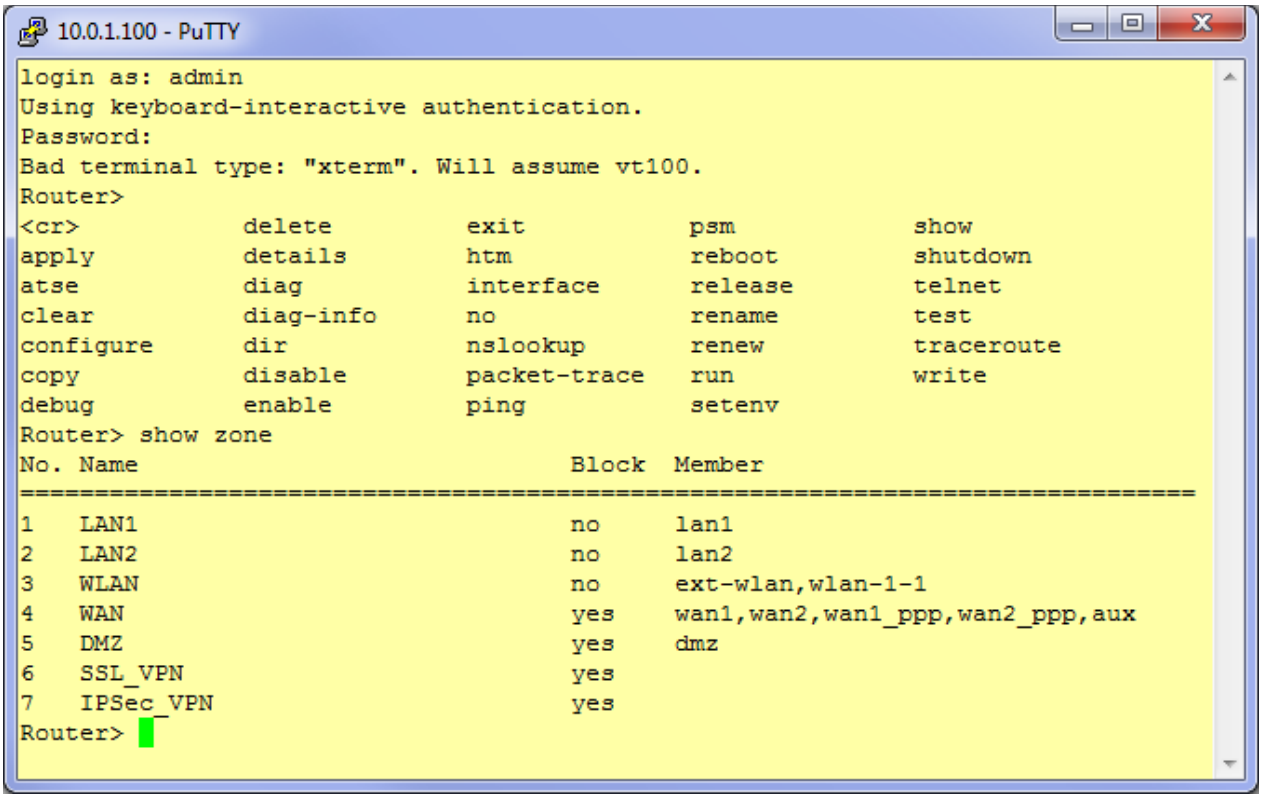
- Via **une interface Web** (le plus courant car se basant sur des technologies open Source non soumises aux licences et aux coûts de développement moins élevés) :



- Via une **interface** développée pour telle ou telle **plateforme cible (**ci-dessous « win32 »)



- Via un **accès SSH** en ligne de commande :



La société Zyxel (constructeur Coréen) propose ce genre de pare-feu. La majorité de sa gamme est d'ailleurs étudiée pour les TPE, PME ou les télétravailleurs. Notez qu'il existe une multitude de marques proposant des produits similaires.

Décortiquons l'interface de ce genre de pare-feu.

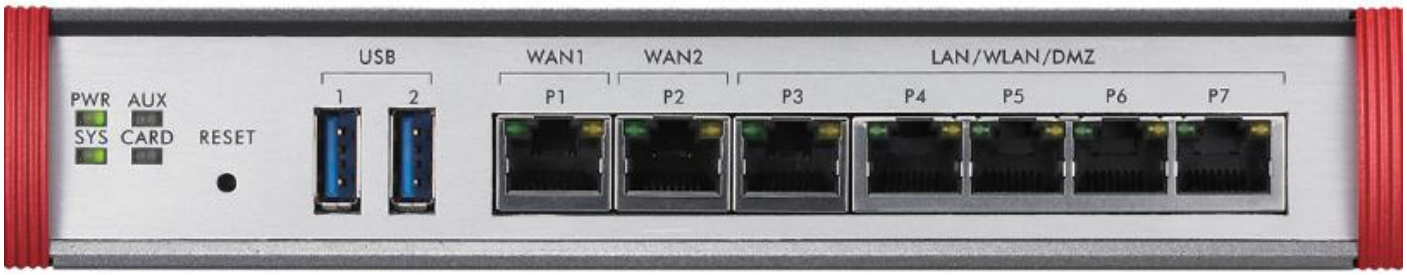
Prenons l'exemple du ***ZyWall USG 100, UTM milieu de gamme***.

> **Note** : La plupart des pare-feu fonctionnent de la même manière que celui-ci, cet exemple pourra largement vous servir pour appréhender d'autres modèles ou marques de pare-feu sans le moindre souci.

Ce pare-feu se présente dans un boitier dépourvu de toutes connexions clavier ou souris, inutile de vouloir raccorder un écran : il n'est pas fait pour cela. Cela permet de la protéger de tout accès physique non autorisé.

Une compromission physique (vol, accès, arrêt du pare-feu etc.) du boitier aurait juste pour conséquence d'alerter, de par le non fonctionnement des accès au réseau, les administrateurs du site et serait également sans conséquence pour les données chiffrées à l'intérieur du boitier.
En effet seul un bouton discret de remise à zéro est présent, un « reset hardware » rétablie uniquement les paramètres d'usine : donc très peu de chance de dérober discrètement les mots de passe ou d'altérer la politique de sécurité en place.

Etudions la façade avant du produit.



Nous pouvons voir :

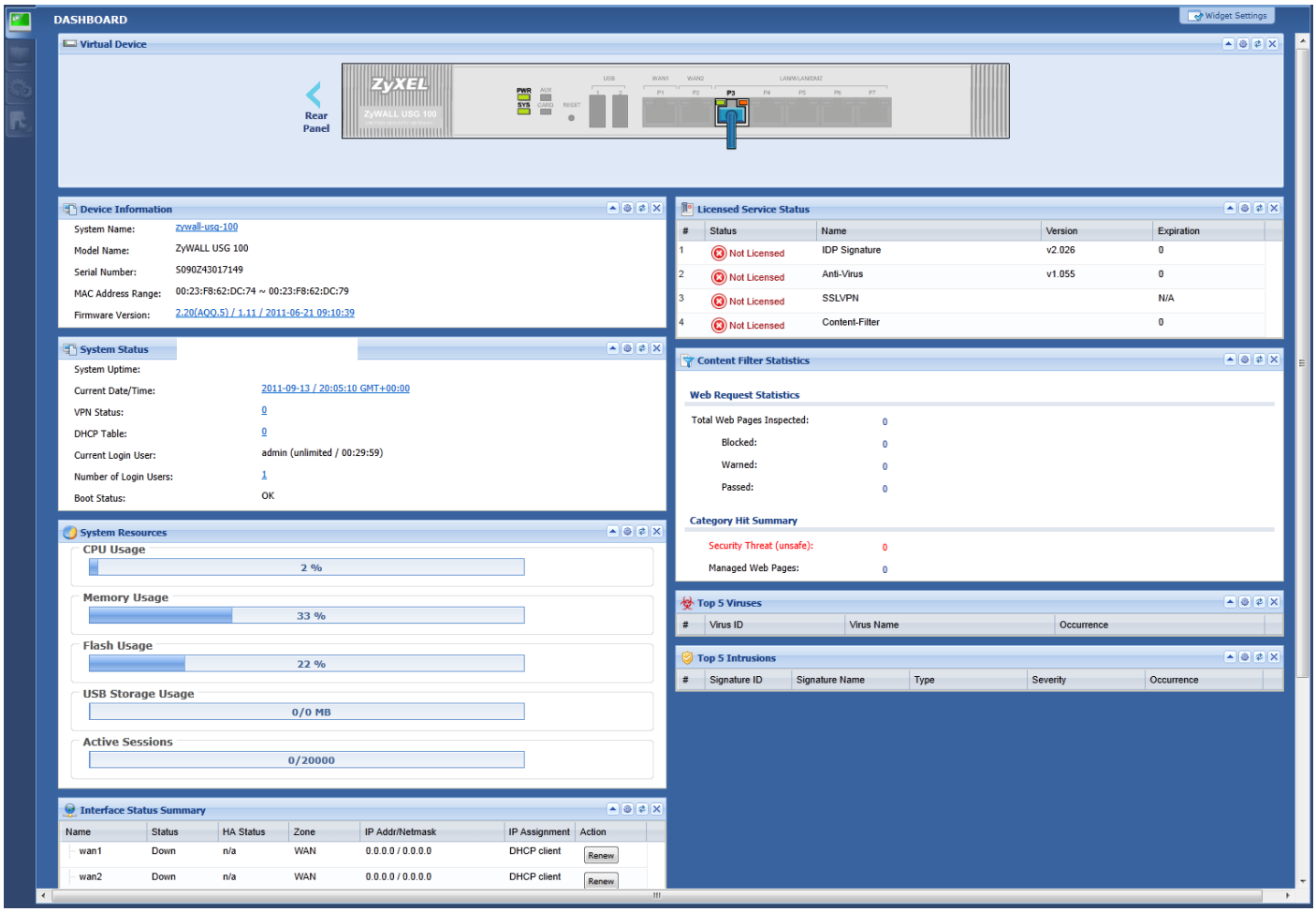
- Les voyants d'états du pare-feu,
- Les connecteurs USB pour stocker des journaux, firmware, configurations, paramétrer le pare-feu en un clic ou installer des clefs de connexion 3G pour la haute disponibilité en cas de panne du réseau filaire (ADSL etc.).
- Les ports RJ45 (Gigabit) dédiés par zones de sécurité ou assignables :
    - P1 et P2 : ports WAN (avec possibilité d'agrégats de bande passante),
    - P3 à P7 : ports assignables à la demande à des DMZ, LAN ou WLAN.

Bref c'est assez complet, modulaire et légèrement évolutif.

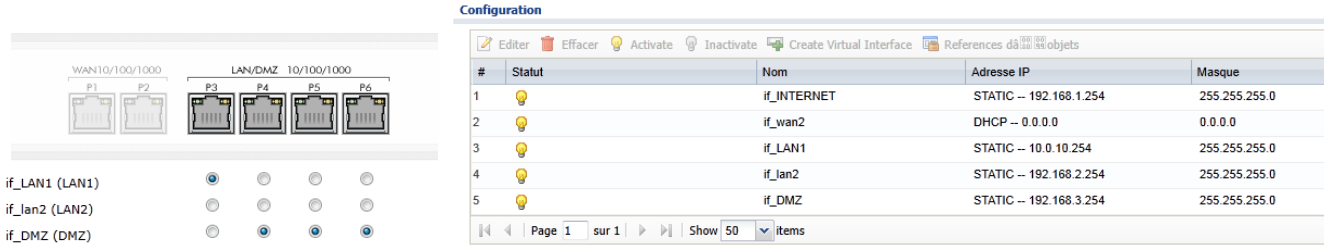
Nous allons maintenant gérer cet « Appliance » via son interface Web, seul un navigateur suffit pour gérer la totalité des fonctionnalités du pare-feu.

Une fois connecté vous avez sur un seul et même écran un certain nombre d'informations critiques (avec affichage paramètrable) :

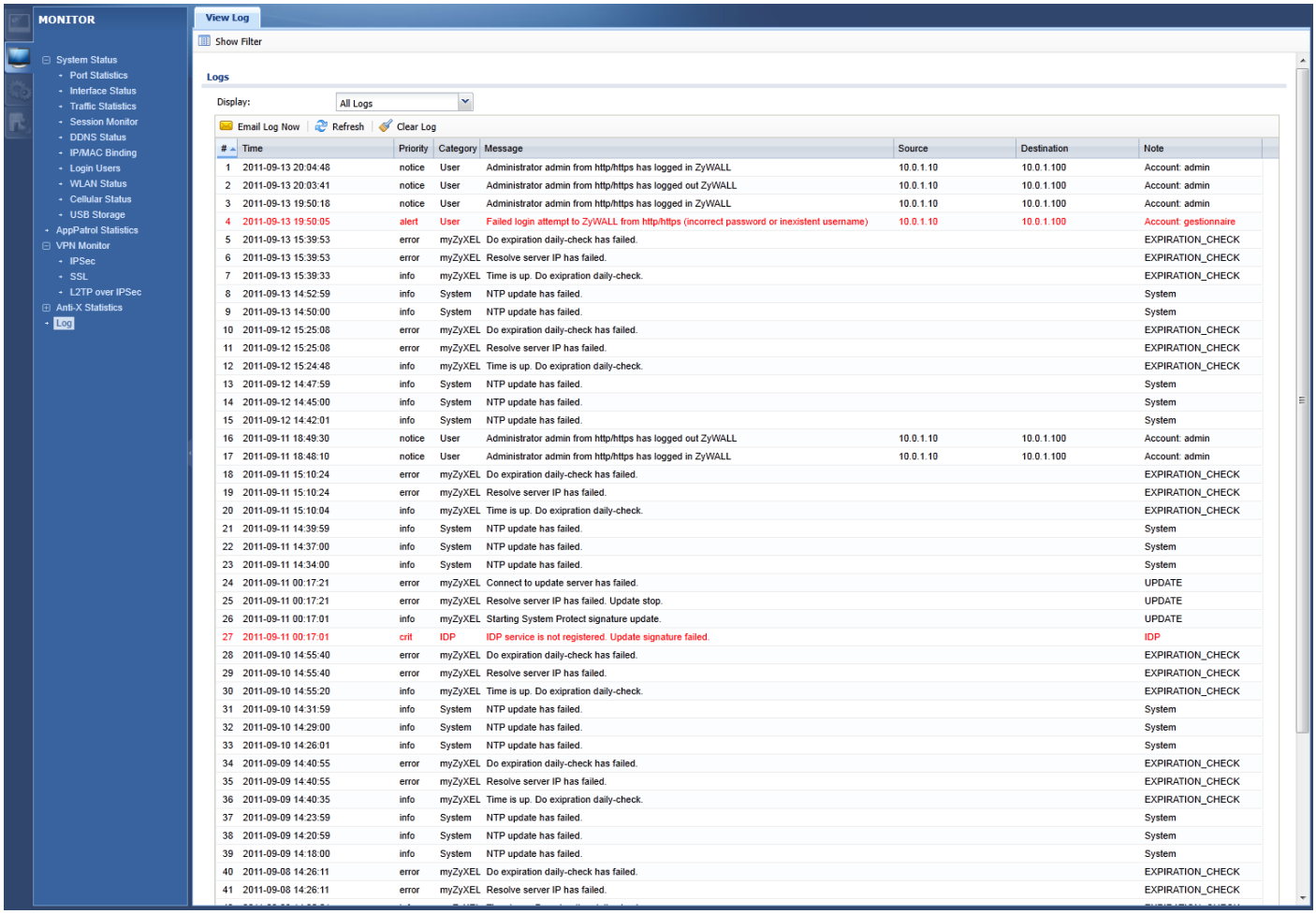
- Informations sur le pare-feu (nom, modèle, numéro de série, MAC addresse, Firmware),
- Versions des moteurs de filtrage de flux, de détéction d'intrusion, de tunnel SSL VPN et d'antivirus,
- L'état du pare-feu (uptime, date,VPN montés, tables DHCP, utilisateurs connectés),
- Les statistiques et états du filtrage des flux, de l'anti-virus, des intrusions,
- L'utilisation des ressources (CPU, mémoire, stockage flash, usb, sessions actives),
- La configuration des interfaces réseaux.



Ensuite vous pouvez placer chaque port physique dans une zone de sécurité :

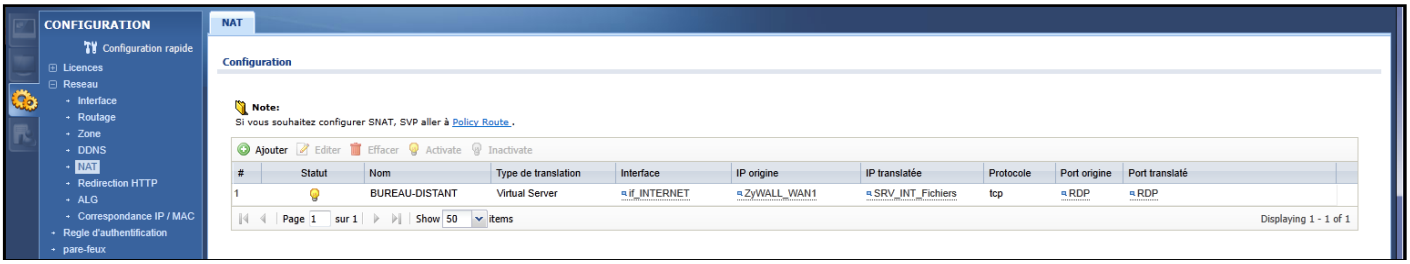


Voici un aperçu de ce qu'on peut apercevoir dans le module de journalisation :



Il y a là l'essentiel pour analyser un disfonctionnement ou encore un accès suspect. La journalisation est un élément crucial pour un pare-feu il est donc fortement conseillé de rediriger vos journaux vers un serveur « CEF/VRPT/syslog » sécurisé.

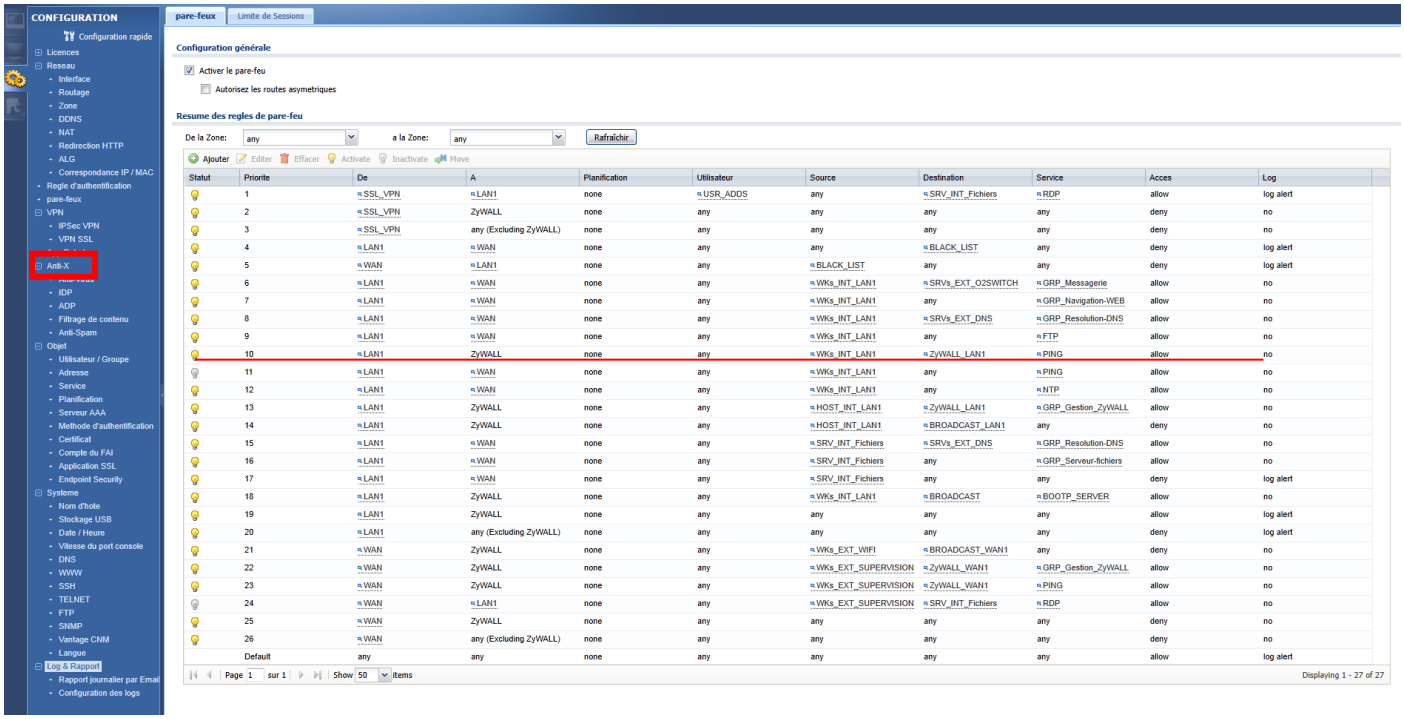
Vous pouvez également configurer plusieurs types de NAT avec tous types de translations (ports, adresses)



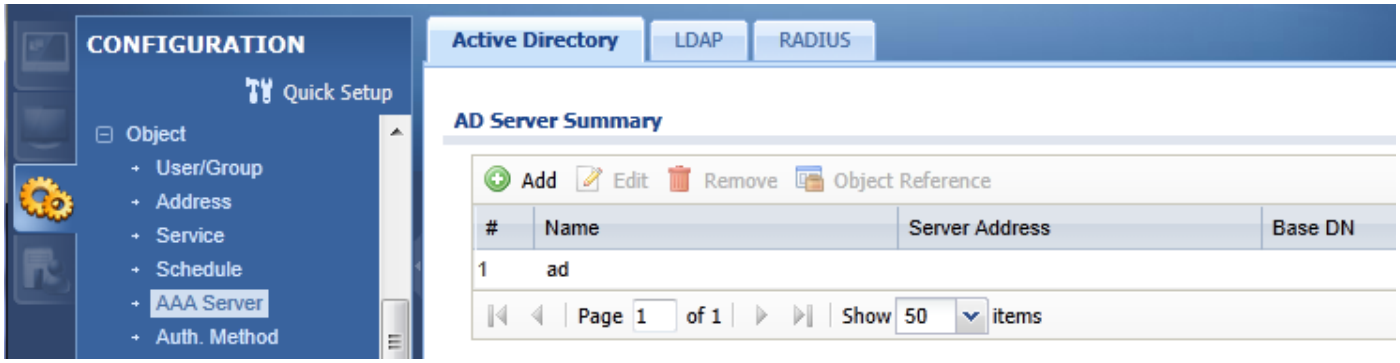
Enfin ci-dessous le module crucial d'un pare-feu : les règles de filtrage.
C'est ici que vous allez mettre en place votre politique de sécurité.

Vous pouvez constater que ces dernières sont gérées par zone (LAN1, LAN2, WAN, DMZ, etc.).
Il est possible d'appliquer une planification pour l'activation ou désactivation de votre règle.

Enfin on retrouve les traditionnels champs source, destination, service, accès (autorisé ou non) et journalisation.



Ces règles peuvent être soumises à des contraintes authentification cela permet de n'autoriser un accès qu'à certaines personnes s'étant correctement authentifié via un serveur RADIUS, LDAP, AD etc.



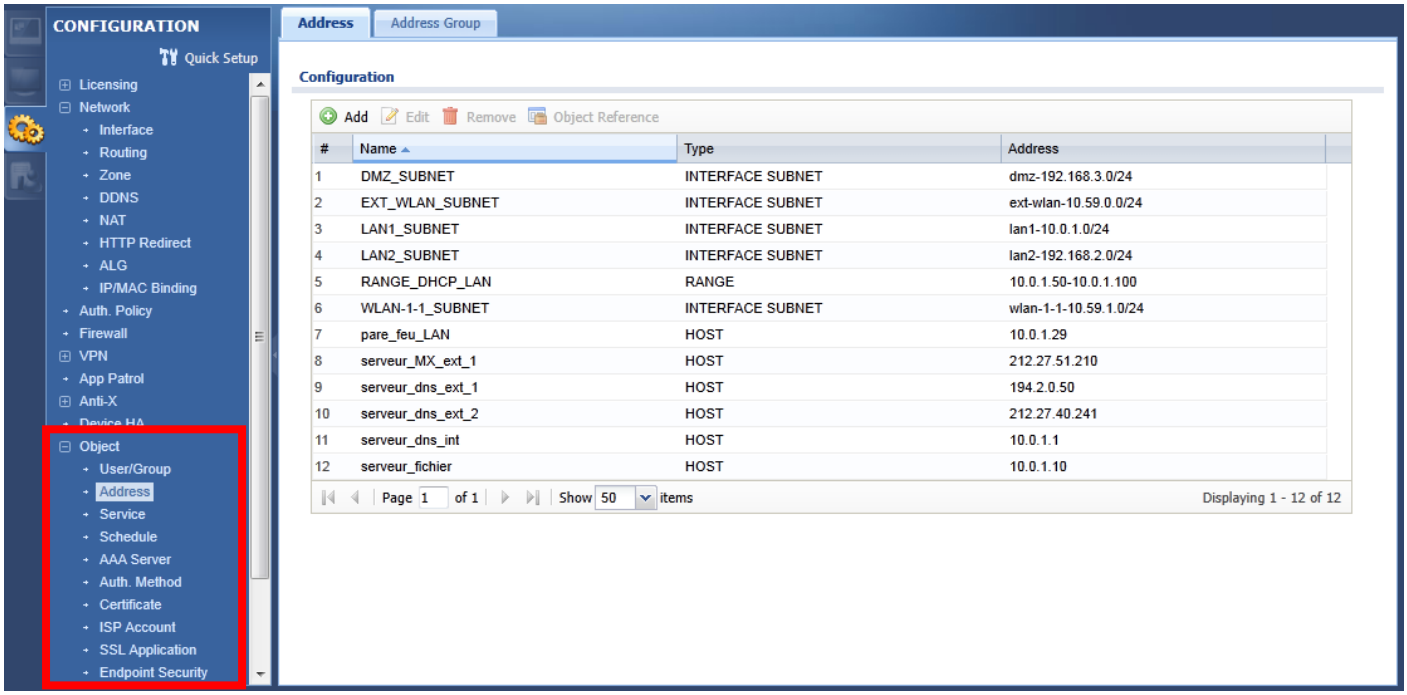
Sur la capture écran ci-dessous il est intéressant de voir que ce genre pare-feu se gère via des objets et regroupement de ces derniers : on gagne ainsi en flexibilité.

La modification via des objets permet de régler un ensemble impressionnant de paramètres en un clic de souris.

En fait si vous avez correctement mené votre étude de l'existant vous devez être en possession de la cartographie réseau, des éléments le constituant et des flux connus transitant dans votre organisation. Cela sera facilement modélisable grâce au modèle objet de votre pare-feu, à savoir :

- Les Utilisateurs (acteurs) ➔ « User/Group »,
- Les hôtes (serveurs, éléments actifs, stations de travails, commutateurs, plages réseaux, sous-réseaux, etc.) ➔ « Address »,
- Les flux gérés (protocoles) ➔ « Service »,
- Serveurs et méthodes d'authentification (RADIUS, LDAP, AD) ➔ « AAA Server »,
- Etc.

Ici la modélisation de quelques adresses des éléments du réseau :



Enfin voici un résumé des possibilités de ce type de pare-feu (discussion)

En fait nous venons de voir les fonctionnalités basiques de ce genre de pare-feu UTM. L'énumération et le paramétrage de toutes prendrait bien plus d'une journée.
Il faut savoir que les réglages concernant les filtrages de flux, antivirale, IDS sont beaucoup plus pointus que la partie filtrage des paquets. A eux seuls ces modules feraient l'objet d'un cours séparé.

Vous pouvez déjà vous rendre compte des possibilités proposées par un produit milieu de gamme en comparaison d'un GNU/Linux « from scratch » ou d'une distribution dédiées sécurité. Ce n'est pas vraiment le même monde.
D'autant plus que l'intelligence interne (durcissement de la pile IP, contre-mesures aux DoS, etc.) du pare-feu n'est pas dévoilée par le fabricant, par soucis de protection du savoir-faire. Et là, le niveau de connaissance pour arriver à un tel niveau de sécurisation de l'OS du pare-feu n'est vraiment pas à la portée de toutes les têtes, on dira plutôt qu'il est réservé à une certaine élite.

Maintenant intéressons-nous à des modèles haut de gamme.

Grandes comptes

La grosse différence avec un pare-feu UTM matériel milieu de gamme (SOHO) va essentiellement se jouer sur :

- Le débit de filtrage (mode VPN, Filtrage de Flux) : en gros la puissance de l'ASIC responsable du chiffrage et du bus système qui relie les ports réseau,
- La présence de module haute disponibilité et d'équilibrage de charge (HA, Cluster etc.)
- Les modules de supervisions très poussés : à ce niveau on travaille en temps réels sur des centaines de milliers de sessions, avec alertes sur des comportements anormaux du réseau etc.,
- La gestion de plusieurs « Appliance » répartis sur de très grands réseaux,
- L'interopérabilité avec d'autres briques sécurités (sonde IDS, chiffreur SSL-VPN etc.),
- Les abonnements et garanties souscrits en longue durée (pour la mise à jour des modules).

Voici quelques-uns des acteurs du marché qui proposent des UTM pour grands comptes :

- WatchGuard (Gamme XTM, constructeur Américain),
- Netasq,
- Baracuda,
- Fortinet,
- NetScreen,
- Cisco,
- Etc.

Pour étayer cet état de fait il suffit de regarder les plaquettes des constructeurs pour s'apercevoir que certaines sociétés proposent des boitiers upgradable et modulaire à souhait.
Si vous achetez l'Appliance de base, vous pourrez toujours augmenter sa puissance de traitement via mise à jour logiciel (firmware) ; le constructeur ayant choisi le même hardware pour tous les modèles de sa gamme de produits

Exemple :

> Chez WatchGuard pour la série XTM 8 : vous pourrez passer du modèle XTM 810 au 830 sans changement de matériel.

WatchGuard® Model	WatchGuard® XTM 810	WatchGuard® XTM 820	WatchGuard® XTM 830
Ideal For	Main offices/headquarters that need strong security and a solution that offers room for growth.	Main offices/headquarters looking for fast throughput and strong security that grows with changing needs.	Main offices/headquarters that need enterprise-grade performance & security
Hardware			
Model Upgradeable	✔	✔	N/A
Interfaces	10: 10/100/1000	10: 10/100/1000	10: 10/100/1000
DMZs	8	8	8
Security			
Application Proxies	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3, SIP, H.323, TFTP	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3, SIP, H.323, TFTP	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3, SIP, H.323, TFTP
Intrusion Prevention (DOS, DDOS, PAD, port scanning, spoofing attacks, address space probes, and more)	✔	✔	✔
Wireless Models Only	N/A	N/A	N/A
User Authentication with transparent Windows authentication	✔	✔	✔
Performance			
Firewall Throughput**	3 Gbps	4 Gbps	5 Gbps
VPN Throughput**	1 Gbps	1.4 Gbps	1.7 Gbps
XTM Throughput**	1 Gbps	1.3 Gbps	1.6 Gbps
Concurrent Sessions* (bi-directional)	500,000	750,000	1,000,000

Nous allons survoler en images les modules clef de ce genre de solution.

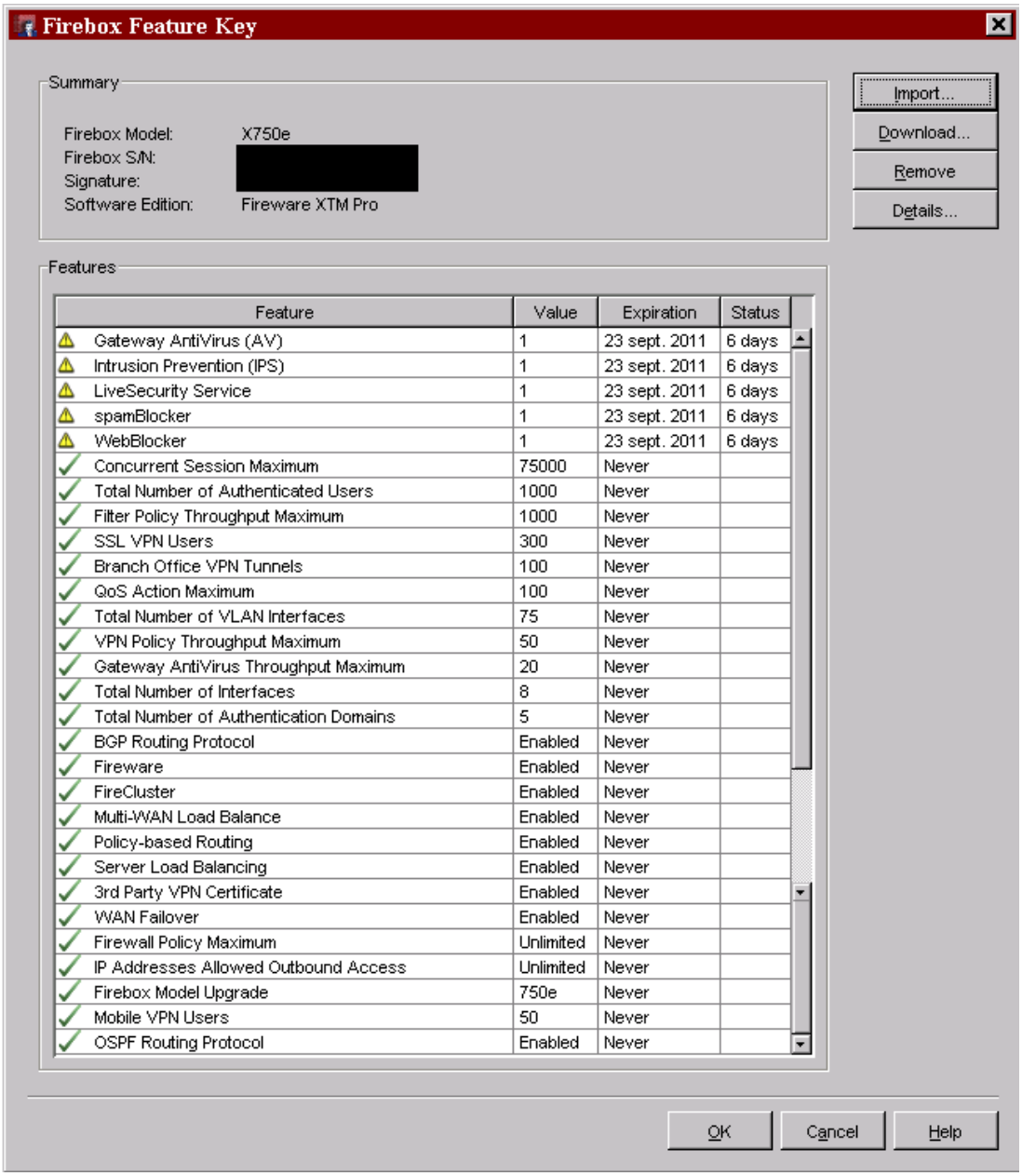
Attardons-nous sur le WatchGuard x750e.
Il s'agit d'un modèle remplacé par les XTM séries 8 mais sa mise en œuvre est un condensé des « Best Practices ».

Tout d'abord l'intégration physique avec un châssis rackable, dépourvu de connexions clavier, souris, etc.
Ce pare-feu propose juste un écran LCD permettant d'afficher :

- L'état matériel du pare-feu,
- Les paramètres réseaux de base des 8 interfaces,
- La charge CPU et mémoire,
- La version du firmware en place,
- Enfin l'uptime.

Ainsi que les traditionnels : ports console (RS232), ports RJ45 Gigabits, 4 boutons pour la navigation dans les menus d'affichage du LCD précédent et rien de plus !
Bref, comme précédemment, rien qui permettre de compromettre sérieusement le pare-feu.

Voici un aperçu des modules disponibles dans ce type de pare-feu matériel:



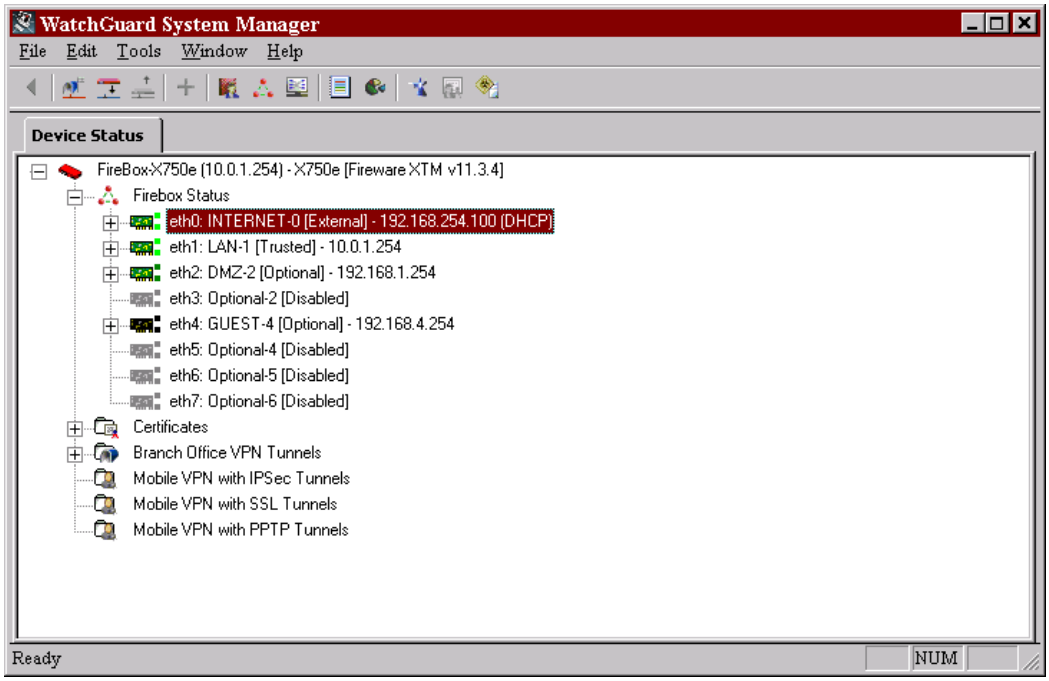
Certains de ces modules sont optionnels et payants d'autres sont fournis de base sans souscription supplémentaire.

Sur le WatchGuard x750e on les distingue grâce à la date d'expiration de souscription : passé ce délai il faudra renouveler votre abonnement au service désiré.

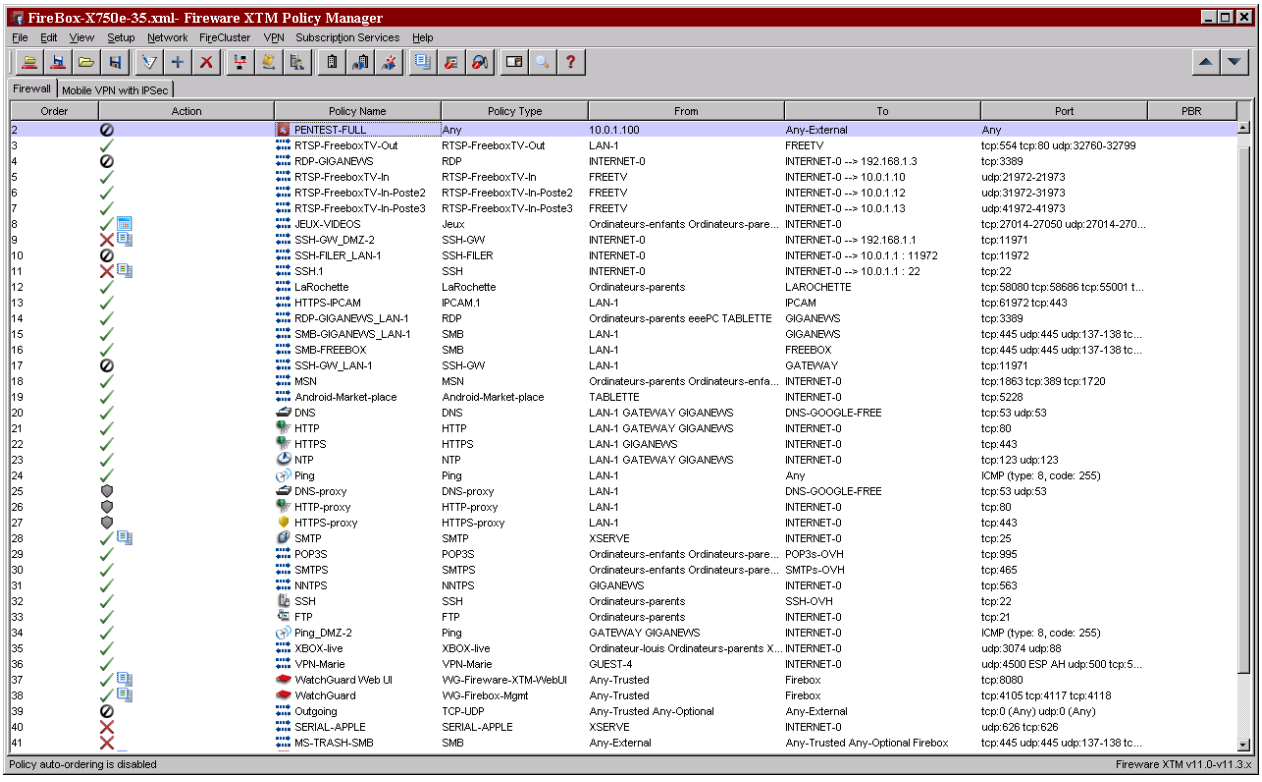
Ici on constate que le pare-feu propose 5 services optionnels avec abonnement :

- Le module antiviral,
- Le module IPS (prévention d'intrusion),
- Le module de blocage de spam,
- Le module de filtrage de flux applicatif (Web etc.),
- Le module LiveSecurity.

WSM (WatchGuard System Manager) est la principale interface de gestion. Elle vous permet de gérer un parc conséquent de pare-feu (ici un seul). Elle permet d'accéder à la plupart des autres modules de gestion du pare-feu. En un coup d'œil vous avez accès à l'état physique de vos pare-feu (interfaces réseau up/down, tunnels VPN, PKI etc.) :

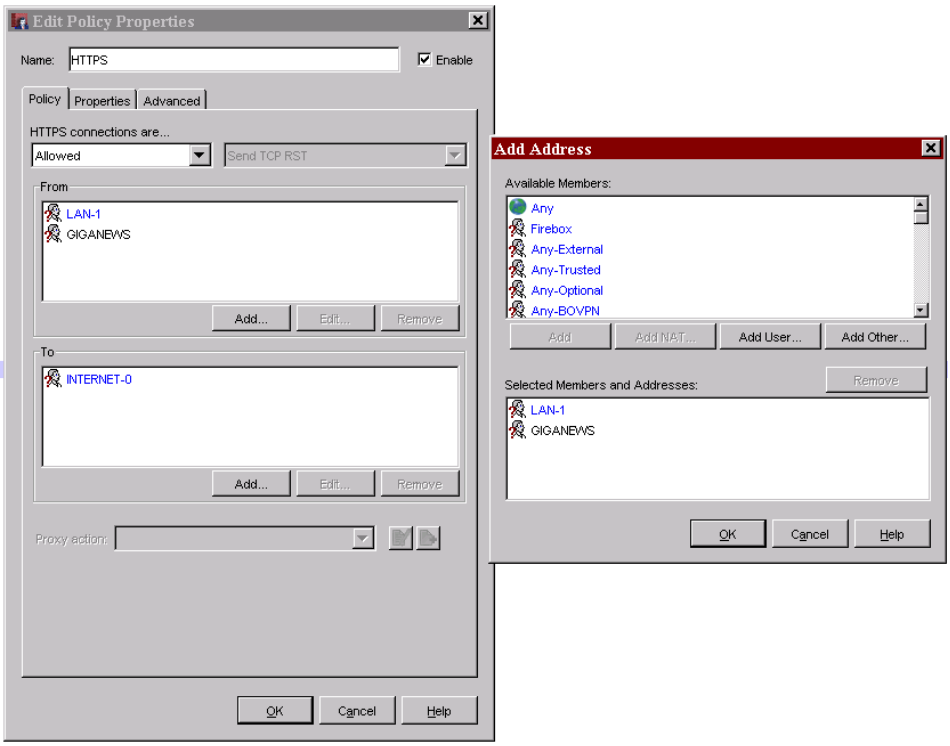


XTM policy Manager : comme sur le pare-feu précédent un module de gestion des règles de filtrage est présent.
C'est un outil très complet et complexe à prendre en main, vouloir enumérer les possibilités offertes (QoS, VLAN Tagging, Planification etc.) reviendrez à écrire plus de 1000 pages d'explications.



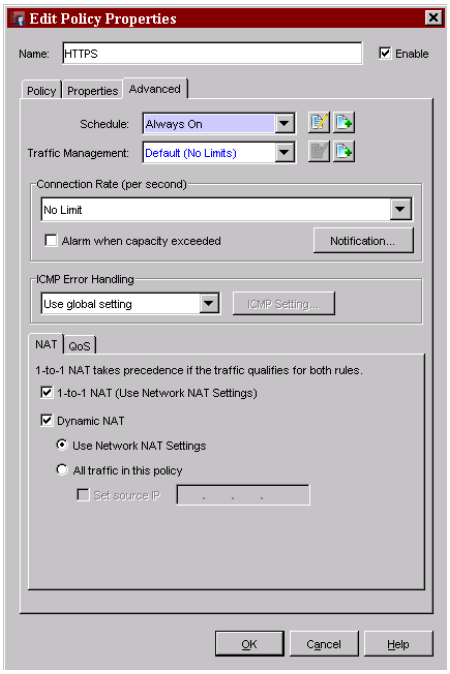
Tout comme sur le pare-feu précédent une approche objet de la modélisation de votre politique de sécurité est possible. Elle est même vivement conseillé avec ce type de pare-feu.

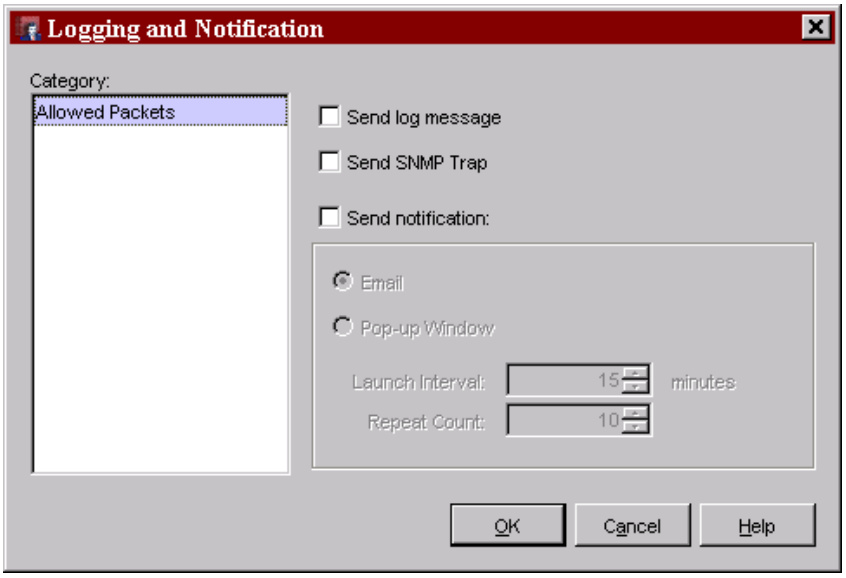
Voici comment il est possible de choisir des objets « source » (From) et « destination » (To) parmis une liste modifiable d'objets (hôtes, utilisateurs, réseau etc.) :



Enfin sachez que pour chaque règle vous pouvez appliquer une multitude d'autres paramètres :

- Gestion du trafic (bande passante),
- Planification,
- Qualité de service (QoS),
- Translation d'adresse,
- Journalisation avancée,
- Etc.

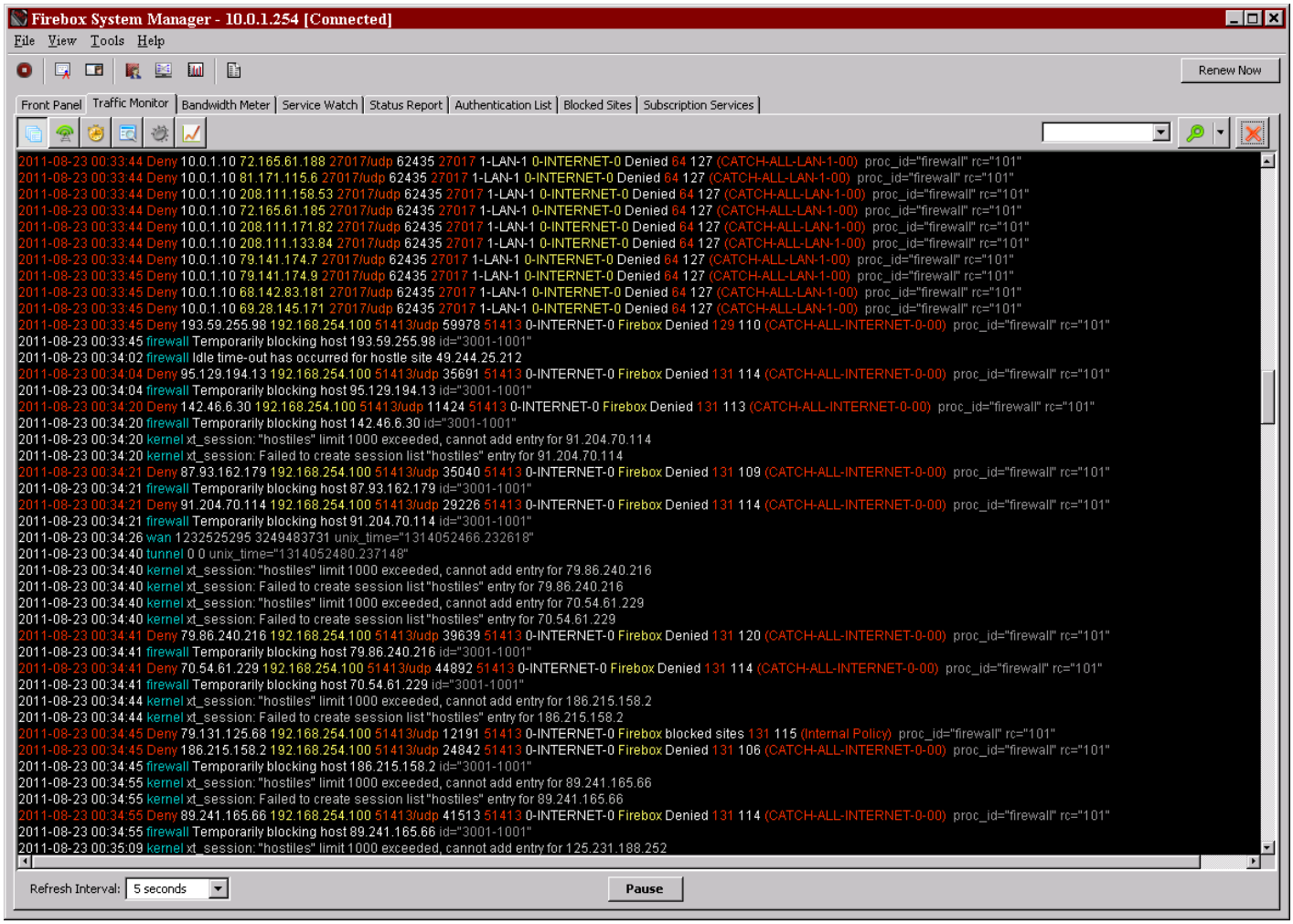




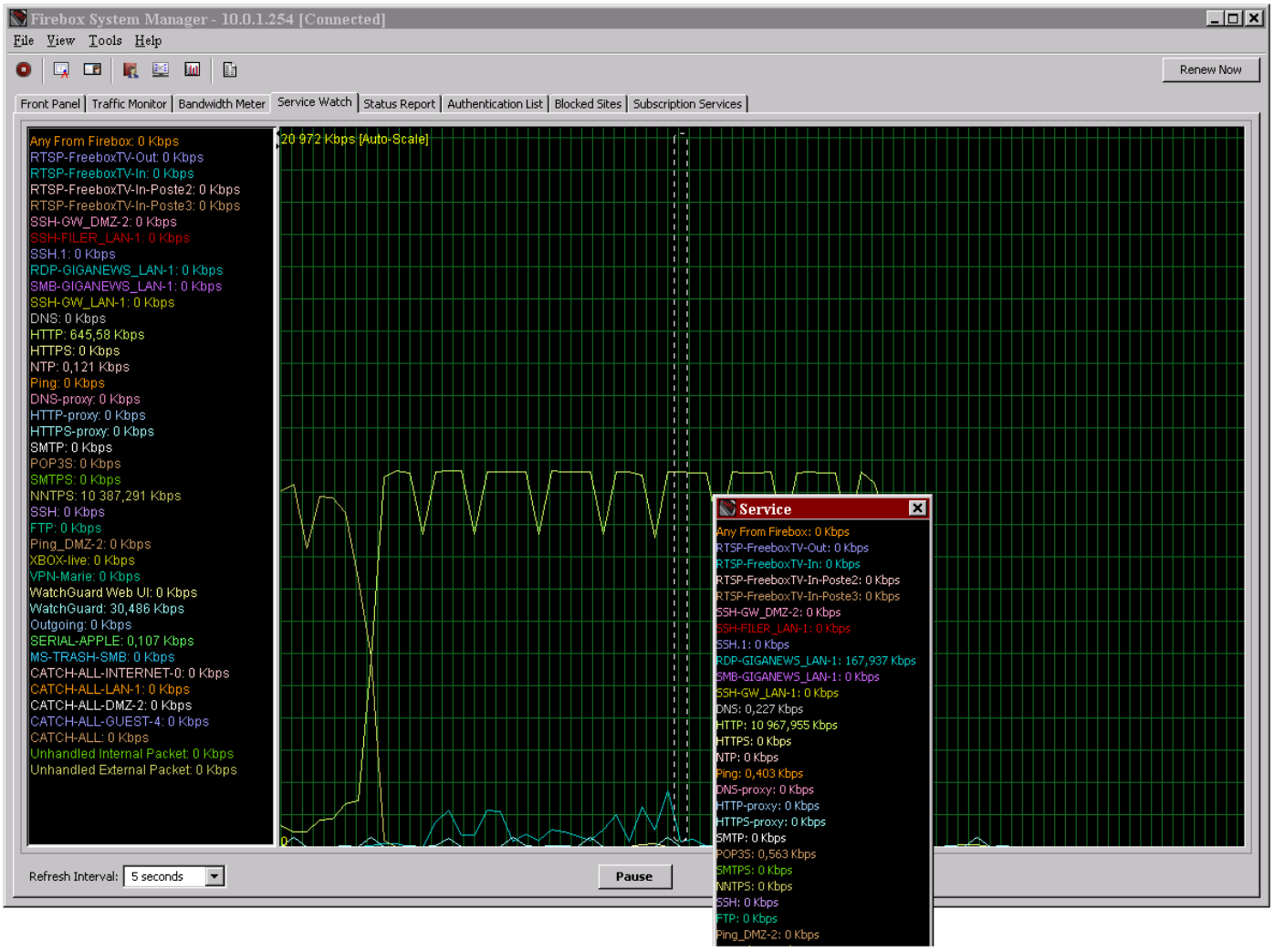
FSM (Firebox System Manager) est le module permettant de monitorer et superviser votre pare-feu, il est très complet.
Avec, vous pouvez, en temps réel :

- Visualiser l'état général du pare-feu,
- Contrôler le trafic, le noyau, les accès autorisés/interdits, les menaces détéctées,
- Visualiser la bande passante par interface,
- Visualiser l'allocation de bande passante par service,
- Avoir un rapport du status système (noyau Linux, ces modules etc.)
- Une liste des adresses bloquées,
- Un liste des utilisateurs authentifiés,
- Un état des souscriptions des modules optionnels,
- L'état des tunnels VPN actifs,
- Etc.

Voici l'écran permetttant de contrôler tout le trafic qui transite par le pare-feu :

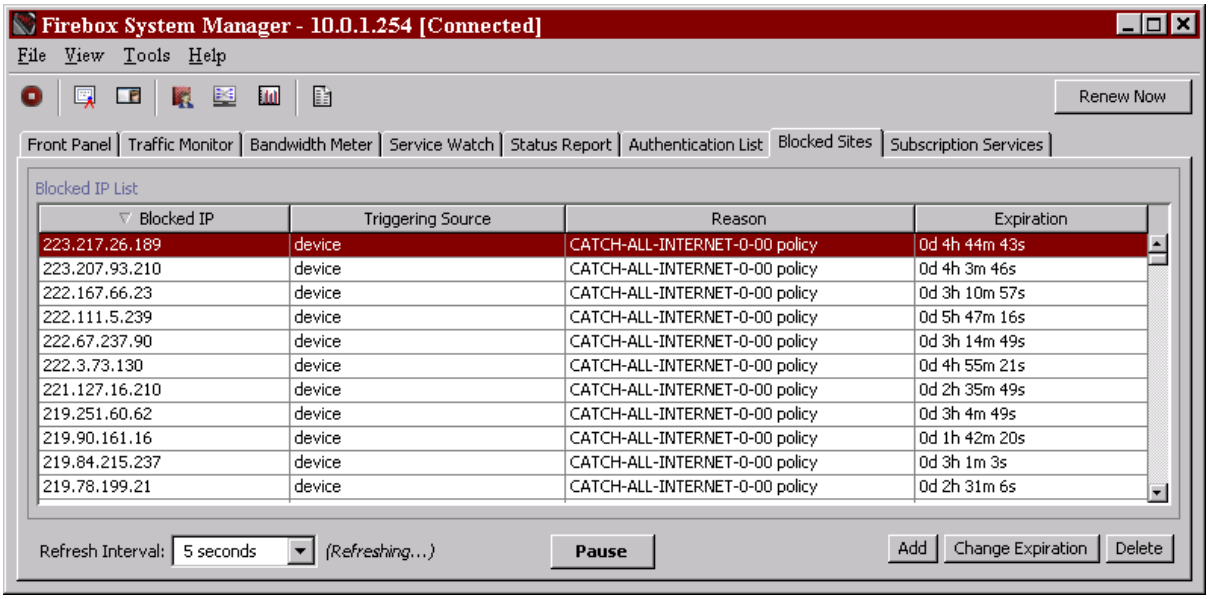


La capture suivante montre l'analyseur de débit réseau par service (protocole) :



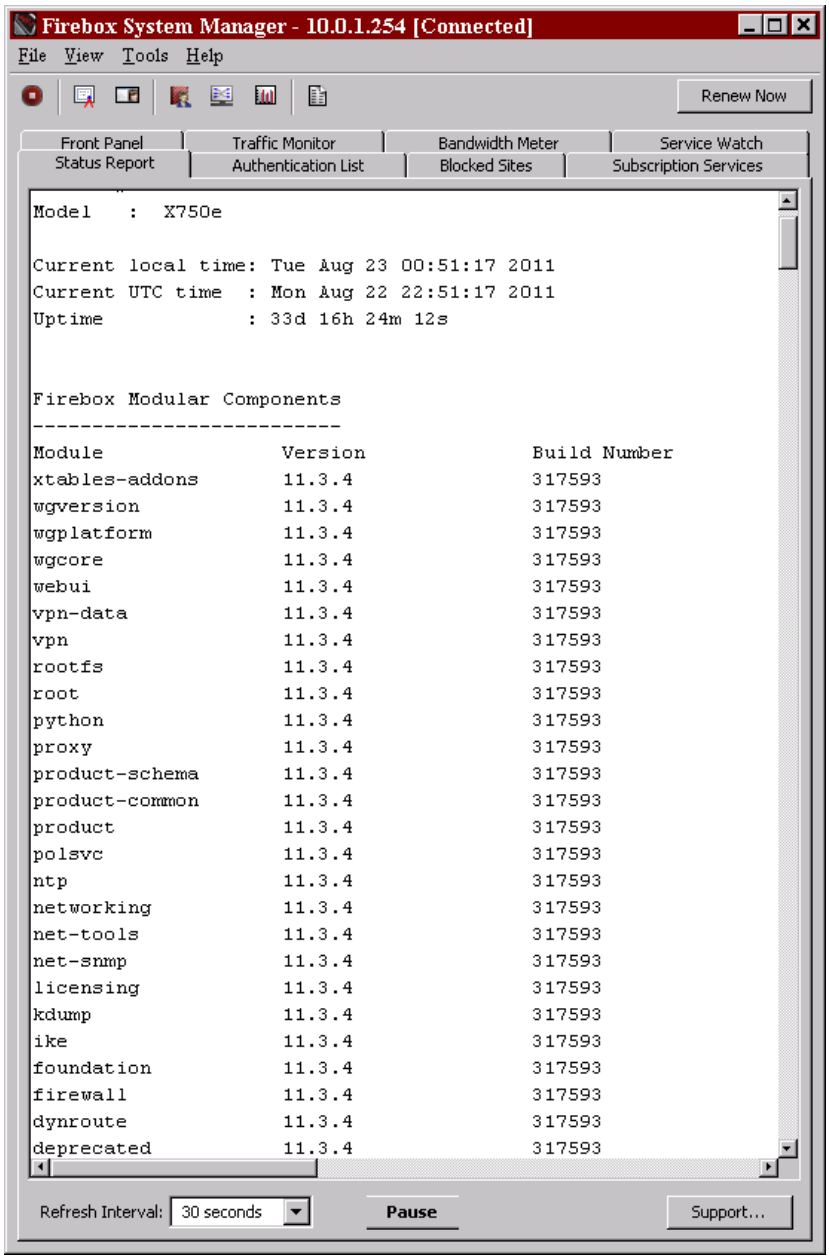
Cet outil est très pratique pour connaitre la cause d'un engorgement réseau provoqué par un service donné. Il permet également de s'assurer que la bande passante disponible est utilisée à bon escient.
Le graphique affiché est complétement paramétrable (couleur, service, échelle etc.).

L'onglet suivant permet de lister les sites bloqués temporairement par le pare-feu :



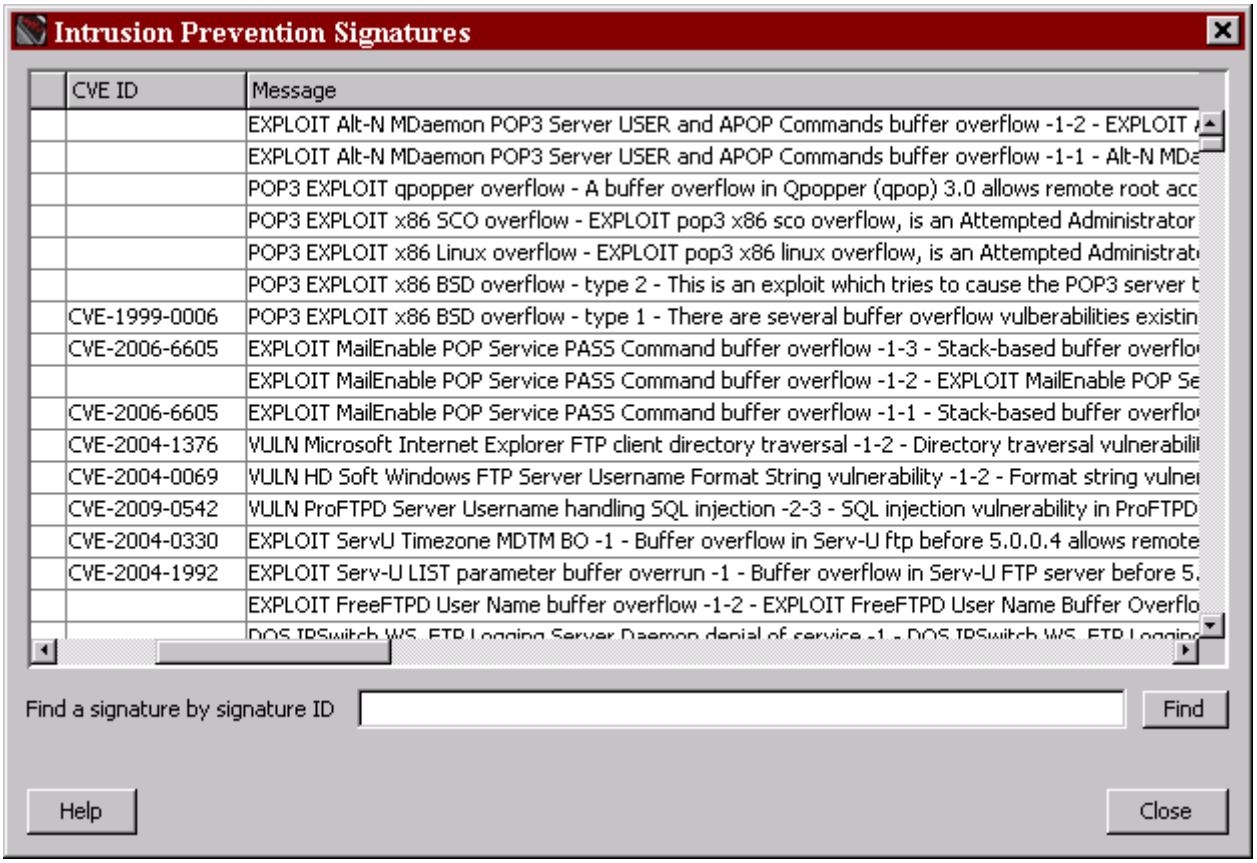
Cet onglet affiche un rapport du status système à savoir :

- Le noyau Linux,
- Ces modules,
- Les interfaces et la configuration réseaux (ifconfig, route, mii-tools, arp, dhcpd),
- Les journaux du pare-feu,
- La liste des processus Linux,
- L'utilisation de la mémoire,
- La charge système globale,
- L'état du cluster et du load balancing.



Le module ***IPS (Intrusion Prevention Signature)*** comme son nom l'indique permet de stopper les menaces. Il s'appuie sur une base de données d'attaques.

Pour des produits comme les WatchGuard XTM une palette de 15 000 types d'attaques est déjà codée. Avec le module IPS le pare-feu met à jour en permanence sa base d'attaque/contre-mesures, en voici un court extrait :



Grâce à ce genre de module les intrusions réseau sont donc en partie identifées et bloquées : elles sont souvent identifiées comme « internal-policy ».

Voici les services assurés par le module IPS :

- Protection complète contre un large éventail de vulnérabilités de sécurité connues et de points faibles dans les applications, les bases de données et les systèmes d'exploitation.

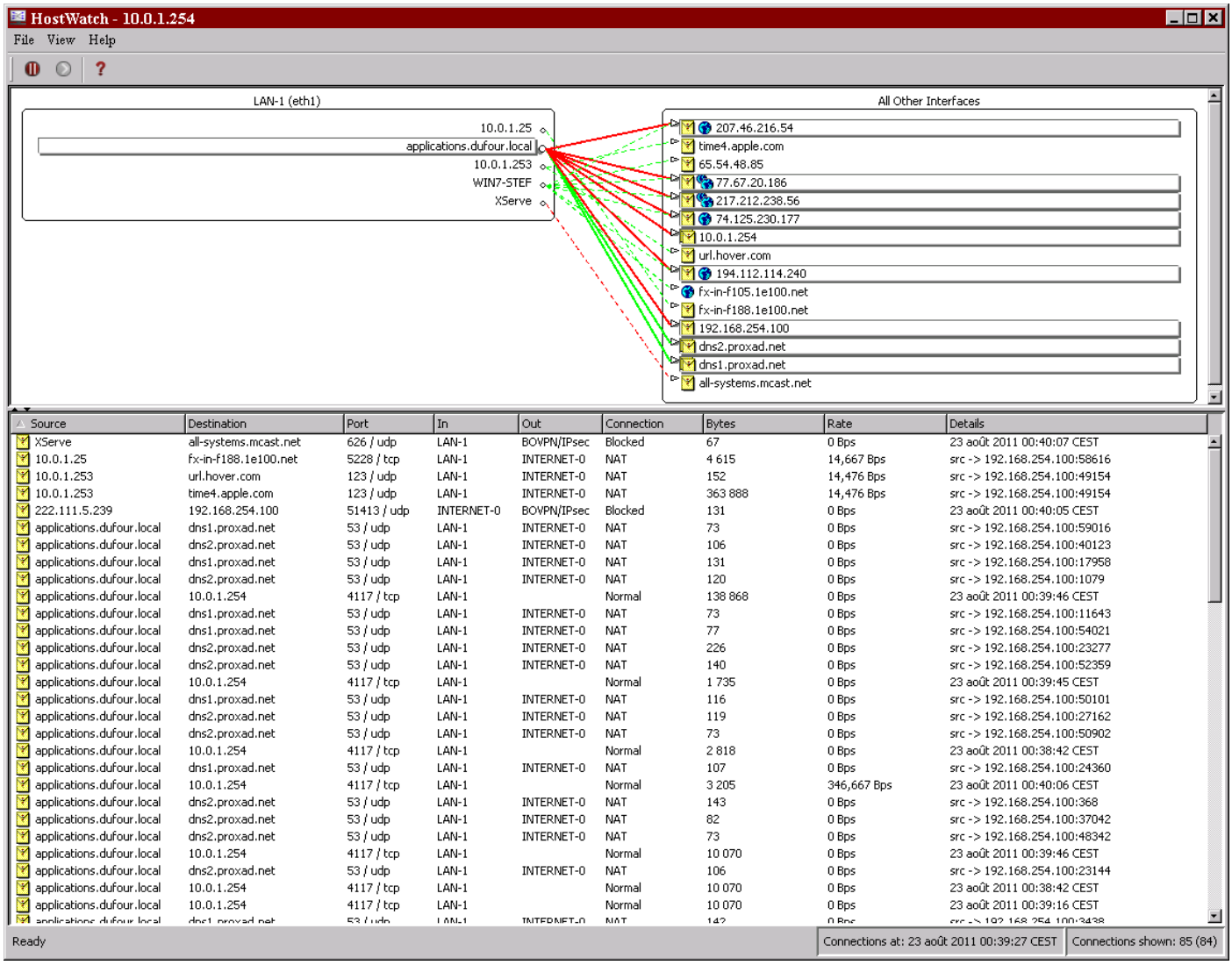
- Plus de 15 000 signatures protègent contre un vaste ensemble de menaces, dont les injections SQL, les scripts entre sites (XSS), les dépassements de mémoire tampon, le refus de service et les inclusions à distance de fichiers.

- Base de données des signatures actualisée en permanence, pour garantir une protection étendue et opportune. Nouvelles signatures mises en circulation dès l'apparition de nouvelles menaces. Analyse comportemental du trafic bloquant des menaces encore non identifiées

- Analyse tous les protocoles principaux, notamment HTTP, HTTPS, FTP, TCP, UDP, DNS, SMTP et POP3 pour bloquer les attaques de protocoles, du réseau et des applications.

- Garde les logiciels espions hors du réseau en bloquant ceux rencontrés lors de la navigation Internet, et en identifant les logiciels espions qui tentent de contacter l'hôte.

Enfin **HostWatch** est une console de monitoring qui vous permet de visualiser graphiquement les connexions en temps-réel. Ici il vous suffit de choisir une interface réseau ensuite vous pouvez visualiser les connexions en cours pour une machine donnée.
A partir de cette interface vous pouvez bloquer un site distant douteux, ou une machine de votre propre réseau :



Conclusion

Tout au long de ce cours vous avez pu vous apercevoir que tout est perfectible en matière d'architecture sécurisée mais surtout qu'en matière de sécurité informatique : le 100% est inatteignable.

Alors on limite les intrusions, sans relâche avec une vigilance de tous les jours.

Le pare-feu bien que pierre angulaire du dispositif ne peut se soustraire à une rigueur et formation des principaux acteurs de la sécurité informatique : les experts et les utilisateurs.

Le point de départ commence donc par la sensibilisation, des autorités dirigeantes puis des utilisateurs aux risques encourus et moyens pour s'en prémunir.

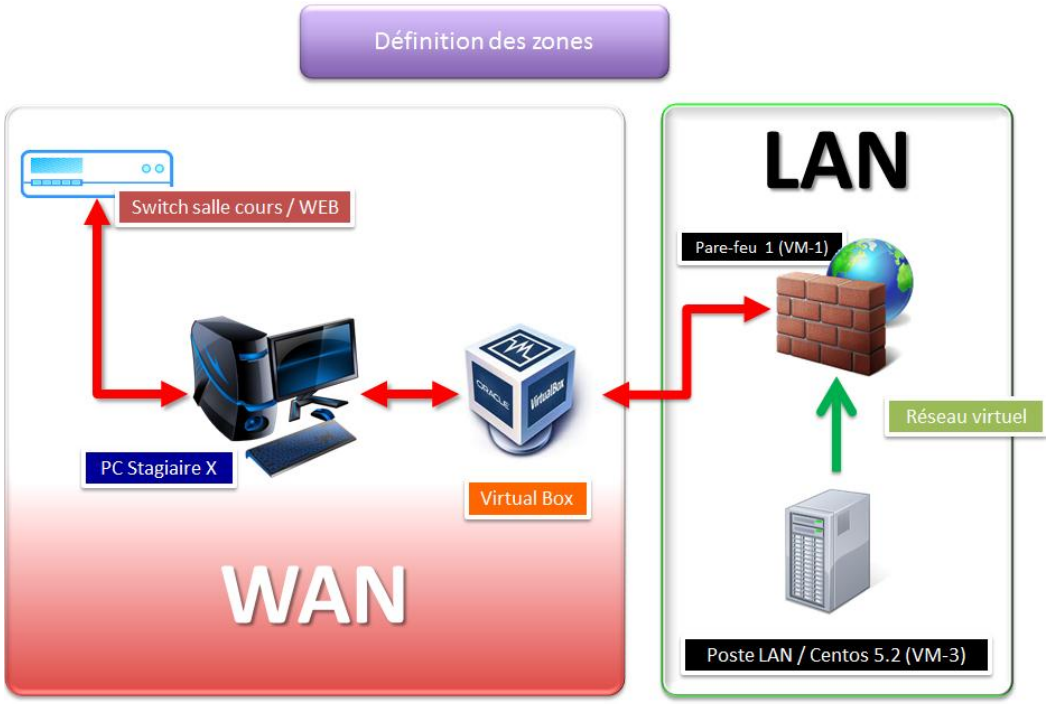
De plus on s'aperçoit que la principale qualité d'un expert en sécurité reste encore et toujours le bon sens et la maitrise des concepts de bases.
Vous aurez compris que vouloir sécuriser un SI avec des outils développés à la va vite ou des briques systèmes inappropriées est souvent catastrophique en terme de sécurité : autant ne rien faire.

En milieu professionnel (production) le pare-feu expérimental n'a pas sa place. Alors exit les pare-feu « from scrtach » et surtout choisissez votre pare-feu en adéquation de ce que vous avez à protéger.

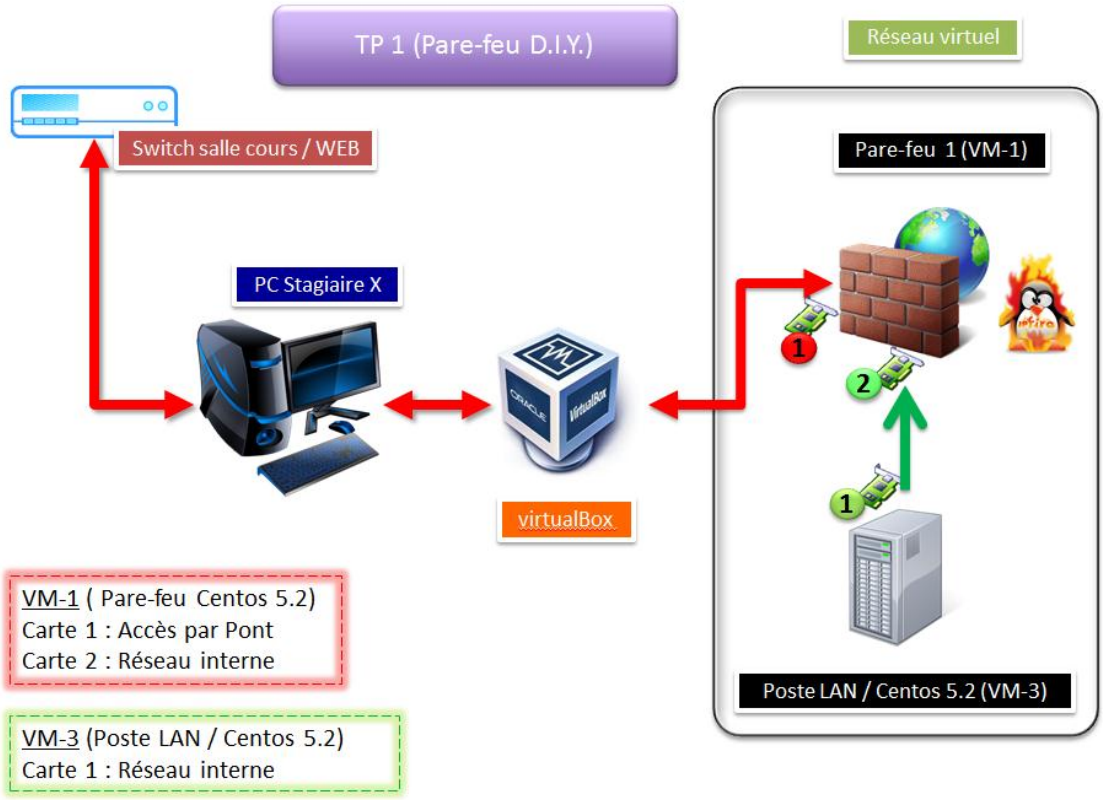
Placer un pare-feu à plusieurs milliers d'euros pour protéger 6 stations de travail ne rime pas à grand-chose : une fois de plus le bon sens et la maîtrise des concepts de bases doivent être à l'honneur quand on souhaite déployer un pare-feu.

TRAVAUX PRATIQUES

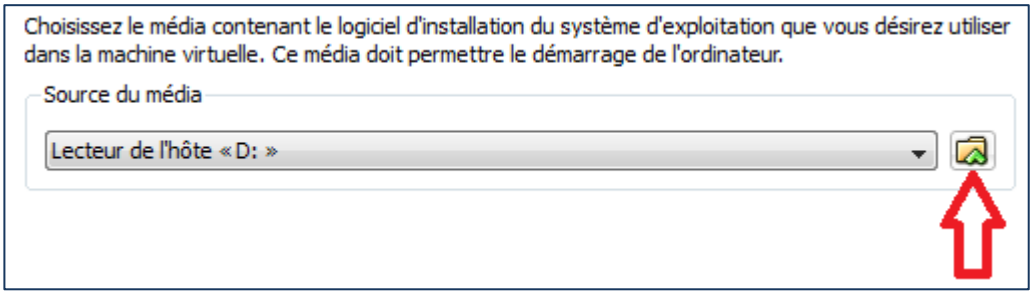
Considération des zones :



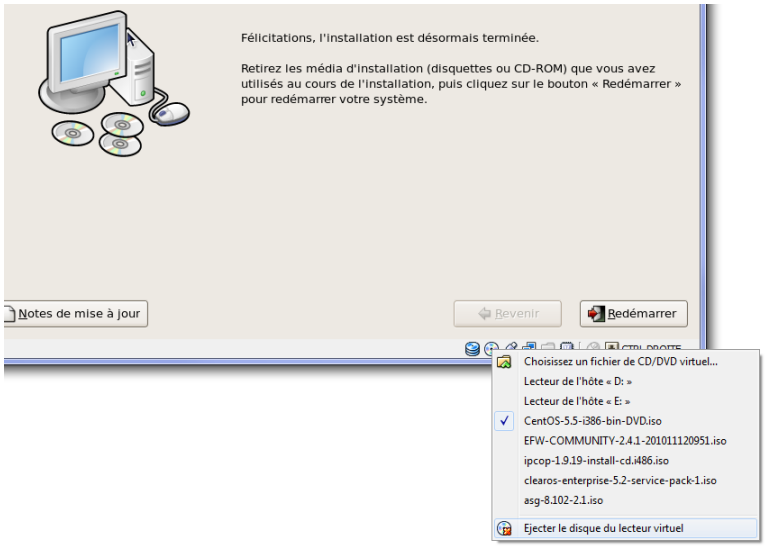
TP N°1 : Pare-feu « from scratch » sur Centos (RedHat©)



1- Installez votre station d'administration (modèle Linux RedHat) du pare-feu (***VM-3 Poste LAN-Admin***) qui fera également office de client du LAN. Procédez comme suit :
   a. Sous Virtual Box :
      Nom = « ***VM-3 Poste LAN-Admin*** »
      Système d'exploitation = « ***Linux*** »
      Version = « ***RedHat*** »
   b. Ensuite tout paramètre par défaut (« suivant »x fois),
   c. Une fois la VM créée cliquez sur « Réseau » puis choisir « **Carte 1** » et sélectionnez « **Réseau interne** ».
   d. Démarrez votre VM en choisissant l'image ISO de Centos-5.5-i386

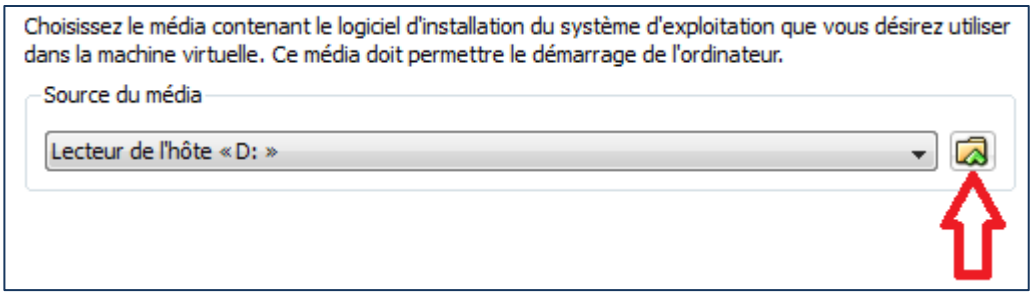


   e. Déroulez une **installation « Desktop »** par défaut et en « Français »,
   f. Mettez une **IP fixe en 10.0.10.100/255.255.255.0** (désactiver IPv6),
   g. Renseignez la passerelle et un serveur DNS avec 10.0.10.254 (votre pare-feu fera, pour les besoins du cours relais DNS et passerelle),
   h. « Suivant » puis saisissez un mot de passe fort (dont vous vous rappellerez),
   i. Ne faites pas de personnalisation, choisissez « Suivant » à chaque demande (votre Centos s'installe en 8mn environ),
   j. A la demande éjectez le DVD-ROM via un clic droit sur le lecteur de CD, puis cliquez sur « Redémarrer » :

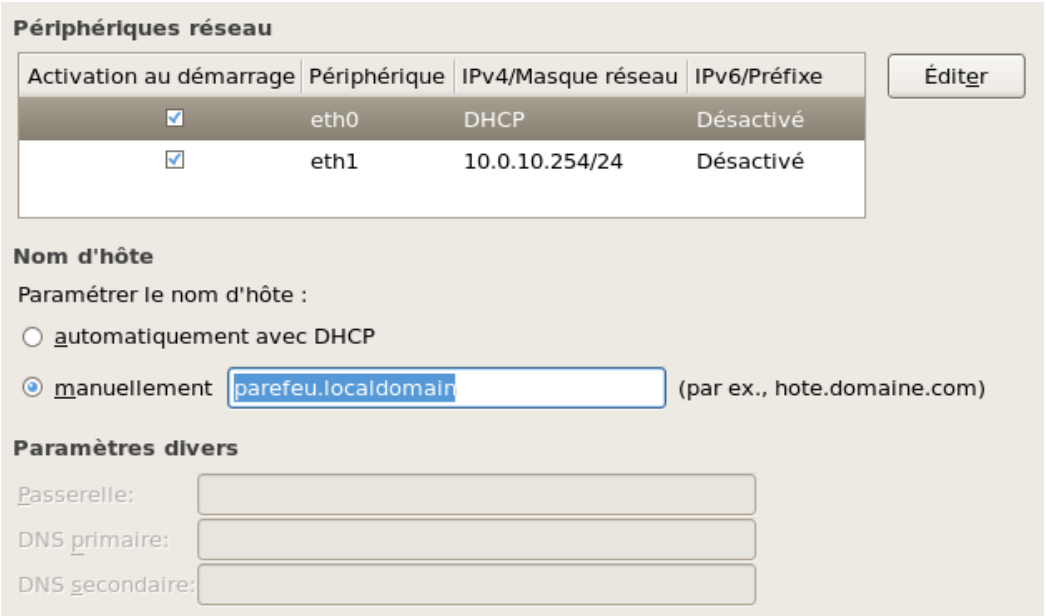


   k. Après redémarrage, cliquez sur « Avancer »puis laissez « Pare-feu : activé » en décochant SSH,
   l. Laissez « SE Linux : strict »,
   m. Créez un compte « stagiaireX » qui sera simple utilisateur sur votre station d'administration.
   n. Connectez-vous avec votre station d'administration (Eventuellement vous pouvez changer la résolution de la VM : « Système/Administration/Affichage » et onglet « Paramètres » et « Matériel/Type Ecran : LCD … »),
   o. Faites des tests de connectivités (Ping, Tracert)

2- Installez votre pare-feu (***VM-1 Pare-feu DIY***) qui doit avoir deux cartes réseaux virtuelles. Une sur la salle de cours (WAN pour nous) et l'autre sur votre LAN interne (« Réseau interne » Virtual Box).
   a. Sous Virtual Box :
      Nom = « ***VM-1 Pare-feu DIY*** »
      Système d'exploitation = « ***Linux*** »
      Version = « ***RedHat*** »
   b. Ensuite laissez tous les paramètres par défaut (« suivant » x fois),
   c. Une fois la VM créée cliquez sur « Réseau » puis choisir :
      « **Carte 1** » et sélectionnez « Accès par **Accès par pont** »,
      « **Carte 2** » et sélectionnez « **Réseau interne** ».
   d. Démarrez votre VM en choisissant l'image ISO de Centos-5.5-i386



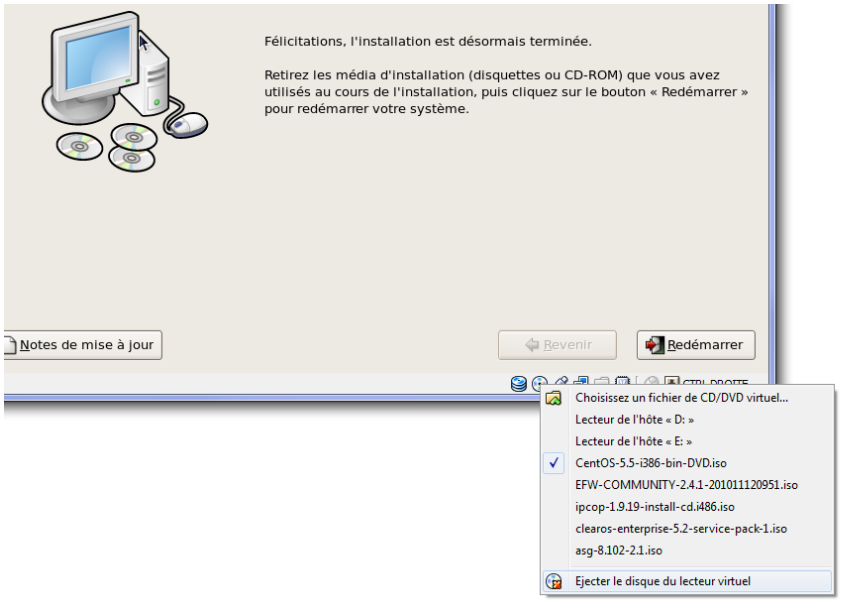
   e. Déroulez une **installation « De base »** par défaut et en « Français »,
   f. Mettez ***DHCP*** pour la patte WAN (Externe) c'est à dire l'interface ***eth0*** (ayant un « accès par pont ») et décochez IPV6,
   g. Puis une ***IP fixe en 10.0.10.254/255.255.255*** pour la patte LAN(Interne) pour l'interface ***eth1*** qui sera ***active au démarrage*** (ayant un accès « réseau interne ») et décochez IPV6.



   h. « Suivant » puis saisissez un mot de passe fort (dont vous vous rappellerez),
   i. Désélectionnez TOUT puis choisissez « ***Personnaliser maintenant*** », et « suivant »,
   j. Désléctionnez TOUT les paquetages sauf « ***vi*** » et « ***Système de base/Base*** » :

k. Cliquez sur « suivant », votre Centos s'installe en 4 mn environ,

l. A la demande éjectez le DVD-ROM via un clic droit sur le lecteur de CD, puis cliquez sur « Redémarrer » :

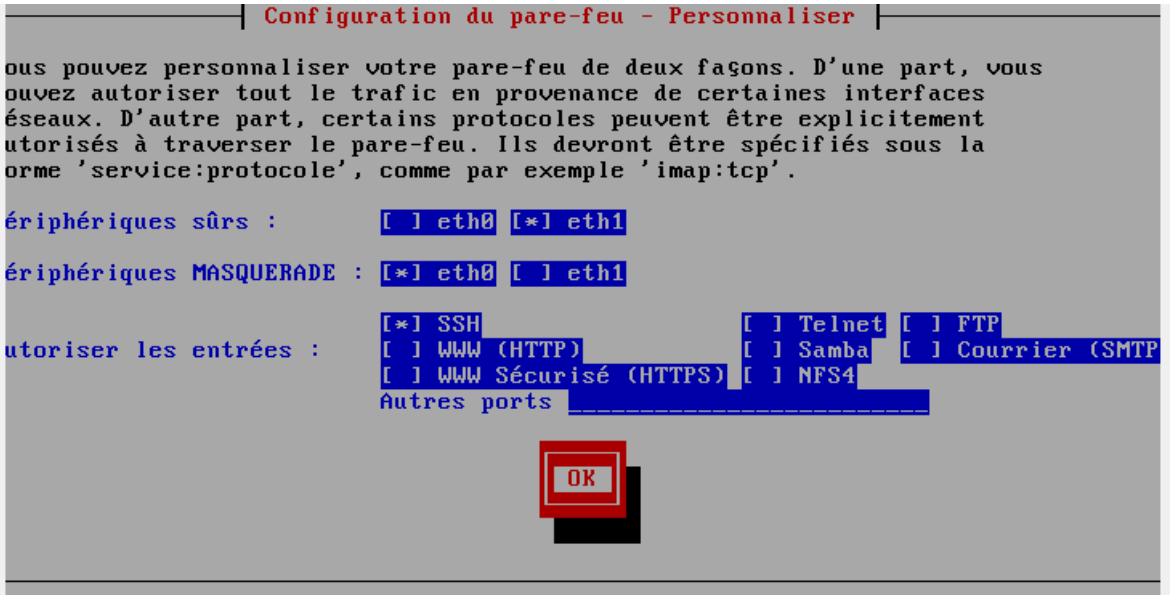


m. Après redémarrage, n'ayant pas installé l'interface graphique (gnome ou kde) vous vous retrouvez en mode texte, sélectionnez « ***configuration du pare-feu*** » puis « ***Exécutez l'outil*** » :

Note : On navigue dans les menus avec les touches « TAB » et « ENTER ».

n. Sélectionnez sur « ***Personnalisation*** »,

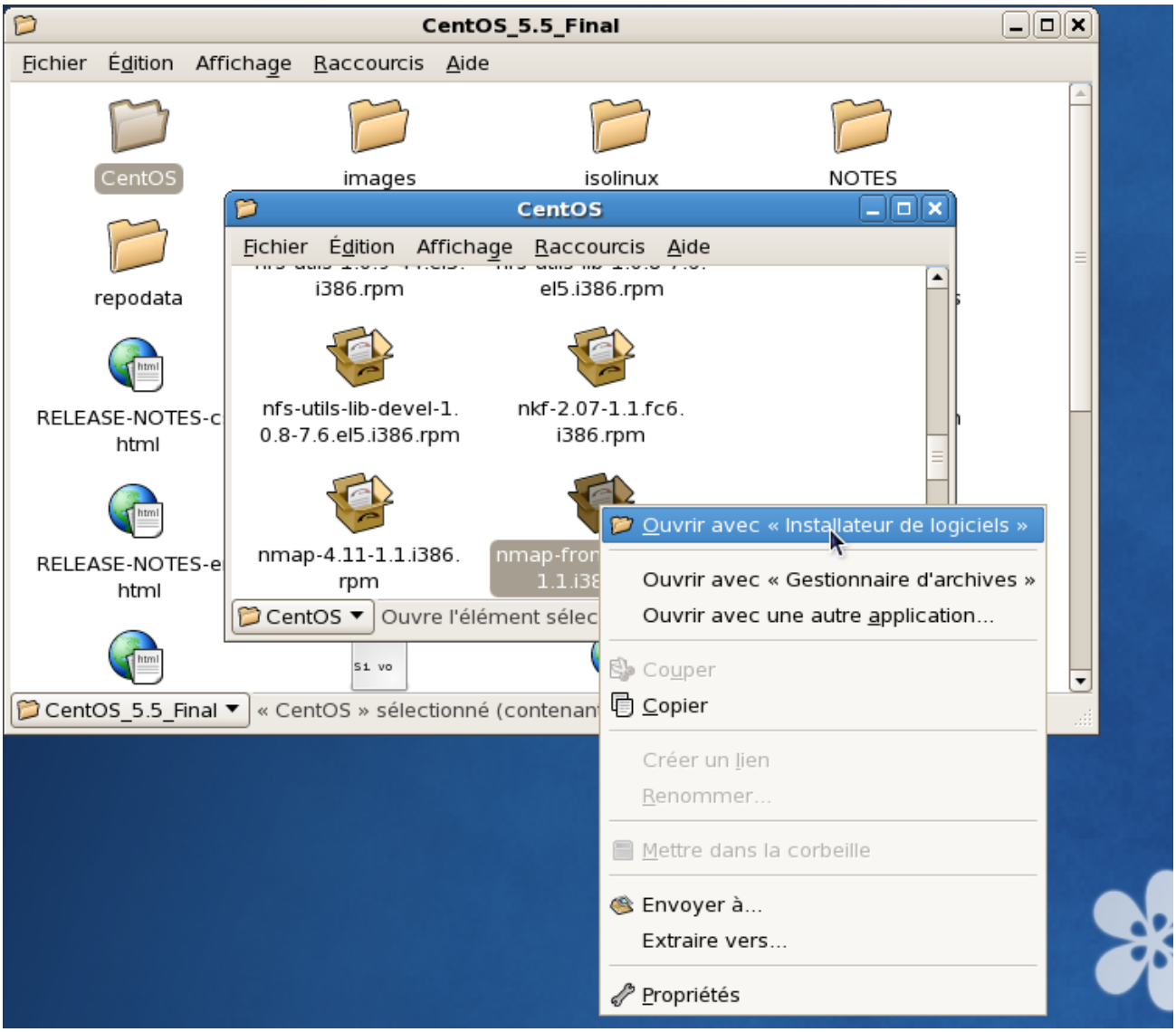
o. Enfin sélectionnez les paramètres suivants :



p. Sortez en validant à chaque fois avec « ***OK*** », puis à la fin « ***Quittez*** »

q. Vous disposez d'une pare-feu/routeur opérationnel.

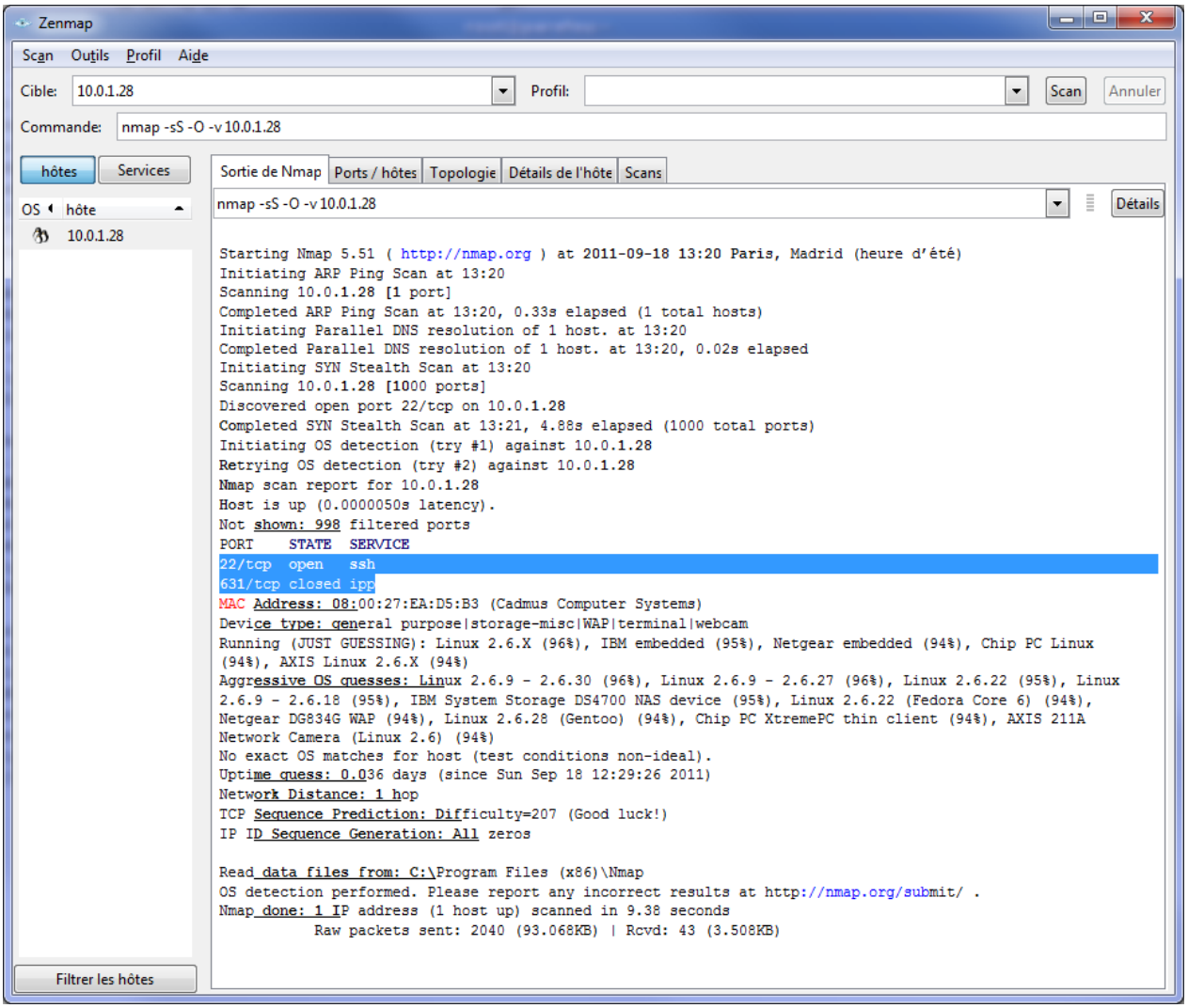
1. Maintenant **connectez-vous sur votre VM-3** (Poste Admin/lan),
2. Ouvrez un **terminal** et faites à nouveau des **tests de connectivité** (Ping, Tracert etc.) :
   Le pare-feu est accessible mais nous ne pouvons pas sortir sur le réseau de la salle de cours.
3. Installez l'outil « nmap » sur votre station Centos (pour ce faire remettez le DVD-ROM puis double-cliquez sur « ***nmap*** » :



4. Avec le **terminal basculez avec l'utilisateur « root »** puis faites un scan de port de votre pare-feu, quels sont les ports ouverts ?

```
nmap -sS -O -v 10.0.10.254
```

5. Vous pouvez effectuer un scan de port (avec nmap win32) depuis votre station Windows XP sur votre pare-feu (connectez-vous sur votre pare-feu pour connaître son adresse obtenu par bail DHCP) :



Vous constatez que l'installation par défaut ouvre le port 22/ssh sur le LAN mais, plus fâcheux, également sur le WAN ….

6. Connectez-vous en « root » via « ssh » sur votre pare-feu depuis votre VM-3 (Poste Admin/LAN),

```
[root@localhost ~]# ssh root@10.0.10.254
The authenticity of host '10.0.10.254 (10.0.10.254)' can't be established.
RSA key fingerprint is 0c:37:f3:0d:37:42:56:a2:0b:80:8f:f3:67:33:a0:79.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.10.254' (RSA) to the list of known hosts.
root@10.0.10.254's password:
Last login: Sun Sep 18 12:43:20 2011 from 10.0.10.100
[root@parefeu ~]#
```

7. Créez un compte « stagiaireX » qui sera simple utilisateur sur votre pare-feu :

```
adduser stagiaireX
passwd stagiaireX
```

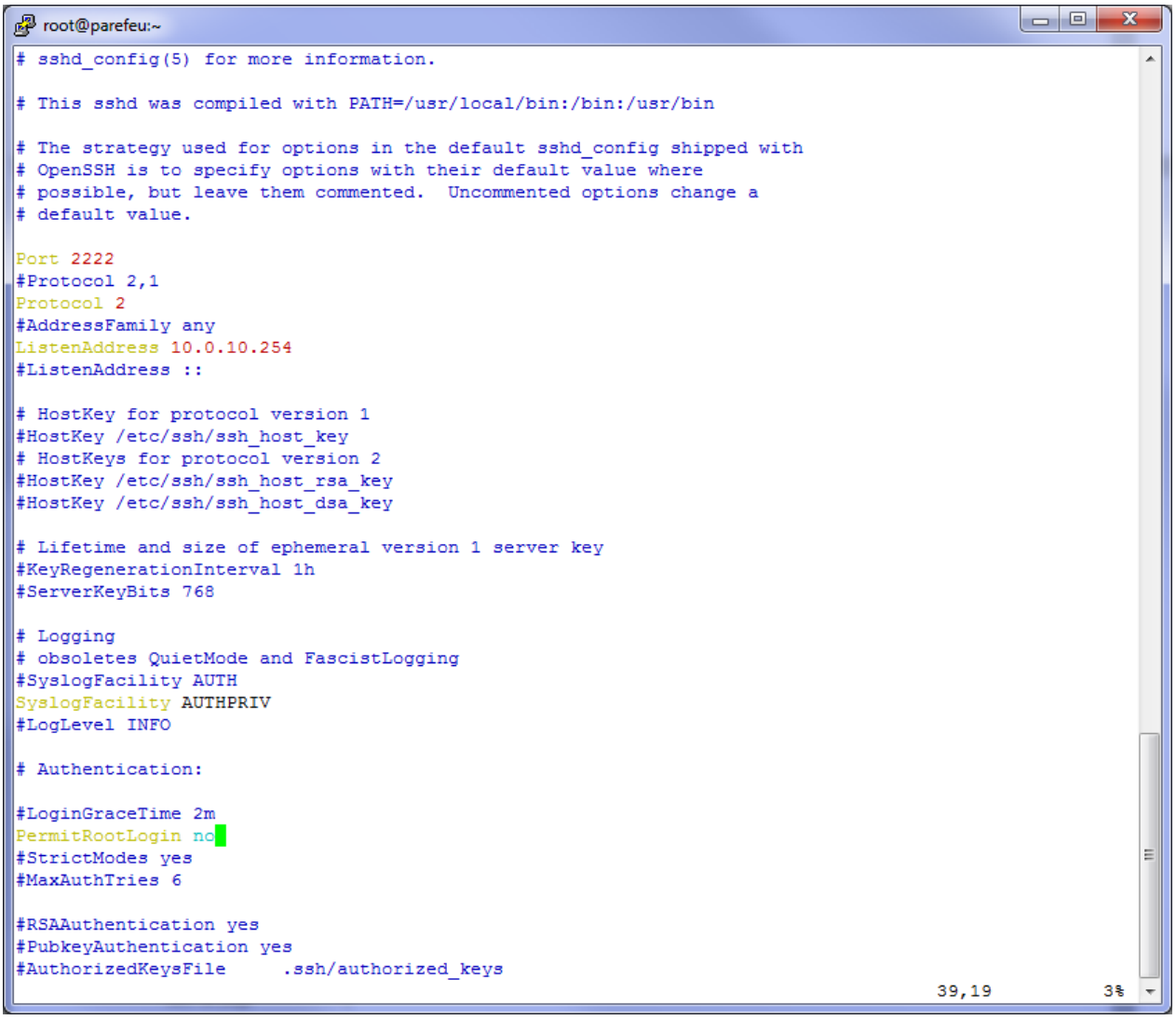
8. Quelles sont vos règles de filtrage par défaut de votre pare-feu ?

   iptables-save

9. Pourquoi le réseau WAN n'est-il pas accessible depuis votre VM-3 ADM/LAN ? Faites en sorte que votre réseau WAN soit visible depuis votre station VM-3 ADM/LAN

   Aide : Forward et Nat.

10. Hardenning basique : verrouillez l'accès SSH :
    - Pas de connexion directe avec « root »,
    - Changement du port « ssh » par défaut 22 à 2222,
    - Modifiez l'interface d'écoutes : interdisez l'accès depuis le WAN,
    - Modifiez le port autorisé pour SSH dans vos règles de pare-feu (iptables -R INPUT x etc.).

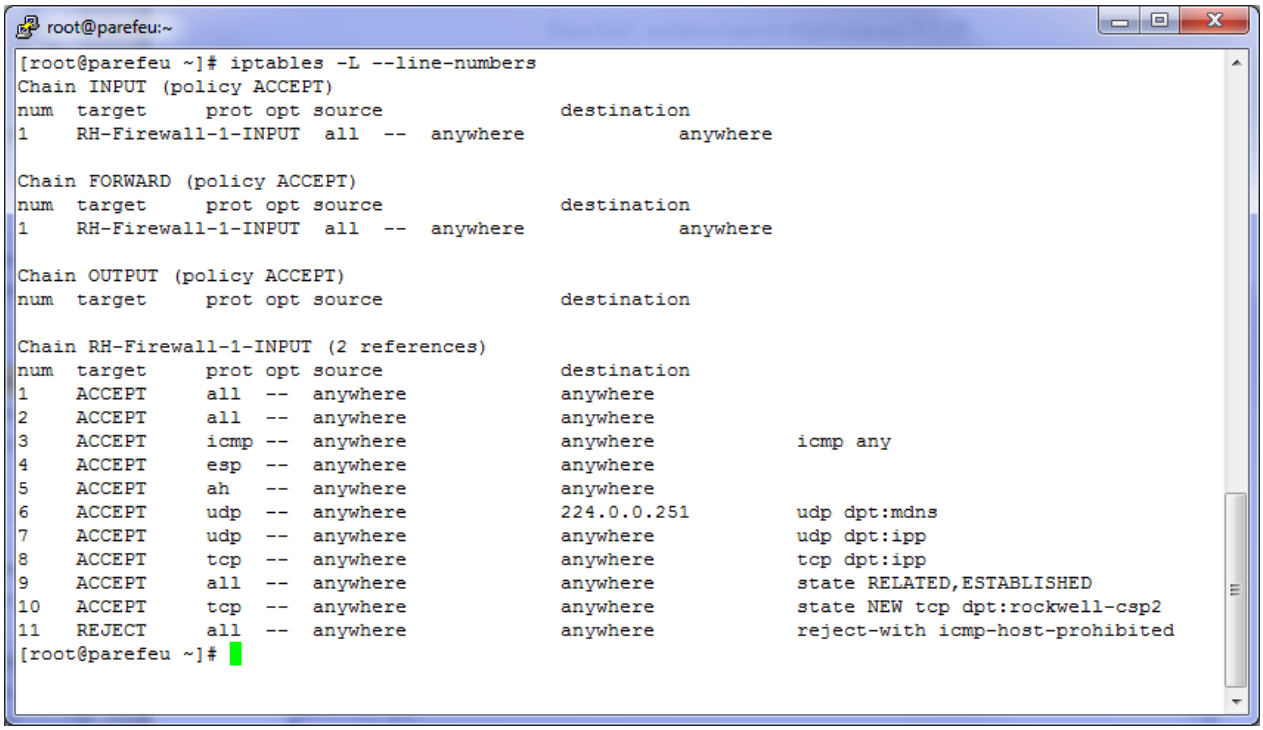


   Sauvegardez vos règles pour le prochain redémarrage (service iptables save)

   Aide :

   iptables -R RH-Firewall-1-INPUT 10 -p tcp --dport 2222 -m state --state NEW -j ACCEPT

Cette installation basique est intéressante mais ne permet pas de comprendre la mise en place de toutes les règles « iptables » en présence.



De plus tout le trafic sortant de votre pare-feu (OUTPUT) est autorisé, ce qui rompt avec les « best practice ». Les politiques sont toutes par défaut sur ACCEPT …

Vous allez paramétrer NetFilter pour partir sur de bonnes bases …

- Mettez en production le **script fourni ci-dessous** (n'oubliez pas de faire « chmod +x script.sh » pour le rendre exécutable, puis sauvez votre config avec un « service iptables save »),
- Ouvrez les ports adéquats pour permettre **l'administration via « ssh » depuis la station VM-3**,
- Faites en sortes que votre **station d'administration** (Poste LAN : VM-3) puisse **accéder au Web**
- Effectuez un scan de port depuis votre station d'administration et consultez les journaux de votre pare-feu : le scan a-t-il était détecté ?
- *Bonus* : Faites en sortes que votre **station d'administration** (Poste LAN : VM-3) puisse **accéder aux partages CIFS (Windows) de la salle de cours**, aidez-vous des journaux pour prendre connaissances des ports à ouvrir.

Astuce : Pour debugger vos règles de pare-feu utiliser la commande suivante :

```
tail -f /var/log/messages
```

pour avoir une console TTY avec une meilleure résolution « vi /etc/grub.conf », puis à la fin de l'option du Kernel « … vga=791 ».

OPTIONNEL : Si vous avez fini le TP essayez de comprendre et à l'issue mettre en production le script fourni en annexe « Pare-feu multizones », des adaptations sont nécessaires.

Script à mettre en place

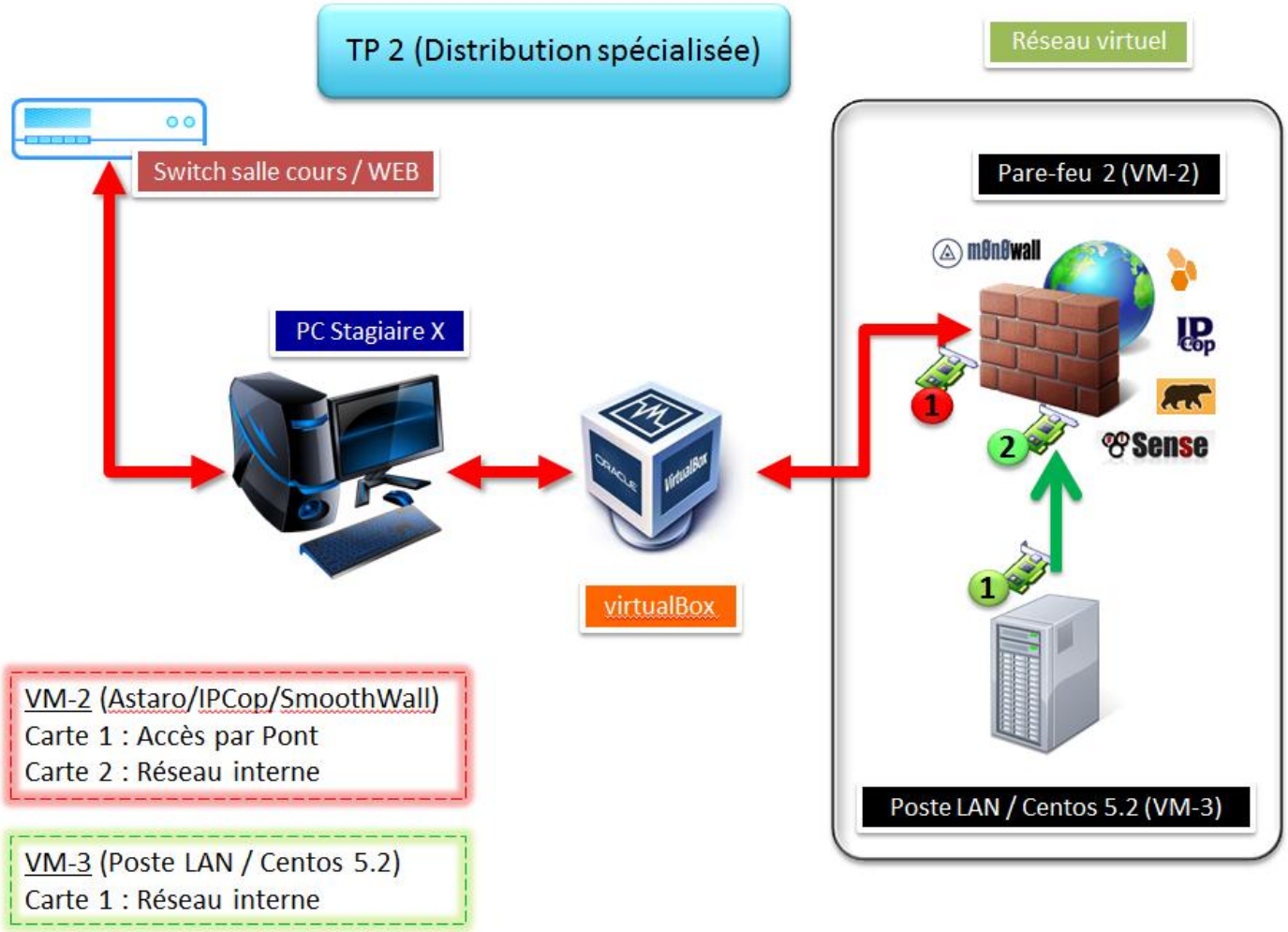
```
#!/bin/sh
# Mise en place du pare-feu
Nom_PareFeu=`hostname`
echo "Configuration des regles de filtrage de $Nom_PareFeu !"

#
###############################################################################
# Binaires utilises
IPT=/sbin/iptables
IFCONFIG=/sbin/ifconfig
#
###############################################################################
# Variables

# Variables :les interfaces reseaux du pare-feu
if_lo="lo"
if_wan="eth0"
if_lan="eth1"
#if_dmz="eth2"

# Variables :les reseaux geres par le pare-feu
net_wan="dhcp"
net_lan="10.0.10.0/24"
#net_dmz="192.168.254.0/24"

# Variables :les adresses IP du pare-feu
ad_parefeu_wan=`$IFCONFIG $if_wan | grep "inet adr" | awk -F: '{print $2}' | awk
{'print $1}'`
ad_parefeu_lan=`$IFCONFIG $if_lan | grep "inet adr" | awk -F: '{print $2}' | awk
{'print $1}'`
#ad_parefeu_dmz=`/sbin/ifconfig $if_dmz | grep "inet adr" | awk -F: '{print $2}' | awk
{'print $1}'`

# Variables :les adresses IP des hotes geres par le pare-feu
any="0.0.0.0/0"
station_admin="10.0.10.100/32"
serveur_fichier="10.0.10.1/32"
serveur_mail="10.0.10.2/32"
serveur_dns_interne="10.0.10.3/32"
serveur_dns_externe_1="212.27.40.240"
serveur_proxy="10.0.10.3/32"
#serveur_ntp="ntp"
# Etc.
```

```
#
################################################################################
# Mise en place de la politique restrictive (on remet tout a zero et DROP tout paquets
IP)
# Et des chaines utilisateur

# Effacement de toutes les regles dans toutes les chaines (tables filter, nat et
mangle) : -F
$IPT -t filter -F
$IPT -t nat -F
$IPT -t mangle -F
# Effacement de toutes les regles dans toutes les chaines utilisateurs (tables filter,
nat et mangle) : -X
$IPT -t filter -X
$IPT -t nat -X
$IPT -t mangle -X

# Definition de la politique de filtrage par defaut (-P) des chaines de la table
"filter"
# on "DROP" tous les paquets.
$IPT -t filter -P FORWARD DROP
$IPT -t filter -P INPUT DROP
$IPT -t filter -P OUTPUT DROP

# Definition de la politique de translation d'adresse par defaut des chaines de la
table "nat"
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT

# Definition de la politique de marquage des paquets par defaut des chaines de la table
"mangle"
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P FORWARD ACCEPT
$IPT -t mangle -P INPUT ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT
$IPT -t mangle -P POSTROUTING ACCEPT

# On cree la chaine utilisateur de journalisation des paquets rejetes
#$IPT -X LOG_DROP
$IPT -N LOG_DROP
$IPT -A LOG_DROP -j LOG --log-prefix  'NF PACKET DROP ==>' --log-level info # On
journalise le paquet indesirable
$IPT -A LOG_DROP -j DROP # On DROP le paquet apres l'avoir journalise

# Dans le même esprit on peut creer la chaine utilisateur de journalisation des paquets
acceptes
#$IPT -X LOG_ACCEPT
$IPT -N LOG_ACCEPT
$IPT -A LOG_ACCEPT -j LOG --log-prefix  'NF PACKET ACCEPT ==>' --log-level info # On
journalise le paquet desirable
$IPT -A LOG_ACCEPT -j ACCEPT # On ACCEPT le paquet apres l'avoir journalise
```

```
#
################################################################################
# Mise en place de la politique de securité active

# Ajout de regle (-A : APPEND)
# Autorisation du trafic entrant et sortant (-i et -o) sur l'interface de "loopback"
(lo)
# Note : Quand on omet le parametre -t cela signifie que nous indiquons implicitement
la table "filter"
$IPT -t filter -A INPUT -p all -i $if_lo -j ACCEPT
$IPT -t filter -A OUTPUT -p all -o $if_lo -j ACCEPT

# Mise en place du SPI (Stateful_Packets_Inspection) pour tout protocoles : le suivi de
connexion TCP/IP
$IPT -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -t filter -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Ajout des regles par protocole

# Gestion ICMP
# ICMP en entree et en sortie sur le pare-feu
$IPT -t filter -A INPUT -p icmp -j ACCEPT
$IPT -t filter -A OUTPUT -p icmp -j ACCEPT
# ICMP vers le reseau exterieur
$IPT -t filter -A FORWARD -p icmp -j ACCEPT

# Administration du pare-feu via SSH pour la station_admin depuis le LAN (tcp/udp)
$IPT -t filter -A INPUT -i $if_lan -s $station_admin -d $ad_parefeu_lan -p tcp --sport
1024:65535 --dport 2222 -m state --state NEW -j ACCEPT
$IPT -t filter -A INPUT -i $if_lan -s $station_admin -d $ad_parefeu_lan -p udp --sport
1024:65535 --dport 2222 -m state --state NEW -j ACCEPT

# Administration SSH pour la station_admin vers l'exterieur (tcp/udp)
#$IPT -t filter -A FORWARD -s $station_admin -d $any -p tcp --sport 1024:65535 --dport
22 -m state --state NEW -j ACCEPT
#$IPT -t filter -A FORWARD -s $station_admin -d $any -p udp --sport 1024:65535 --dport
22 -m state --state NEW -j ACCEPT

# Autorisation des demandes DNS vers l'exterieur (udp)
$IPT -t filter -A FORWARD -s $net_lan -d $serveur_dns_externe_1 -p udp --dport 53 -j
ACCEPT

# Navigation Web pour le poste du LAN : station_admin
#$IPT -t filter -A FORWARD -s $station_admin -d $any -p tcp --sport 1024:65535 --dport
80 -m state --state NEW -j ACCEPT

# Autorisation des requetes DNS du pare-feu vers l'exterieur
#$IPT -t filter -A OUTPUT -o $if_wan -d $serveur_dns_externe_1 -p udp --dport 53 -j
ACCEPT

# TABLE NAT
# une fois proteger, nous allons mettre en place la translation d'adresse : SNAT
# ... afin de permettre aux stations de la zone "LAN" de pouvoir sortir en se faisant
passer pour le pare-feu
$IPT -t nat -A POSTROUTING -o $if_wan -j MASQUERADE
# Note : en general seul le serveur proxy est SNATter, pas les stations clientes,
# mais comme nous ne montons pas de PROXY


# ROUTAGE
# Note: Activation du routage (ip_forward)
echo 1 > /proc/sys/net/ipv4/ip_forward
# Sur centos : dans le fichier /etc/sysctl
```

```
################################################################################
# FIN DU SCRIPT
#
# On logue les paquets indesirables (sans chaine utilisateur + /etc/syslog.conf
==>kern.=info /var/log/iptables.log + service syslogd restart
$IPT -t filter -A FORWARD -j LOG --log-prefix 'FORWARD_PKTS_DROP ==> ' --log-level info
$IPT -t filter -A INPUT -j LOG --log-prefix 'INPUT_PKTS_DROP ==> ' --log-level info
$IPT -t filter -A OUTPUT -j LOG --log-prefix 'OUTPUT_PKTS_DROP ==> ' --log-level info
# ... avec chaine utilisateur LOG_DROP
#$IPT -t filter -A FORWARD -j LOG_DROP
#$IPT -t filter -A INPUT -j LOG_DROP
#$IPT -t filter -A OUTPUT -j LOG_DROP

# CATCH-ALL", au cas ou l'on n'utilise pas la chaine utilisateur "LOG_DROP"
# on "DROP" tous les paquets.
$IPT -t filter -A FORWARD -j DROP
$IPT -t filter -A INPUT -j DROP
$IPT -t filter -A OUTPUT -j DROP
```

TP N°2 : Pare-feu distribution spécialisée



Cet exercice est dans l'esprit du précédent mais en mettant, cette fois, en œuvre une distribution dédiée.

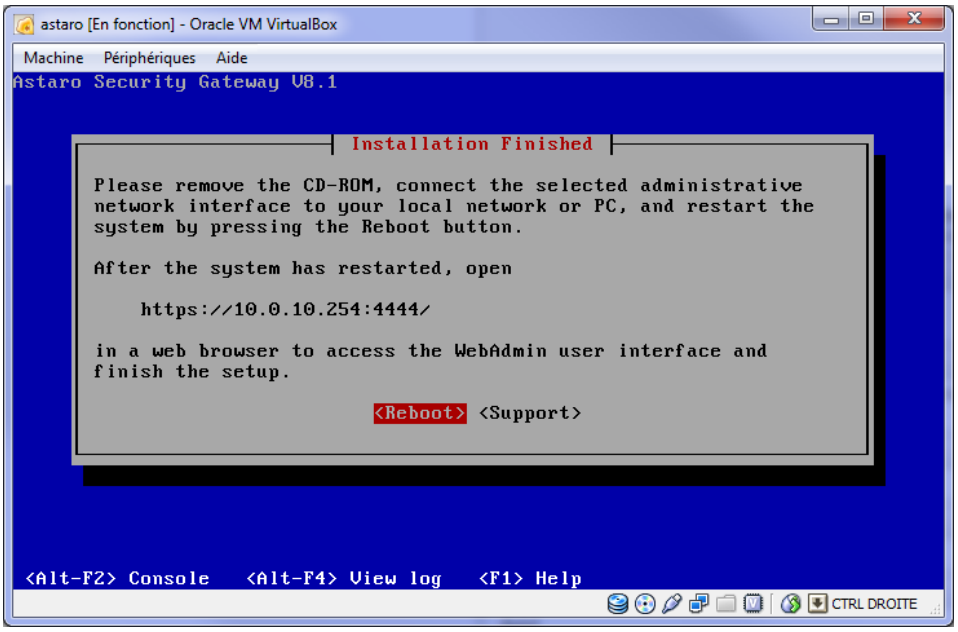
Voici les cahiers de charges de notre pare-feu :

- Verrouiller le pare-feu pour les accès entrant et sortant (hormis l'administration depuis le LAN)
- Pouvoir administrer le pare-feu depuis la station VM-3 (via « ssh » ou navigateur Web),
- Pourvoir surfer sur internet depuis le LAN,
- Faites en sortes que votre **station d'administration** (Poste LAN : VM-3) puisse **accéder aux partages CIFS (Windows) de la salle de cours**, aidez-vous des journaux pour prendre connaissances des ports à ouvrir,
- Effectuez un scan de port depuis votre station d'administration et consultez l'IDS(activez le d'abord) et les journaux de votre pare-feu : le scan a-t-il était détecté ?

Au choix :

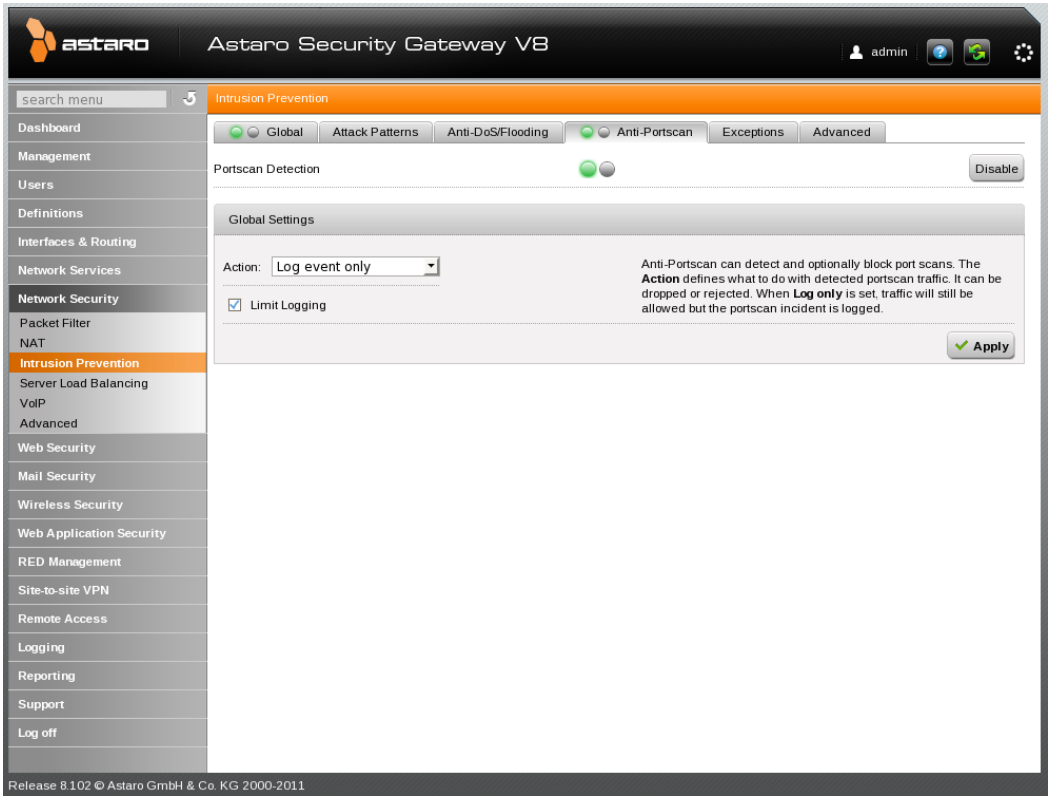
- Astaro (prendre un disque virtuel de 11Go),

  Installation sans aucune difficulté particulière. Il faut bien suivre les indications à l'écran. Donc soyez attentifs au moment de choisir vos interfaces WAN (externe)et LAN (Externe)

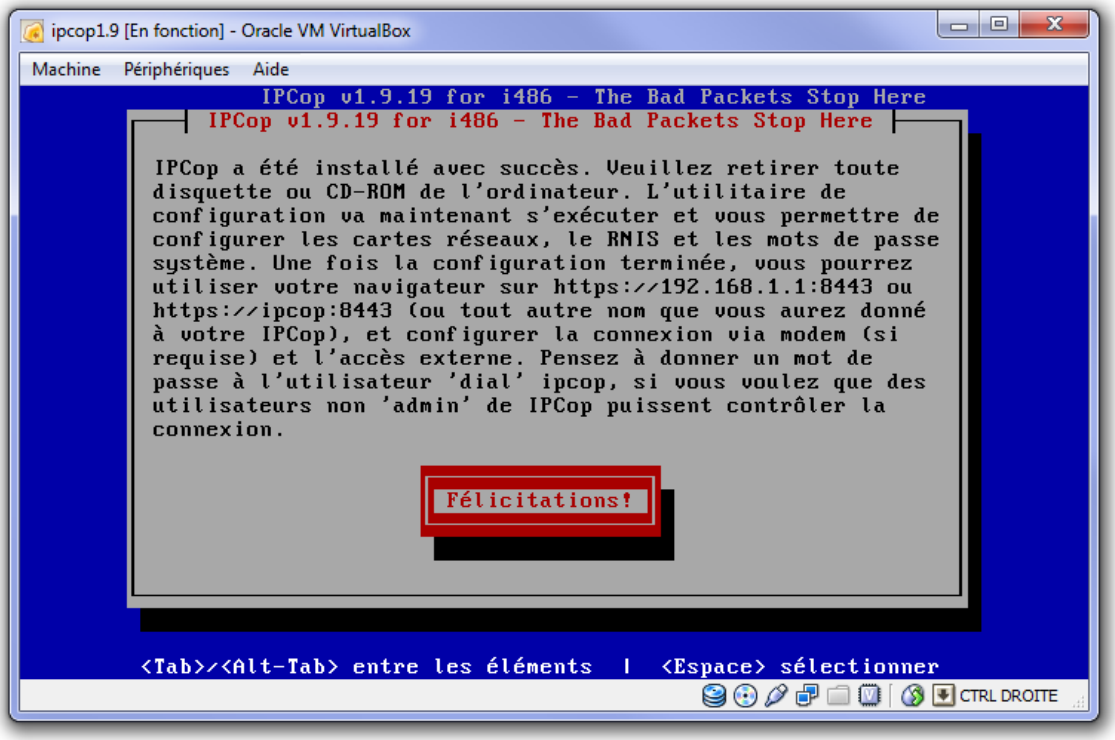


  Ensuite tout se passe sous une interface Web :

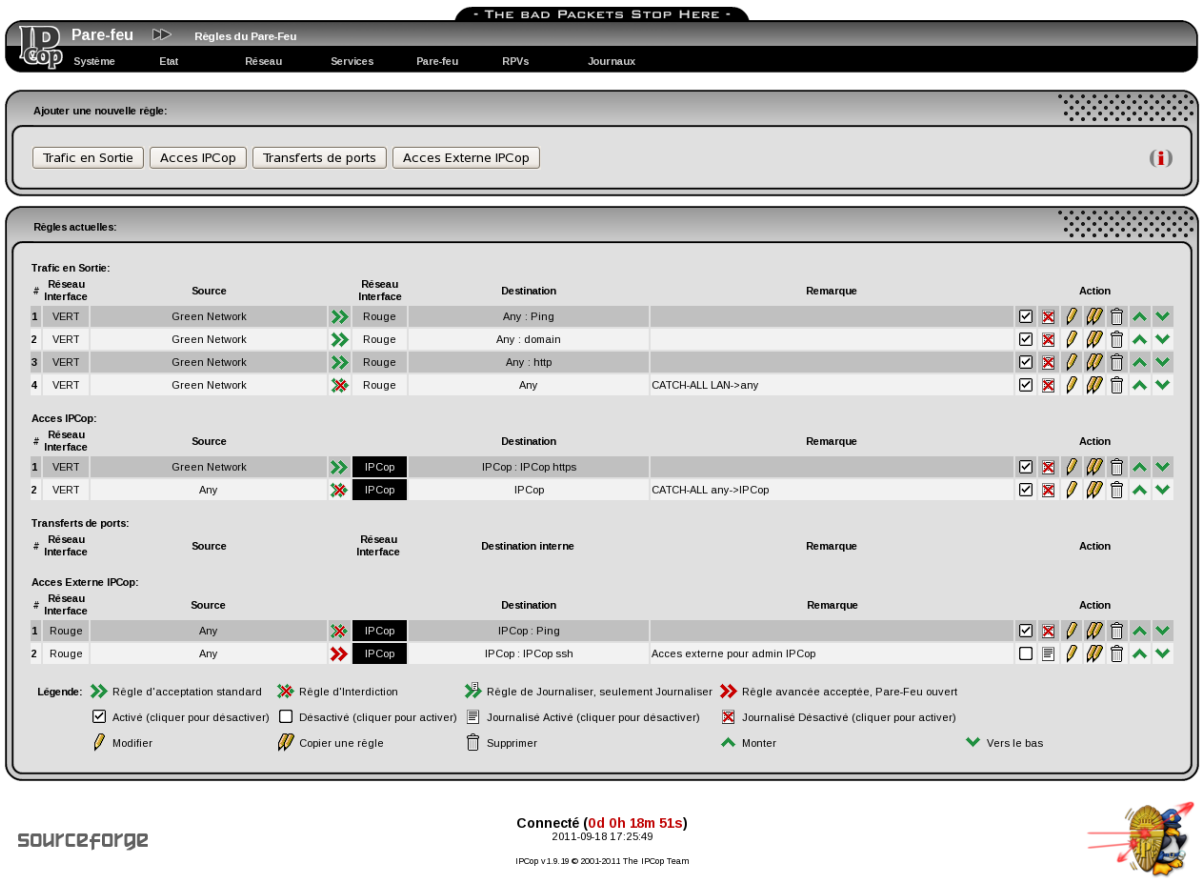
  Ex. : Port scan sur Astaro :



- ***IPCop 1.9 (ou IPCop 1.4 + Add-ons BOT)***,
  Installation sans aucune difficulté particulière. Comme pour Astaro il faut bien suivre les indications à l'écran. Donc soyez attentifs au moment de choisir vos interfaces GREEN et RED.



Ensuite tout se passe sous une interface Web :



http://www.ipcop.org/2.0.0/en/admin/html/

TP N°3 : Prise en main d'un pare-feu professionnel

Prise en main pare-feu professionnel : ZyWALL USG 100

https://<IP_ZYWALL>:443
user : stagiairex
password : wqazsx_2011

Naviguez dans :

- L'interface,
- Définition du rôle de chaque port Ethernet,
- Configuration du comportement de l'interface LAN1,
- Configuration d'un DNAT,
- Les flux de vos zones, combien sont présents par défaut ?,
- Les règles de filtrage : quelle est la politique par défaut de ce pare-feu ?,
- Les objets,
- Quels sont les modules fonctionnalités principales supplémentaires implémentées ?
- Les logs,

TP N°4 : PenTesting

Hacking, le PenTesting.

Testez la distribution Back TRACK 5 RC1 (mettez là en zone wan ou lan) pour évaluer la robustesse de votre pare-feu avec des attaques standards.

1. Effectuez une prise d'empreinte d'OS.
2. Faites plusieurs type de scan de port,
3. Votre pare-feu vous a-t-il détecté ?
4. Observez les journaux,
5. Cherchez d'éventuelles failles sur les ports ouverts.

ANNEXES

Sources, remerciements

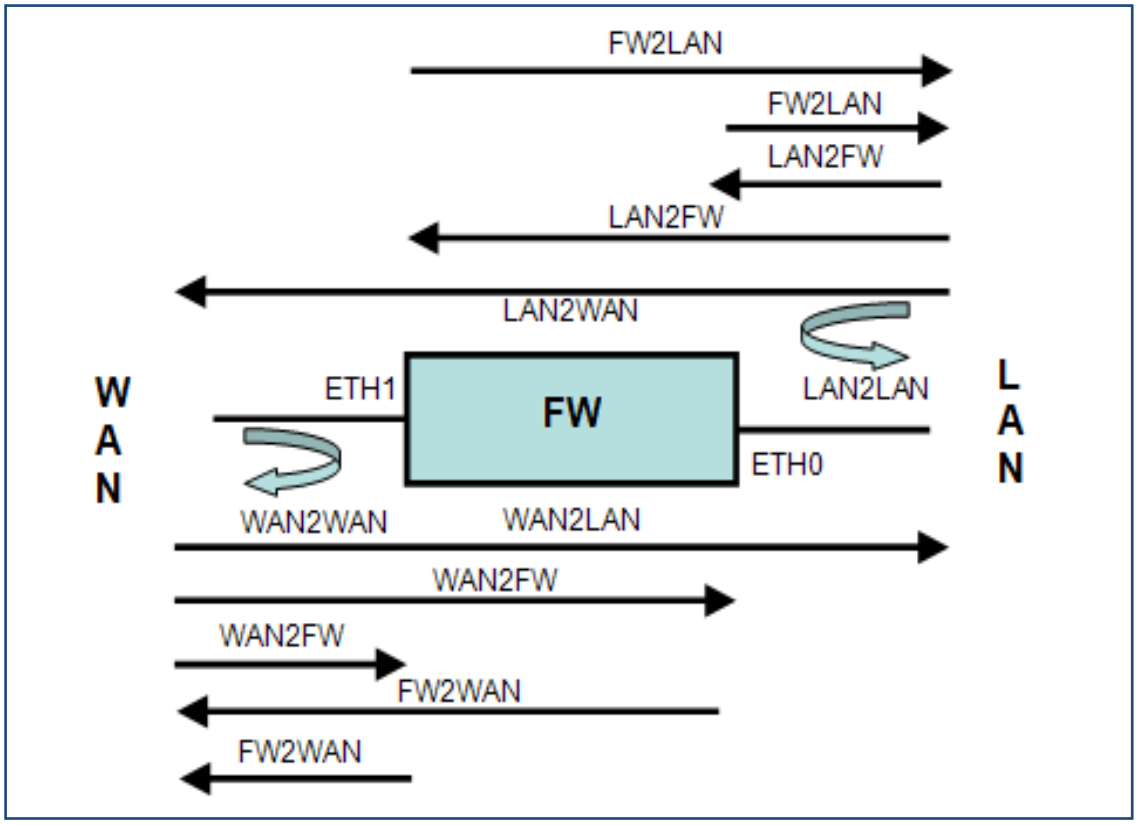
Ce cours s'appuie largement sur les connaissances gracieusement mis à disposition par les personnes et sites citées ci-dessous :

- Renaud BIDOU,
- Christian CALECA (depuis 2001 ce monsieur aide beaucoup ...),
- Diamond-editions (« Firewall votre meilleur ennemi acte I & II),
- Wikipédia,

Pare-feu multizone (les chaînes utilisateurs de Netfilter)

Largement inspiré du script de pare-feu de **R. DORIGNY**.

Flux en présence :



```
#!/bin/bash
# Mise en place du pare-feu
Nom_PareFeu=`hostname`
echo "Configuration des regles de filtrage de $Nom_PareFeu !"

# ##############################################################################
# Binaires utilises
IPT=/sbin/iptables
```

```
# ########################################################################
# Objets

# Objets : interfaces
if_lo="lo"          # interface loopback (interne au pare-feu)
if_wan="eth0"       # interface connectée à la zone WAN (externe)
if_lan="eth1"       # interface connectée à la zone LAN (interne)
#if_dmz="eth2"      # interface connectée à la zone DMZ (optionelle)

# Objets : reseaux
net_wan="dhcp/static" # ==> TODO récuperer depuis if_wan
net_lan="10.0.10.0/24"
#net_dmz="192.168.254.0/24"

# Objets : adresses IP
adr_parefeu_wan=`/sbin/ifconfig $if_wan | grep "inet adr" | awk -F: '{print $2}' | awk {'print $1}'`
adr_parefeu_lan=`/sbin/ifconfig $if_lan | grep "inet adr" | awk -F: '{print $2}' | awk {'print $1}'`
#adr parefeu dmz=`/sbin/ifconfig $if_dmz | grep "inet adr" | awk -F: '{print $2}' | awk {'print $1}'`
adr_any="0.0.0.0/0"
adr_station_admin="10.0.10.100/32"
adr_serveur_fichier="10.0.10.1/32"
adr_serveur_mail="10.0.10.2/32"
adr_serveur_dns_interne="10.0.10.3/32"
adr_serveur_dns_externe_1="212.27.40.240"
adr_serveur_proxy="10.0.10.3/32"
#adr_serveur_ntp="ntp"
# Etc.

# Objets : flux
# Création des chaines UTILISATEURS dans le table FILTER
# Trafic LAN vers any
$IPT -t filter -N LAN_to_WAN
 #$IPT -t filter -N LAN_to_DMZ
$IPT -t filter -N LAN_to_LAN
$IPT -t filter -N LAN_to_FW
# Trafic WAN vers any
$IPT -t filter -N WAN_to_LAN
 #$IPT -t filter -N WAN_to_DMZ
$IPT -t filter -N WAN_to_WAN
$IPT -t filter -N WAN_to_FW
# Trafic du pare-feu vers any
$IPT -t filter -N FW_to_LAN
$IPT -t filter -N FW_to_WAN
 #$IPT -t filter -N FW_to_DMZ
$IPT -t filter -N FW_to_FW
# Trafic ICMP (Ping)
$IPT -t filter -N ICMP-ACC
$IPT -t filter -N ICMP-FIL

# Objets : journalisation
# On cree la chaine utilisateur de journalisation des paquets rejetes
#$IPT -X LOG_DROP
$IPT -N LOG_DROP
$IPT -A LOG_DROP -j LOG --log-prefix  'NF PACKET DROP ==>' --log-level info # On
journalise le paquet indesirable
$IPT -A LOG_DROP -j DROP # On DROP le paquet apres l'avoir journalise
# Dans le même esprit on peut creer la chaine utilisateur de journalisation des paquets
acceptes
#$IPT -X LOG_ACCEPT
$IPT -N LOG_ACCEPT
$IPT -A LOG_ACCEPT -j LOG --log-prefix  'NF PACKET ACCEPT ==>' --log-level info # On
journalise le paquet desirable
$IPT -A LOG_ACCEPT -j ACCEPT # On ACCEPT le paquet apres l'avoir journalise
```

```
# ########################################################################
# INITIALISATION du pare-feu
```

```
# Mise en place de la politique de filtrage par defaut :
# On remet tout efface les chaines et DROP tout paquets IP.
# Intialisation : Effacement de toutes les regles dans toutes les chaines (tables
filter, nat et mangle) : -F
$IPT -t filter -F
$IPT -t nat -F
$IPT -t mangle -F
# Intialisation : Effacement de toutes les regles dans toutes les chaines utilisateurs
(tables filter, nat et mangle) : -X
$IPT -t filter -X
$IPT -t nat -X
$IPT -t mangle -X
# Intialisation : Definition de la politique de filtrage par defaut (-P) des chaines de
la table "filter"
# on "DROP" tous les paquets traversant (FORWARD), à destination (INPUT) ou sortant
(OUTPUT) du pare-feu.
$IPT -t filter -P FORWARD DROP
$IPT -t filter -P INPUT DROP
$IPT -t filter -P OUTPUT DROP
# Intialisation : Definition de la politique de translation d'adresse par defaut des
chaines de la table "nat"
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT
# Intialisation : Definition de la politique de marquage des paquets par defaut des
chaines de la table "mangle"
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P FORWARD ACCEPT
$IPT -t mangle -P INPUT ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT
$IPT -t mangle -P POSTROUTING ACCEPT
# Intialisation : Mise en place des redirections des flux vers les chaines UTILISATEURS
gérées (les jumps)
# LAN_to_any ($res_lan)
iptables -t filter -A FORWARD -s $res_lan -d $res_lan -i $if_lan -o $if_lan -j LAN_to_LAN
#iptables -t filter -A FORWARD -s $res_lan -d  $res_dmz -i $if_lan -o $if_dmz -j LAN_to_DMZ
iptables -t filter -A FORWARD -s $res_lan -d ! $res_lan -i $if_lan -o $if_wan -j LAN_to_WAN
iptables -t filter -A INPUT -s $res_lan -d $adr_parefeu_lan -i $if_lan -j LAN_to_FW
# WAN_to_any (! $res_lan)
iptables -t filter -A FORWARD -s ! $res_lan -d $res_lan -i $if_wan -o $if_lan -j WAN_to_LAN
#iptables -t filter -A FORWARD -s ! $res_lan -d  $res_dmz -i $if_wan -o $if_dmz -j WAN_to_DMZ
iptables -t filter -A FORWARD -s ! $res_lan -d ! $res_lan -i $if_wan -o $if_wan -j WAN_to_WAN
iptables -t filter -A INPUT -s ! $res_lan -d $adr_parefeu_wan -i $if_wan -j WAN_to_FW
# FW_to_any ($adr_parefeu_wan ou lan)
iptables -t filter -A OUTPUT -d $res_lan -o $if_lan -j FW_to_LAN
#iptables -t filter -A FORWARD -s $res_lan -d  $res_dmz -i $if_lan -o $if_dmz -j FW_to_DMZ
iptables -t filter -A OUTPUT -d ! $res_lan -o $if_wan -j FW_to_WAN
iptables -t filter -A INPUT -i $if_lo -j FW_to_FW
iptables -t filter -A OUTPUT -o $if_lo -j FW_to_FW
```

```
# ######################################################################
# GESTION DES FLUX

# Flux : Broadcast
########################################################################
#Chaîne FORWARD
#LAN
$IPT -A FORWARD -d 10.0.10.255/32 -j DROP
#DMZ
#$IPT -A FORWARD -d 192.168.254.255/32 -j DROP
#ANY
$IPT -A FORWARD -d 255.255.255.255/32 -j DROP
#Chaîne INPUT
#LAN
$IPT -A INPUT -d 10.0.10.255/32 -j DROP
#DMZ
#$IPT -A INPUT -d 192.168.254.255/32 -j DROP
#ANY
$IPT -A INPUT -d 255.255.255.255/32 -j DROP
#Chaîne OUTPUT
#LAN
$IPT -A OUTPUT -d 10.0.10.255/32 -j DROP
#DMZ
#$IPT -A OUTPUT -d 192.168.254.255/32 -j DROP
#ANY
$IPT -A OUTPUT -d 255.255.255.255/32 -j DROP

# Flux : liste noire
# ######################################################################
#Black_list="IP1 IP2 IP3 ..."
#for ipBlack in $Black_list;
#do
#  $IPT -A INPUT -s $ipBlack -j LOG_DROP
#  $IPT -A OUTPUT -d $ipBlack -j LOG_DROP
#  $IPT -A FORWARD -d $ipBlack -j LOG_DROP
#  $IPT -A FORWARD -s $ipBlack -j LOG_DROP
#done

# Flux : ICMP
# ######################################################################
echo "Flux : ICMP"
# Acceptation du protocole ICMP (chaine ICMP-ACC)
iptables -A ICMP-ACC -p icmp -j ACCEPT

# Acceptation fine du protocole ICMP (chaine ICMP-FIL)
#echo-reply
#iptables -A ICMP-FIL -p icmp --icmp-type 0 -j LOGDROP
iptables -A ICMP-FIL -p icmp --icmp-type 0 -j ACCEPT
#destination-unreachable
iptables -A ICMP-FIL -p icmp --icmp-type 3 -j ACCEPT
#source-quench
iptables -A ICMP-FIL -p icmp --icmp-type 4 -j ACCEPT
#echo-request
#iptables -A ICMP-FIL -p icmp --icmp-type 8 -j LOGDROP
iptables -A ICMP-FIL -p icmp --icmp-type 8 -j ACCEPT
#Time-exceed
iptables -A ICMP-FIL -p icmp --icmp-type 11 -j ACCEPT
#Parameter-problem
iptables -A ICMP-FIL -p icmp --icmp-type 12 -j ACCEPT

#source ./zones/FW_to_any.sh #TODO avec des zones denses en terme de règles
# Flux : FW_to_FW (loopback)
########################################################################
echo "Flux : FW -> FW (loopback)"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A FW_to_FW -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A FW_to_FW -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

$IPT -A FW_to_FW -p all -j ACCEPT

# Flux : FW_to_LAN
################################################################################
echo "Flux : FW -> LAN"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A FW_to_LAN -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FW_to_LAN -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

#Protocole : ICMP
iptables -A FW_to_LAN -p icmp -j ICMP-FIL

# Journalisation + CATCH-ALL des paquets INVALID
iptables -A FW_to_LAN -j LOG_DROP

# Flux : FW_to_WAN
################################################################################
echo "Flux : FW -> WAN"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A FW_to_WAN -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FW_to_WAN -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT
#Protocole ICMP
iptables -A FW_to_WAN -p icmp -j ICMP-FIL

# Journalisation + CATCH-ALL des paquets INVALID
iptables -A FW_to_WAN -j LOG_DROP

#source ./zones/LAN_to_any.sh #TODO avec des zones denses en terme de règles
# Flux : LAN_to_WAN
################################################################################
echo "Flux : LAN -> WAN"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A LAN_to_WAN -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A LAN_to_WAN -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

# Protocole : SSH
iptables -A LAN_to_WAN -p TCP --dport 22 --sport 1024:65535 -m state --state NEW -j ACCEPT
# Protocole : NNTP
iptables -A LAN_to_WAN -p TCP --dport 119 --sport 1024:65535 -m state --state NEW -j ACCEPT
# Protocole : HTTP
iptables -A LAN_to_WAN -p TCP --dport 80 --sport 1024:65535 -m state --state NEW -j ACCEPT
# Protocole : FTP et FTP-DATA (requetes et reponses sortantes)
#Connexions serveurs FTP
iptables -A LAN_to_WAN -p tcp -m state --state NEW --dport 21 -j ACCEPT
iptables -A LAN_to_WAN -p tcp -m state --state RELATED --sport 20 -j ACCEPT
#pour le mode ftp-passif
iptables -A LAN_to_WAN -p tcp -m state --state RELATED --dport 1024:65535 --sport 1024:65535 -j ACCEPT
#Protocole : ICMP
iptables -A LAN_to_WAN -p icmp -j ICMP-FIL

# Journalisation + CATCH-ALL des paquets INVALID
iptables -A LAN_to_WAN -j LOG_DROP

# Flux : LAN_to_LAN
################################################################################
echo "Flux : LAN_to_LAN"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A LAN_to_LAN -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A LAN_to_LAN -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

#Protocole ICMP
iptables -A LAN_to_LAN -p icmp -j ICMP-FIL

# Journalisation + CATCH-ALL des paquets INVALID
```

```
iptables -A LAN_to_LAN -j LOG_DROP

# Flux : LAN_to_FW
################################################################################
echo "Flux : LAN_to_FW"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A LAN_to_FW -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A LAN_to_FW -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

#Protocole ICMP
iptables -A LAN_to_FW -p icmp -j ICMP-FIL

# Journalisation + CATCH-ALL des paquets INVALID
iptables -A LAN_to_FW -j LOG_DROP

#source ./zones/WAN_to_any.sh #TODO avec des zones denses en terme de règles
# Flux : WAN_to_LAN
################################################################################
echo "Flux : WAN -> LAN"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A WAN_to_LAN -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A WAN_to_LAN -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

#Protocole : ICMP
iptables -A WAN_to_LAN -p icmp -j ICMP-FIL

# Journalisation + CATCH-ALL des paquets INVALID
iptables -A WAN_to_LAN -j LOG_DROP

# Flux : WAN_to_WAN
################################################################################
echo "Flux : WAN -> WAN"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A WAN_to_WAN -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A WAN_to_WAN -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT

# Journalisation + CATCH-ALL des paquets INVALID
iptables -A WAN_to_WAN -j LOG_DROP

# Flux : WAN_to_FW
################################################################################
echo "Flux : WAN -> FW"
# Mise en place du SPI (RELATED, ESTABLISHED)
iptables -A WAN_to_FW -p TCP -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A WAN_to_FW -p UDP -m state --state RELATED,ESTABLISHED -j ACCEPT
#Protocole ICMP
iptables -A WAN_to_FW -p icmp -j ICMP-FIL

# Journalisation + CATCH-ALL des paquets INVALID
iptables -A WAN_to_FW -j LOG_DROP

#source ./zones/Unknow.sh #TODO avec des zones denses en terme de règles
# Flux : Inconnu
################################################################################
# On logue les paquets indesirables
# Mise en place : sans chaine utilisateur + /etc/syslog.conf ==>kern.=info
/var/log/iptables.log + service syslogd restart
$IPT -t filter -A FORWARD -j LOG --log-prefix 'FORWARD_PKTS_DROP ==> ' --log-level info
$IPT -t filter -A INPUT -j LOG --log-prefix 'INPUT_PKTS_DROP ==> ' --log-level info
$IPT -t filter -A OUTPUT -j LOG --log-prefix 'OUTPUT_PKTS_DROP ==> ' --log-level info


#source ./nat/NAT.sh #TODO avec des zones denses en terme de règles
# Flux : Translation d'adresse (NAT)
$IPT -t nat -A POSTROUTING -o $if_wan -j MASQUERADE
# Note : en general seul le serveur proxy est SNATter, pas les stations clientes,
```

```
# mais comme nous ne montons pas de PROXY

#source ./marquage/MANGLE.sh #TODO avec des zones denses en terme de règles
# Flux : Marquage de paquet (MANGLE)

# CATCH-ALL", au cas ou l'on passe à travers la chaine utilisateur "LOG_DROP"
# on "DROP" tous les paquets.
$IPT -t filter -A FORWARD -j DROP
$IPT -t filter -A INPUT -j DROP
$IPT -t filter -A OUTPUT -j DROP
```

List of TCP and UDP port numbers

From Wikipedia, the free encyclopedia
Jump to: navigation, search

This is a list of Internet socket port numbers used by protocols of the Transport Layer of the Internet Protocol Suite for the establishment of host-to-host communications.

Originally, these port numbers were used by the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), but are used also for the Stream Control Transmission Protocol (SCTP), and the Datagram Congestion Control Protocol (DCCP). SCTP and DCCP services usually use a port number that matches the service of the corresponding TCP or UDP implementation if they exist. The Internet Assigned Numbers Authority (IANA) is responsible for maintaining the official assignments of port numbers for specific uses.[1] However, many unofficial uses of both well-known and registered port numbers occur in practice.

Contents

Table legend

Color coding of table entries

Official	Port/application combination is registered with IANA
Unofficial	Port/application combination is **not** registered with IANA
Conflict	Port is in use for multiple applications (may be official or unofficial)

Well-known ports: 0–1023

The port numbers in the range from 0 to 1023 are the *well-known ports*. They are used by system processes that provide widely-used types of network services. On Unix-like operating systems, a process must execute with superuser privileges to be able to bind a network socket to an IP address using one of the well-known ports.

Port	TCP	UDP	Description	Status
0		UDP	Reserved	Official
1	TCP	UDP	TCP Port Service Multiplexer (TCPMUX)	Official
2	TCP	UDP	CompressNET[2] Management Utility[3]	Official
3	TCP	UDP	CompressNET[2] Compression Process[4]	Official
4	TCP	UDP	Unassigned	Official
5	TCP	UDP	Remote Job Entry	Official
6	TCP	UDP	Unassigned	Official

7	TCP	UDP	Echo Protocol	Official
8	TCP	UDP	Unassigned	Official
9	TCP	UDP	Discard Protocol	Official
10	TCP	UDP	Unassigned	Official
11	TCP	UDP	Active Users (systat service)[5][6]	Official
12	TCP	UDP	Unassigned	Official
13	TCP	UDP	Daytime Protocol (RFC 867)	Official
14	TCP	UDP	Unassigned	Official
15	TCP	UDP	netstat service[5]	Unofficial
16	TCP	UDP	Unassigned	Official
17	TCP	UDP	Quote of the Day	Official
18	TCP	UDP	Message Send Protocol	Official
19	TCP	UDP	Character Generator Protocol (CHARGEN)	Official
20	TCP		FTP—data transfer	Official
21	TCP		FTP—control (command)	Official
22	TCP	UDP	Secure Shell (SSH)—used for secure logins, file transfers (scp, sftp) and port forwarding	Official
23	TCP		Telnet protocol—unencrypted text communications	Official
24	TCP	UDP	Priv-mail : any private mail system.	Official
25	TCP		Simple Mail Transfer Protocol (SMTP)—used for e-mail routing between mail servers	Official
26	TCP	UDP	Unassigned	Official
27	TCP	UDP	NSW User System FE	Official
34	TCP	UDP	Remote File (RF)—used to transfer files between machines	Unofficial
35	TCP	UDP	Any private printer server protocol	Official
37	TCP	UDP	TIME protocol	Official
39	TCP	UDP	Resource Location Protocol[7] (RLP)—used for determining the location of higher level services from hosts on a network	Official
40	TCP	UDP	Unassigned	Official
41	TCP	UDP	Graphics	Official
42	TCP	UDP	nameserver, ARPA Host Name Server Protocol	Official
42	TCP	UDP	WINS	Unofficial
43	TCP		WHOIS protocol	Official
47	TCP	UDP	NI FTP[7]	Official
49	TCP	UDP	TACACS Login Host protocol	Official
50	TCP	UDP	Remote Mail Checking Protocol[8]	Official
51	TCP	UDP	IMP Logical Address Maintenance	Official
52	TCP	UDP	XNS (Xerox Network Systems) Time Protocol	Official
53	TCP	UDP	Domain Name System (DNS)	Official
54	TCP	UDP	XNS (Xerox Network Systems) Clearinghouse	Official
55	TCP	UDP	ISI Graphics Language (ISI-GL)	Official
56	TCP	UDP	XNS (Xerox Network Systems) Authentication	Official
56	TCP	UDP	Route Access Protocol (RAP)[9]	Unofficial
57	TCP		Mail Transfer Protocol (MTP)	Unofficial
58	TCP	UDP	XNS (Xerox Network Systems) Mail	Official
67		UDP	Bootstrap Protocol (BOOTP) Server; also used by Dynamic Host Configuration Protocol (DHCP)	Official
68		UDP	Bootstrap Protocol (BOOTP) Client; also used by Dynamic Host Configuration Protocol (DHCP)	Official
69		UDP	Trivial File Transfer Protocol (TFTP)	Official

70	TCP		Gopher protocol	Official
71	TCP		NETRJS protocol	Official
72	TCP		NETRJS protocol	Official
73	TCP		NETRJS protocol	Official
74	TCP		NETRJS protocol	Official
79	TCP		Finger protocol	Official
80	TCP	UDP	Hypertext Transfer Protocol (HTTP)	Official
81	TCP		Torpark—Onion routing	Unofficial
82		UDP	Torpark—Control	Unofficial
83	TCP		MIT ML Device	Official
88	TCP	UDP	Kerberos—authentication system	Official
90	TCP	UDP	dnsix (DoD Network Security for Information Exchange) Securit Attribute Token Map	Official
90	TCP	UDP	Pointcast	Unofficial
99	TCP		WIP Message Protocol	Unofficial
101	TCP		NIC host name	Official
102	TCP		ISO-TSAP (Transport Service Access Point) Class 0 protocol[10]	Official
104	TCP	UDP	ACR/NEMA Digital Imaging and Communications in Medicine	Official
105	TCP	UDP	CCSO Nameserver Protocol (Qi/Ph)	Official
107	TCP		Remote TELNET Service[11] protocol	Official
108	TCP	UDP	SNA Gateway Access Server [12]	Official
109	TCP		Post Office Protocol v2 (POP2)	Official
110	TCP		Post Office Protocol v3 (POP3)	Official
111	TCP	UDP	ONC RPC (SunRPC)	Official
113	TCP		ident—Authentication Service/Identification Protocol,[13] used by IRC servers to identify users	Official
113		UDP	Authentication Service[13] (auth)	Official
115	TCP		Simple File Transfer Protocol (SFTP)	Official
117	TCP		UUCP Path Service	Official
118	TCP	UDP	SQL (Structured Query Language) Services	Official
119	TCP		Network News Transfer Protocol (NNTP)—retrieval of newsgroup messages	Official
123		UDP	Network Time Protocol (NTP)—used for time synchronization	Official
135	TCP	UDP	DCE endpoint resolution	Official
135	TCP	UDP	Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service,[14] used to remotely manage services including DHCP server, DNS server and WINS. Also used by DCOM	Unofficial
137	TCP	UDP	NetBIOS NetBIOS Name Service	Official
138	TCP	UDP	NetBIOS NetBIOS Datagram Service	Official
139	TCP	UDP	NetBIOS NetBIOS Session Service	Official
143	TCP		Internet Message Access Protocol (IMAP)—management of email messages	Official
152	TCP	UDP	Background File Transfer Program (BFTP)[15]	Official
153	TCP	UDP	SGMP, Simple Gateway Monitoring Protocol	Official
156	TCP	UDP	SQL Service	Official
158	TCP	UDP	DMSP, Distributed Mail Service Protocol[16]	Unofficial
161		UDP	Simple Network Management Protocol (SNMP)	Official
162	TCP	UDP	Simple Network Management Protocol Trap (SNMPTRAP)[17]	Official
170	TCP		Print-srv, Network PostScript	Official
175	TCP		VMNET (IBM z/VM, z/OS & z/VSE - Network Job Entry(NJE))	Official

177	TCP	UDP	X Display Manager Control Protocol (XDMCP)	Official
179	TCP		BGP (Border Gateway Protocol)	Official
194	TCP	UDP	Internet Relay Chat (IRC)	Official
199	TCP	UDP	SMUX, SNMP Unix Multiplexer	Official
201	TCP	UDP	AppleTalk Routing Maintenance	Official
209	TCP	UDP	The Quick Mail Transfer Protocol	Official
210	TCP	UDP	ANSI Z39.50	Official
213	TCP	UDP	Internetwork Packet Exchange (IPX)	Official
218	TCP	UDP	Message posting protocol (MPP)	Official
220	TCP	UDP	Internet Message Access Protocol (IMAP), version 3	Official
256	TCP	UDP	2DEV "2SP" Port	Unofficial
259	TCP	UDP	ESRO, Efficient Short Remote Operations	Official
264	TCP	UDP	BGMP, Border Gateway Multicast Protocol	Official
280	TCP	UDP	http-mgmt	Official
308	TCP		Novastor Online Backup	Official
311	TCP		Mac OS X Server Admin (officially AppleShare IP Web administration)	Official
318	TCP	UDP	PKIX TSP, Time Stamp Protocol	Official
319		UDP	Precision time protocol event messages	Official
320		UDP	Precision time protocol general messages	Official
323	TCP	UDP	IMMP, Internet Message Mapping Protocol	Unofficial
350	TCP	UDP	MATIP-Type A, Mapping of Airline Traffic over Internet Protocol	Official
351	TCP	UDP	MATIP-Type B, Mapping of Airline Traffic over Internet Protocol	Official
366	TCP	UDP	ODMR, On-Demand Mail Relay	Official
369	TCP	UDP	Rpc2portmap	Official
370	TCP		codaauth2—Coda authentication server	Official
370		UDP	codaauth2—Coda authentication server	Official
370		UDP	securecast1—Outgoing packets to NAI's servers [18][*dead link*]	Unofficial
371	TCP	UDP	ClearCase albd	Official
383	TCP	UDP	HP data alarm manager	Official
384	TCP	UDP	A Remote Network Server System	Official
387	TCP	UDP	AURP, AppleTalk Update-based Routing Protocol[19]	Official
389	TCP	UDP	Lightweight Directory Access Protocol (LDAP)	Official
401	TCP	UDP	UPS Uninterruptible Power Supply	Official
402	TCP		Altiris, Altiris Deployment Client	Unofficial
411	TCP		Direct Connect Hub	Unofficial
412	TCP		Direct Connect Client-to-Client	Unofficial
427	TCP	UDP	Service Location Protocol (SLP)	Official
443	TCP		HTTPS (Hypertext Transfer Protocol over SSL/TLS)	Official
444	TCP	UDP	SNPP, Simple Network Paging Protocol (RFC 1568)	Official
445	TCP		Microsoft-DS Active Directory, Windows shares	Official
445	TCP		Microsoft-DS SMB file sharing	Official
464	TCP	UDP	Kerberos Change/Set password	Official
465	TCP		Cisco protocol	Unofficial
465	TCP		SMTP over SSL	Unofficial
475	TCP	UDP	tcpnethaspsrv (Aladdin Knowledge Systems Hasp services, TCP/IP version)	Official
497	TCP		Dantz Retrospect	Official
500		UDP	Internet Security Association and Key Management Protocol (ISAKMP)	Official
501	TCP		STMF, Simple Transportation Management Framework—DOT NTCIP 1101	Unofficial

502	TCP	UDP	asa-appl-proto, Protocol	Unofficial
502	TCP	UDP	Modbus, Protocol	Unofficial
504	TCP	UDP	Citadel—multiservice protocol for dedicated clients for the Citadel groupware system	Official
510	TCP		First Class Protocol	Unofficial
512	TCP		Rexec, Remote Process Execution	Official
512		UDP	comsat, together with biff	Official
513	TCP		rlogin	Official
513		UDP	Who	Official
514	TCP		Shell—used to execute non-interactive commands on a remote system (Remote Shell, rsh, remsh)	Official
514		UDP	Syslog—used for system logging	Official
515	TCP		Line Printer Daemon—print service	Official
517		UDP	Talk	Official
518		UDP	NTalk	Official
520	TCP		efs, extended file name server	Official
520		UDP	Routing Information Protocol (RIP)	Official
524	TCP	UDP	NetWare Core Protocol (NCP) is used for a variety things such as access to primary NetWare server resources, Time Synchronization, etc.	Official
525		UDP	Timed, Timeserver	Official
530	TCP	UDP	RPC	Official
531	TCP	UDP	AOL Instant Messenger, IRC	Unofficial
532	TCP		netnews	Official
533		UDP	netwall, For Emergency Broadcasts	Official
540	TCP		UUCP (Unix-to-Unix Copy Protocol)	Official
542	TCP	UDP	commerce (Commerce Applications)	Official
543	TCP		klogin, Kerberos login	Official
544	TCP		kshell, Kerberos Remote shell	Official
545	TCP		OSIsoft PI (VMS), OSISoft PI Server Client Access	Unofficial
546	TCP	UDP	DHCPv6 client	Official
547	TCP	UDP	DHCPv6 server	Official
548	TCP		Apple Filing Protocol (AFP) over TCP	Official
550		UDP	new-rwho, new-who	Official
554	TCP	UDP	Real Time Streaming Protocol (RTSP)	Official
556	TCP		Remotefs, RFS, rfs_server	Official
560		UDP	rmonitor, Remote Monitor	Official
561		UDP	monitor	Official
563	TCP	UDP	NNTP protocol over TLS/SSL (NNTPS)	Official
587	TCP		e-mail message submission[20] (SMTP)	Official
591	TCP		FileMaker 6.0 (and later) Web Sharing (HTTP Alternate, also see port 80)	Official
593	TCP	UDP	HTTP RPC Ep Map, Remote procedure call over Hypertext Transfer Protocol, often used by Distributed Component Object Model services and Microsoft Exchange Server	Official
604	TCP		TUNNEL profile,[21] a protocol for BEEP peers to form an application layer tunnel	Official
623		UDP	ASF Remote Management and Control Protocol (ASF-RMCP)	Official
631	TCP	UDP	Internet Printing Protocol (IPP)	Official
631	TCP	UDP	Common Unix Printing System (CUPS)	Unofficial
635	TCP	UDP	RLZ DBase	Official
636	TCP	UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	Official

639	TCP	UDP	MSDP, Multicast Source Discovery Protocol	Official
641	TCP	UDP	SupportSoft Nexus Remote Command (control/listening): A proxy gateway connecting remote control traffic	Official
646	TCP	UDP	LDP, Label Distribution Protocol, a routing protocol used in MPLS networks	Official
647	TCP		DHCP Failover protocol[22]	Official
648	TCP		RRP (Registry Registrar Protocol)[23]	Official
651	TCP	UDP	IEEE-MMS	Official
652	TCP		DTCP, Dynamic Tunnel Configuration Protocol	Unofficial
653	TCP	UDP	SupportSoft Nexus Remote Command (data): A proxy gateway connecting remote control traffic	Official
654	TCP		Media Management System (MMS) Media Management Protocol (MMP)[24]	Official
657	TCP	UDP	IBM RMC (Remote monitoring and Control) protocol, used by System p5 AIX Integrated Virtualization Manager (IVM)[25] and Hardware Management Console to connect managed logical partitions (LPAR) to enable dynamic partition reconfiguration	Official
660	TCP		Mac OS X Server administration	Official
665	TCP		sun-dr, Remote Dynamic Reconfiguration	Unofficial
666		UDP	Doom, first online first-person shooter	Official
674	TCP		ACAP (Application Configuration Access Protocol)	Official
691	TCP		MS Exchange Routing	Official
692	TCP		Hyperwave-ISP	Official
694	TCP	UDP	Linux-HA High availability Heartbeat	Official
695	TCP		IEEE-MMS-SSL (IEEE Media Management System over SSL)[26]	Official
698		UDP	OLSR (Optimized Link State Routing)	Official
699	TCP		Access Network	Official
700	TCP		EPP (Extensible Provisioning Protocol), a protocol for communication between domain name registries and registrars (RFC 5734)	Official
701	TCP		LMP (Link Management Protocol (Internet)),[27] a protocol that runs between a pair of nodes and is used to manage traffic engineering (TE) links	Official
702	TCP		IRIS[28][29] (Internet Registry Information Service) over BEEP (Blocks Extensible Exchange Protocol)[30] (RFC 3983)	Official
706	TCP		Secure Internet Live Conferencing (SILC)	Official
711	TCP		Cisco Tag Distribution Protocol[31][32][33]—being replaced by the MPLS Label Distribution Protocol[34]	Official
712	TCP		Topology Broadcast based on Reverse-Path Forwarding routing protocol (TBRPF) (RFC 3684)	Official
712		UDP	Promise RAID Controller	Unofficial
720	TCP		SMQP, Simple Message Queue Protocol	Unofficial
749	TCP	UDP	Kerberos (protocol) administration	Official
750	TCP		rfile	Official
750		UDP	loadav	Official
750		UDP	kerberos-iv, Kerberos version IV	Official
751	TCP	UDP	pump	Official
751	TCP	UDP	kerberos_master, Kerberos authentication	Unofficial
752	TCP		qrh	Official
752		UDP	qrh	Official
752		UDP	passwd_server, Kerberos Password (kpasswd) server	Unofficial
753	TCP		Reverse Routing Header (rrh)[35]	Official

753		UDP	Reverse Routing Header (rrh)	Official
753		UDP	userreg_server, Kerberos userreg server	Unofficial
754	TCP		tell send	Official
754	TCP		krb5_prop, Kerberos v5 slave propagation	Unofficial
754		UDP	tell send	Official
760	TCP	UDP	ns	Official
760	TCP	UDP	krbupdate [kreg], Kerberos registration	Unofficial
782	TCP		Conserver serial-console management server	Unofficial
783	TCP		SpamAssassin spamd daemon	Unofficial
829	TCP		CMP (Certificate Management Protocol)	Unofficial
843	TCP		Adobe Flash socket policy server	Unofficial
847	TCP		DHCP Failover protocol	Official
848	TCP	UDP	Group Domain Of Interpretation (GDOI) protocol	Official
860	TCP		iSCSI (RFC 3720)	Official
873	TCP		rsync file synchronisation protocol	Official USA only
888	TCP		cddbp, CD DataBase (CDDB) protocol (CDDBP)—unassigned but widespread use	Unofficial
901	TCP		Samba Web Administration Tool (SWAT)	Unofficial
901	TCP		VMware Virtual Infrastructure Client (UDP from server being managed to management console)	Unofficial
901		UDP	VMware Virtual Infrastructure Client (UDP from server being managed to management console)	Unofficial
902	TCP		ideafarm-door 902/tcp self documenting Door: send 0x00 for info	Official
902	TCP		VMware Server Console (TCP from management console to server being Managed)	Unofficial
902		UDP	ideafarm-door	Official
902		UDP	VMware Server Console (UDP from server being managed to management console)	Unofficial
903	TCP		VMware Remote Console [36]	Unofficial
904	TCP		VMware Server Alternate (if 902 is in use, i.e. SUSE linux)	Unofficial
911	TCP		Network Console on Acid (NCA)—local tty redirection over OpenSSH	Unofficial
953	TCP	UDP	Domain Name System (DNS) RNDC Service	Unofficial
981	TCP		SofaWare Technologies Remote HTTPS management for firewall devices running embedded Check Point FireWall-1 software	Unofficial
987	TCP		Microsoft This Secure Hypertext Transfer Protocol (HTTPS) port makes Windows SharePoint Services viewable through Remote Web Workplace	Unofficial
989	TCP	UDP	FTPS Protocol (data): FTP over TLS/SSL	Official
990	TCP	UDP	FTPS Protocol (control): FTP over TLS/SSL	Official
991	TCP	UDP	NAS (Netnews Administration System)	Official
992	TCP	UDP	TELNET protocol over TLS/SSL	Official
993	TCP		Internet Message Access Protocol over SSL (IMAPS)	Official
995	TCP		Post Office Protocol 3 over TLS/SSL (POP3S)	Official
999	TCP		ScimoreDB Database System	Unofficial
1001	TCP	UDP	JtoMB Tibbo device servers	Unofficial
1002	TCP		Opsware agent (aka cogbot)	Unofficial
1023	TCP	UDP	Reserved[11]	Official

Registered ports: 1024–49151

The range of port number from 1024 to 49151 are the registered ports. They are assigned by IANA for specific service upon application by a requesting entity.[1] On most systems registered ports can be used by ordinary users.

Port	TCP	UDP	Description	Status
1024	TCP	UDP	Reserved[1]	Official
1025	TCP		NFS or IIS or Teradata	Unofficial
1026	TCP		Often used by Microsoft DCOM services	Unofficial
1029	TCP		Often used by Microsoft DCOM services	Unofficial
1058	TCP	UDP	nim, IBM AIX Network Installation Manager (NIM)	Official
1059	TCP	UDP	nimreg, IBM AIX Network Installation Manager (NIM)	Official
1080	TCP		SOCKS proxy	Official
1085	TCP	UDP	WebObjects	Official
1098	TCP	UDP	rmiactivation, RMI Activation	Official
1099	TCP	UDP	rmiregistry, RMI Registry	Official
1109		UDP	Reserved[1]	Official
1109	TCP		Reserved[1]	Official
1109	TCP		Kerberos Post Office Protocol (KPOP)	Unofficial
1110		UDP	EasyBits School network discovery protocol (for Intel's CMPC platform)	Unofficial
1140	TCP	UDP	AutoNOC protocol	Official
1167		UDP	phone, conference calling	Unofficial
1169	TCP	UDP	Tripwire	Official
1176	TCP		Perceptive Automation Indigo Home automation server	Official
1182	TCP	UDP	AcceleNet Intelligent Transfer Protocol	Official
1194	TCP	UDP	OpenVPN	Official
1198	TCP	UDP	The cajo project Free dynamic transparent distributed computing in Java	Official
1200	TCP		scol, protocol used by SCOL 3D virtual worlds server to answer world name resolution client request[37]	Official
1200		UDP	scol, protocol used by SCOL 3D virtual worlds server to answer world name resolution client request	Official
1200		UDP	Steam Friends Applet	Unofficial
1214	TCP		Kazaa	Official
1217	TCP		Uvora Online	Unofficial
1220	TCP		QuickTime Streaming Server administration	Official
1223	TCP	UDP	TGP, TrulyGlobal Protocol, also known as "The Gur Protocol" (named for Gur Kimchi of TrulyGlobal)	Official
1234		UDP	VLC media player Default port for UDP/RTP stream	Unofficial
1236	TCP		Symantec BindView Control UNIX Default port for TCP management server connections	Unofficial
1241	TCP	UDP	Nessus Security Scanner	Official
1270	TCP	UDP	Microsoft System Center Operations Manager (SCOM) (formerly Microsoft Operations Manager (MOM)) agent	Official
1293	TCP	UDP	IPSec (Internet Protocol Security)	Official
1301	TCP		Palmer Performance OBDNet	Unofficial
1309	TCP		Altera Quartus jtagd	Unofficial
1311	TCP		Dell OpenManage HTTPS	Official
1313	TCP		Xbiim (Canvii server)	Unofficial

1319	TCP		AMX ICSP	Official
1319	UDP		AMX ICSP	Official
1337		UDP	Men and Mice DNS	Official
1337	TCP		Men and Mice DNS	Official
1337	TCP		PowerFolder P2P Encrypted File Synchronization Program	Unofficial
1337	TCP		WASTE Encrypted File Sharing Program	Unofficial
1352	TCP		IBM Lotus Notes/Domino[38] (RPC) protocol	Official
1387	TCP	UDP	cadsi-lm, LMS International (formerly Computer Aided Design Software, Inc. (CADSI)) LM	Official
1414	TCP		IBM WebSphere MQ (formerly known as MQSeries)	Official
1417	TCP	UDP	Timbuktu Service 1 Port	Official
1418	TCP	UDP	Timbuktu Service 2 Port	Official
1419	TCP	UDP	Timbuktu Service 3 Port	Official
1420	TCP	UDP	Timbuktu Service 4 Port	Official
1431	TCP		Reverse Gossip Transport Protocol (RGTP), used to access a General-purpose Reverse-Ordered Gossip Gathering System (GROGGS) bulletin board, such as that implemented on the Cambridge University's Phoenix system	Official
1433	TCP		MSSQL (Microsoft SQL Server database management system) Server	Official
1434	TCP	UDP	MSSQL (Microsoft SQL Server database management system) Monitor	Official
1470	TCP		Solarwinds Kiwi Log Server	Official
1494	TCP		Citrix XenApp Independent Computing Architecture (ICA) thin client protocol	Official
1500	TCP		NetGuard GuardianPro firewall (NT4-based) Remote Management	Unofficial
1501		UDP	NetGuard GuardianPro firewall (NT4-based) Authentication Client	Unofficial
1503	TCP	UDP	Windows Live Messenger (Whiteboard and Application Sharing)	Unofficial
1512	TCP	UDP	Microsoft Windows Internet Name Service (WINS)	Official
1513	TCP	UDP	Garena Garena Gaming Client	Official
1521	TCP		nCube License Manager	Official
1521	TCP		Oracle database default listener, in future releases official port 2483	Unofficial
1524	TCP	UDP	ingreslock, ingres	Official
1526	TCP		Oracle database common alternative for listener	Unofficial
1527	TCP		Apache Derby Network Server default port	Unofficial
1533	TCP		IBM Sametime IM—Virtual Places Chat Microsoft SQL Server	Official
1547	TCP	UDP	Laplink	Official
1550			Gadu-Gadu (direct client-to-client)	Unofficial
1581		UDP	MIL STD 2045-47001 VMF	Official
1589		UDP	Cisco VQP (VLAN Query Protocol) / VMPS	Unofficial
1627			iSketch	Unofficial
1645	TCP	UDP	radius auth, RADIUS authentication protocol (default for Cisco and Juniper Networks RADIUS servers)	Unofficial
1646	TCP	UDP	radius acct, RADIUS authentication protocol (default for Cisco and Juniper Networks RADIUS servers)	Unofficial
1666	TCP		Perforce	Unofficial
1677	TCP	UDP	Novell GroupWise clients in client/server access mode	Official

1688	TCP		Microsoft Key Management Service for KMS Windows Activation	Unofficial
1701		UDP	Layer 2 Forwarding Protocol (L2F) & Layer 2 Tunneling Protocol (L2TP)	Official
1707		TCP	Romtoc Packet Protocol (L2F) & Layer 2 Tunneling Protocol (L2TP)	Unofficial
1716	TCP		America's Army Massively multiplayer online game (MMO)	Unofficial
1719		UDP	H.323 Registration and alternate communication	Official
1720	TCP		H.323 Call signalling	Official
1723	TCP	UDP	Microsoft Point-to-Point Tunneling Protocol (PPTP)	Official
1725		UDP	Valve Steam Client	Unofficial
1755	TCP	UDP	Microsoft Media Services (MMS, ms-streaming)	Official
1761		UDP	cft-0	Official
1761	TCP		cft-0	Official
1761	TCP		Novell Zenworks Remote Control utility	Unofficial
1762–1768	TCP	UDP	cft-1 to cft-7	Official
1801	TCP	UDP	Microsoft Message Queuing	Official
1812	TCP	UDP	radius, RADIUS authentication protocol	Official
1813	TCP	UDP	radacct, RADIUS accounting protocol	Official
1863	TCP		MSNP (Microsoft Notification Protocol), used by the .NET Messenger Service and a number of Instant Messaging clients	Official
1883	TCP	UDP	MQ Telemetry Transport (MQTT), formerly known as MQIsdp (MQSeries SCADA protocol)	Official
1886	TCP		Leonardo over IP Pro2col Ltd	Unofficial
1900		UDP	Microsoft SSDP Enables discovery of UPnP devices	Official
1920	TCP		IBM Tivoli Monitoring Console (https)	Unofficial
1935	TCP		Adobe Systems Macromedia Flash Real Time Messaging Protocol (RTMP) "plain" protocol	Official
1947	TCP	UDP	SentinelSRM (hasplm), Aladdin HASP License Manager	Official
1967		UDP	Cisco IOS IP Service Level Agreements (IP SLAs) Control Protocol	Unofficial
1970	TCP	UDP	Netop Business Solutions Netop Remote Control	Official
1971	TCP	UDP	Netop Business Solutions Netop School	Official
1972	TCP	UDP	InterSystems Caché	Official
1975–1977		UDP	Cisco TCO (Documentation)	Official
1984	TCP		Big Brother System and Network Monitor	Official
1985		UDP	Cisco HSRP	Official
1994	TCP	UDP	Cisco STUN-SDLC (Serial Tunneling—Synchronous Data Link Control) protocol	Official
1997	TCP		Chizmo Networks Transfer Tool	Unofficial
1998	TCP	UDP	Cisco X.25 over TCP (XOT) service	Official
2000	TCP	UDP	Cisco SCCP (Skinny)	Official
2001		UDP	CAPTAN Test Stand System	Unofficial
2002	TCP		Secure Access Control Server (ACS) for Windows	Unofficial
2030			Oracle Services for Microsoft Transaction Server	Unofficial
2031	TCP	UDP	mobrien-chat(http://chat.mobrien.com:2031)	Official
2041	TCP		Mail.Ru Agent communication protocol	Unofficial
2049		UDP	Network File System	Official
2049		UDP	shilp	Official

2053		UDP	lot105-ds-upd Lot105 DSuper Updates	Official
2053	TCP		lot105-ds-upd Lot105 DSuper Updates	Official
2053	TCP		knetd Kerberos de-multiplexor	Unofficial
2056		UDP	Civilization 4 multiplayer	Unofficial
2073	TCP	UDP	DataReel Database	Official
2074	TCP	UDP	Vertel VMF SA (i.e. App.. SpeakFreely)	Official
2082	TCP		Infowave Mobility Server	Official
2082	TCP		CPanel default	Unofficial
2083	TCP		Secure Radius Service (radsec)	Official
2083	TCP		CPanel default SSL	Unofficial
2086	TCP		GNUnet	Official
2086	TCP		WebHost Manager default	Unofficial
2087	TCP		WebHost Manager default SSL	Unofficial
2095	TCP		CPanel default Web mail	Unofficial
2096	TCP		CPanel default SSL Web mail	Unofficial
2102	TCP	UDP	zephyr-srv Project Athena Zephyr Notification Service server	Official
2103	TCP	UDP	zephyr-clt Project Athena Zephyr Notification Service serv-hm connection	Official
2104	TCP	UDP	zephyr-hm Project Athena Zephyr Notification Service hostmanager	Official
2105	TCP	UDP	IBM MiniPay	Official
2105	TCP	UDP	eklogin Kerberos encrypted remote login (rlogin)	Unofficial
2105	TCP	UDP	zephyr-hm-srv Project Athena Zephyr Notification Service hm-serv connection (should use port 2102)	Unofficial
2144	TCP		Iron Mountain LiveVault Agent	UnOfficial
2145	TCP		Iron Mountain LiveVault Agent	UnOfficial
2156		UDP	Talari Reliable Protocol	Official
2160	TCP		APC Agent	Official
2161	TCP		APC Agent	Official
2181	TCP	UDP	EForward-document transport system	Official
2190		UDP	TiVoConnect Beacon	Unofficial
2200		UDP	Tuxanci game server[39]	Unofficial
2210		UDP	NOAAPORT Broadcast Network	Official
2210	TCP		NOAAPORT Broadcast Network	Official
2210	TCP		MikroTik Remote management for "The Dude"	Unofficial
2211		UDP	EMWIN	Official
2211	TCP		EMWIN	Official
2211	TCP		MikroTik Secure management for "The Dude"	Unofficial
2212		UDP	LeeCO POS Server Service	Official
2212	TCP		LeeCO POS Server Service	Official
2212	TCP		Port-A-Pour Remote WinBatch	Unofficial
2219	TCP	UDP	NetIQ NCAP Protocol	Official
2220	TCP	UDP	NetIQ End2End	Official
2221	TCP		ESET Anti-virus updates	Unofficial
2222	TCP		DirectAdmin default & ESET Remote Administration	Unofficial
2223		UDP	Microsoft Office OS X antipiracy network monitor	Unofficial
2261	TCP	UDP	CoMotion Master	Official
2262	TCP	UDP	CoMotion Backup	Official
2301	TCP		HP System Management Redirect to port 2381	Unofficial
2302		UDP	ArmA multiplayer (default for game)	Unofficial

2302		UDP	Halo: Combat Evolved multiplayer	Unofficial
2303		UDP	ArmA multiplayer (default for server reporting) *(default port for game +1)*	Unofficial
2305		UDP	ArmA multiplayer (default for VoN) *(default port for game +3)*	Unofficial
2369	TCP		Default for BMC Software Control-M/Server—Configuration Agent, though often changed during installation	Official
2370	TCP		Default for BMC Software Control-M/Server—to allow the Control-M/Enterprise Manager to connect to the Control-M/Server, though often changed during installation	Official
2379	TCP		KGS Go Server	Unofficial
2381	TCP		HP Insight Manager default for Web server	Unofficial
2401	TCP		CVS version control system	Unofficial
2404	TCP		IEC 60870-5 -104, used to send electric power telecontrol messages between two systems via directly connected data circuits	Official
2420		UDP	Westell Remote Access	Official
2427		UDP	Cisco MGCP	Official
2447	TCP	UDP	ovwdb—OpenView Network Node Manager (NNM) daemon	Official
2483	TCP	UDP	Oracle database listening for unsecure client connections to the listener, replaces port 1521	Official
2484	TCP	UDP	Oracle database listening for SSL client connections to the listener	Official
2500	TCP		THEÒSMESSENGER listening for TheòsMessenger client connections	Official
2501	TCP		TheosNet-Admin listening for TheòsMessenger client connections	Official
2518	TCP	UDP	Willy	Official
2525	TCP		SMTP alternate	Unofficial
2535	TCP		MADCAP	
2546	TCP	UDP	EVault—Data Protection Services	Unofficial
2593	TCP	UDP	RunUO—Ultima Online server	Unofficial
2598	TCP		new ICA—when Session Reliability is enabled, TCP port 2598 replaces port 1494	Unofficial
2599	TCP		SonicWALL Antispam traffic between Remote Analyzer (RA) and Control Center (CC)	Unofficial
2610	TCP		Dark Ages	Unofficial
2612	TCP	UDP	QPasa from MQSoftware	Official
2638	TCP		Sybase database listener	Unofficial
2636	TCP		Solve Service	Official
2698	TCP	UDP	Citel / MCK IVPIP	Official
2700–2800	TCP		KnowShowGo P2P	Official
2710	TCP		XBT Bittorrent Tracker	Unofficial
2710		UDP	XBT Bittorrent Tracker experimental UDP tracker extension	Unofficial
2710	TCP		Knuddels.de	Unofficial
2735	TCP	UDP	NetIQ Monitor Console	Official
2809	TCP		corbaloc:iiop URL, per the CORBA 3.0.3 specification	Official
2809	TCP		IBM WebSphere Application Server (WAS) Bootstrap/rmi default	Unofficial
2809		UDP	corbaloc:iiop URL, per the CORBA 3.0.3 specification.	Official
2868	TCP	UDP	Norman Proprietary Event Protocol NPEP	Official

2944		UDP	Megaco Text H.248	Unofficial
2945		UDP	Megaco Binary (ASN.1) H.248	Unofficial
2947	TCP		gpsd GPS daemon	Official
2948	TCP	UDP	WAP-push Multimedia Messaging Service (MMS)	Official
2949	TCP	UDP	WAP-pushsecure Multimedia Messaging Service (MMS)	Official
2967	TCP		Symantec AntiVirus Corporate Edition	Unofficial
3000	TCP		Miralix License server	Unofficial
3000	TCP		Cloud9 Integrated Development Environment server	Unofficial
3000		UDP	Distributed Interactive Simulation (DIS), modifiable default	Unofficial
3000	TCP		Ruby on Rails development default[40]	Unofficial
3001	TCP		Miralix Phone Monitor	Unofficial
3001	TCP		Opsware server (Satellite)	Unofficial
3002	TCP		Miralix CSTA	Unofficial
3003	TCP		Miralix GreenBox API	Unofficial
3004	TCP		Miralix InfoLink	Unofficial
3005	TCP		Miralix TimeOut	Unofficial
3006	TCP		Miralix SMS Client Connector	Unofficial
3007	TCP		Miralix OM Server	Unofficial
3008	TCP		Miralix Proxy	Unofficial
3017	TCP		Miralix IVR and Voicemail	Unofficial
3025	TCP		netpd.org	Unofficial
3030	TCP	UDP	NetPanzer	Unofficial
3050	TCP	UDP	gds_db (Interbase/Firebird)	Official
3051	TCP	UDP	Galaxy Server (Gateway Ticketing Systems)	Official
3052	TCP	UDP	APC PowerChute Network [41]	Official
3074	TCP	UDP	Xbox LIVE and/or Games for Windows - LIVE	Official
3100	TCP		HTTP used by Tatsoft as the default listen port	Unofficial
3101	TCP		BlackBerry Enterprise Server communication to cloud	Unofficial
3128	TCP		HTTP used by Web caches and the default for the Squid (software)	Unofficial
3128	TCP		HTTP used by Tatsoft as the default client connection	Unofficial
3225	TCP	UDP	FCIP (Fiber Channel over Internet Protocol)	Official
3233	TCP	UDP	WhiskerControl research control protocol	Official
3235	TCP	UDP	Galaxy Network Service (Gateway Ticketing Systems)	Official
3260	TCP		iSCSI target	Official
3268	TCP	UDP	msft-gc, Microsoft Global Catalog (LDAP service which contains data from Active Directory forests)	Official
3269	TCP	UDP	msft-gc-ssl, Microsoft Global Catalog over SSL (similar to port 3268, LDAP over SSL)	Official
3283	TCP		Apple Remote Desktop reporting (officially *Net Assistant*, referring to an earlier product)	Official
3299	TCP		SAP-Router (routing application proxy for SAP R/3)	Unofficial
3300	TCP	UDP	Debate Gopher backend database system	Unofficial
3305	TCP	UDP	odette-ftp, Odette File Transfer Protocol (OFTP)	Official
3306	TCP	UDP	MySQL database system	Official
3313	TCP		Verisys - File Integrity Monitoring Software	Unofficial
3333	TCP		Network Caller ID server	Unofficial
3333	TCP		CruiseControl.rb[42]	Unofficial
3386	TCP	UDP	GTP' 3GPP GSM/UMTS CDR logging protocol	Official
3389	TCP	UDP	Microsoft Terminal Server (RDP) officially registered as	Official

			Windows Based Terminal (WBT) - Link	
3396	TCP	UDP	Novell NDPS Printer Agent	Official
3412	TCP	UDP	xmlBlaster	Official
3455	TCP	UDP	[RSVP] Reservation Protocol	Official
3423	TCP		Xware xTrm Communication Protocol	Official
3424	TCP		Xware xTrm Communication Protocol over SSL	Official
3478	TCP	UDP	STUN, a protocol for NAT traversal	Official
3483		UDP	Slim Devices discovery protocol	Official
3483	TCP		Slim Devices SlimProto protocol	Official
3516	TCP	UDP	Smartcard Port	Official
3527		UDP	Microsoft Message Queuing	Official
3535	TCP		SMTP alternate	Unofficial
3537	TCP	UDP	ni-visa-remote	Unofficial
3544		UDP	Teredo tunneling	Official
3605		UDP	ComCam IO Port	Official
3606	TCP	UDP	Splitlock Server	Official
3632	TCP		distributed compiler	Official
3689	TCP		Digital Audio Access Protocol (DAAP)—used by Apple's iTunes and AirPort Express	Official
3690	TCP	UDP	Subversion version control system	Official
3702	TCP	UDP	Web Services Dynamic Discovery (WS-Discovery), used by various components of Windows Vista	Official
3723	TCP	UDP	Used by many Battle.net Blizzard games (Diablo II, Warcraft II, Warcraft III, StarCraft)	Unofficial
3724		UDP	World of Warcraft Online gaming MMORPG	Official
3724	TCP		World of Warcraft Online gaming MMORPG	Official
3724	TCP		Club Penguin Disney online game for kids	Unofficial
3784	TCP	UDP	Ventrilo VoIP program used by Ventrilo	Unofficial
3785		UDP	Ventrilo VoIP program used by Ventrilo	Unofficial
3800	TCP		Used by HGG programs	Unofficial
3880	TCP	UDP	IGRS	Official
3868	TCP	SCTP	Diameter base protocol (RFC 3588)	Official
3872	TCP		Oracle Management Remote Agent	Unofficial
3899	TCP		Remote Administrator	Unofficial
3900	TCP		udt_os, IBM UniData UDT OS[43]	Official
3945	TCP	UDP	EMCADS service, a Giritech product used by G/On	Official
3978	TCP	UDP	OpenTTD game (masterserver and content service)	Unofficial
3979	TCP	UDP	OpenTTD game	Unofficial
3999	TCP	UDP	Norman distributed scanning service	Official
4000	TCP	UDP	Diablo II game	Unofficial
4001	TCP		Microsoft Ants game	Unofficial
4007	TCP		PrintBuzzer printer monitoring socket server	Unofficial
4018	TCP	UDP	protocol information and warnings	Official
4069		UDP	Minger Email Address Verification Protocol[44]	Official
4089	TCP	UDP	OpenCORE Remote Control Service	Official
4093	TCP	UDP	PxPlus Client server interface ProvideX	Official
4096	TCP	UDP	Ascom Timeplex BRE (Bridge Relay Element)	Official
4100			WatchGuard Authentication Applet—default	Unofficial
4111	TCP		Xgrid	Official
4116	TCP	UDP	Smartcard-TLS	Official

4125	TCP		Microsoft Remote Web Workplace administration	Unofficial
4172	TCP	UDP	Teradici PCoIP	Official
4201	TCP		TinyMUD and various derivatives	Unofficial
4226	TCP	UDP	Aleph One (game)	Unofficial
4224	TCP		Cisco Audio Session Tunneling	Unofficial
4321	TCP		Referral Whois (RWhois) Protocol[45]	Official
4323		UDP	Lincoln Electric's ArcLink/XT	Unofficial
4433-4436	TCP		Axence nVision	Unofficial
4500		UDP	IPSec NAT Traversal (RFC 3947)	Official
4534		UDP	Armagetron Advanced default server port	Unofficial
4567	TCP		Sinatra default server port in development mode (HTTP)	Unofficial
4569		UDP	Inter-Asterisk eXchange (IAX2)	Official
4610–4640	TCP		QualiSystems TestShell Suite Services	Unofficial
4662		UDP	OrbitNet Message Service	Official
4662	TCP		OrbitNet Message Service	Official
4662	TCP		Default for older versions of eMule[46]	Unofficial
4664	TCP		Google Desktop Search	Unofficial
4672		UDP	Default for older versions of eMule[46]	Unofficial
4711	TCP		eMule optional web interface[46]	Unofficial
4711	TCP		McAfee Web Gateway 7 - Default GUI Port HTTP	Unofficial
4712	TCP		McAfee Web Gateway 7 - Default GUI Port HTTPS	Unofficial
4728	TCP		Computer Associates Desktop and Server Management (DMP)/Port Multiplexer [47]	Official
4747	TCP		Apprentice	Unofficial
4750	TCP		BladeLogic Agent	Unofficial
4840	TCP	UDP	OPC UA TCP Protocol for OPC Unified Architecture from OPC Foundation	Official
4843	TCP	UDP	OPC UA TCP Protocol over TLS/SSL for OPC Unified Architecture from OPC Foundation	Official
4847	TCP	UDP	Web Fresh Communication, Quadrion Software & Odorless Entertainment	Official
4894	TCP	UDP	LysKOM Protocol A	Official
4899	TCP	UDP	Radmin remote administration tool (program sometimes used by a Trojan horse)	Official
4949	TCP		Munin Resource Monitoring Tool	Official
4950	TCP	UDP	Cylon Controls UC32 Communications Port	Official
4982	TCP	UDP	Solar Data Log (JK client app for PV solar inverters)	Unofficial
4993	TCP	UDP	Home FTP Server web Interface Default Port	Unofficial
5000	TCP		commplex-main	Official
5000	TCP		UPnP—Windows network device interoperability	Unofficial
5000	TCP		VTun—VPN Software	Unofficial
5000		UDP	FlightGear multiplayer[48]	Unofficial
5000		UDP	VTun—VPN Software	Unofficial
5001	TCP		commplex-link	Official
5001	TCP		Slingbox and Slingplayer	Unofficial
5001	TCP		Iperf (Tool for measuring TCP and UDP bandwidth performance)	Unofficial
5001		UDP	Iperf (Tool for measuring TCP and UDP bandwidth performance)	Unofficial

5002	TCP		SOLICARD ARX[49]	Unofficial
5003	TCP	UDP	FileMaker	Official
5004	TCP	UDP,DCCP	RTP (Real-time Transport Protocol) media data (RFC 3551, RFC 4571)	Official
5005	TCP	UDP,DCCP	RTP (Real-time Transport Protocol) control protocol (RFC 3551, RFC 4571)	Official
5029	TCP		Sonic Robot Blast 2 : Multiplayer	Unofficial
5031	TCP	UDP	AVM CAPI-over-TCP (ISDN over Ethernet tunneling)	Unofficial
5050	TCP		Yahoo! Messenger	Unofficial
5051	TCP		ita-agent Symantec Intruder Alert[50]	Official
5060	TCP	UDP	Session Initiation Protocol (SIP)	Official
5061	TCP		Session Initiation Protocol (SIP) over TLS	Official
5070	TCP		Binary Floor Control Protocol (BFCP),[51] published as RFC 4582, is a protocol that allows for an additional video channel (known as the content channel) alongside the main video channel in a video-conferencing call that uses SIP. Also used for Session Initiation Protocol (SIP) preferred port for PUBLISH on SIP Trunk to Cisco Unified Presence Server (CUPS)	Unofficial
5082	TCP	UDP	Qpur Communication Protocol	Official
5083	TCP	UDP	Qpur File Protocol	Official
5084	TCP	UDP	EPCglobal Low Level Reader Protocol (LLRP)	Official
5085	TCP	UDP	EPCglobal Low Level Reader Protocol (LLRP) over TLS	Official
5093		UDP	SafeNet, Inc Sentinel LM, Sentinel RMS, License Manager, Client-to-Server	Official
5099	TCP	UDP	SafeNet, Inc Sentinel LM, Sentinel RMS, License Manager, Server-to-Server	Official
5104	TCP		IBM Tivoli Framework NetCOOL/Impact[52] HTTP Service	Unofficial
5106	TCP		A-Talk Common connection	Unofficial
5107	TCP		A-Talk Remote server connection	Unofficial
5108	TCP		VPOP3 Mail Server Webmail	Unofficial
5109	TCP	UDP	VPOP3 Mail Server Status	Unofficial
5110	TCP		ProRat Server	Unofficial
5121	TCP		Neverwinter Nights	Unofficial
5150	TCP	UDP	ATMP Ascend Tunnel Management Protocol[53]	Official
5150	TCP	UDP	Malware Cerberus RAT	Unofficial
5151	TCP		ESRI SDE Instance	Official
5151		UDP	ESRI SDE Remote Start	Official
5154	TCP	UDP	BZFlag	Official
5176	TCP		ConsoleWorks default UI interface	Unofficial
5190	TCP		ICQ and AOL Instant Messenger	Official
5222	TCP		Extensible Messaging and Presence Protocol (XMPP) client connection[54]	Official
5223	TCP		Extensible Messaging and Presence Protocol (XMPP) client connection over SSL	Unofficial
5246		UDP	Control And Provisioning of Wireless Access Points (CAPWAP) CAPWAP control[55]	Official
5247		UDP	Control And Provisioning of Wireless Access Points (CAPWAP) CAPWAP data[55]	Official
5269	TCP		Extensible Messaging and Presence Protocol (XMPP) server connection[54]	Official

5298	TCP	UDP	Extensible Messaging and Presence Protocol (XMPP) JEP-0174: Link-Local Messaging / XEP-0174: Serverless Messaging	Official
5310	TCP	UDP	Ginever.net data communication port	Unofficial
5311	TCP	UDP	Ginever.net data communication port	Unofficial
5312	TCP	UDP	Ginever.net data communication port	Unofficial
5313	TCP	UDP	Ginever.net data communication port	Unofficial
5314	TCP	UDP	Ginever.net data communication port	Unofficial
5315	TCP	UDP	Ginever.net data communication port	Unofficial
5351	TCP	UDP	NAT Port Mapping Protocol—client-requested configuration for inbound connections through network address translators	Official
5353		UDP	Multicast DNS (mDNS)	Official
5355	TCP	UDP	LLMNR—Link-Local Multicast Name Resolution, allows hosts to perform name resolution for hosts on the same local link (only provided by Windows Vista and Server 2008)	Official
5357	TCP	UDP	Web Services for Devices (WSDAPI) (only provided by Windows Vista, Windows 7 and Server 2008)	Unofficial
5358	TCP	UDP	WSDAPI Applications to Use a Secure Channel (only provided by Windows Vista, Windows 7 and Server 2008)	Unofficial
5402	TCP	UDP	mftp, Stratacache OmniCast content delivery system MFTP file sharing protocol	Official
5405	TCP	UDP	NetSupport Manager	Official
5412	TCP	UDP	IBM Rational Synergy (Telelogic_Synergy) (Continuus CM) Message Router	Official
5421	TCP	UDP	NetSupport Manager	Official
5432	TCP	UDP	PostgreSQL database system	Official
5433	TCP		Bouwsoft file/webserver <http://www.bouwsoft.be>	Unofficial
5445		UDP	Cisco Unified Video Advantage	Unofficial
5450	TCP		OSIsoft PI Server Client Access	Unofficial
5457	TCP		OSIsoft PI Asset Framework Client Access	Unofficial
5458	TCP		OSIsoft PI Notifications Client Access	Unofficial
5495	TCP		Applix TM1 Admin server	Unofficial
5498	TCP		Hotline tracker server connection	Unofficial
5499		UDP	Hotline tracker server discovery	Unofficial
5500	TCP		VNC remote desktop protocol—for incoming listening viewer, Hotline control connection	Unofficial
5501	TCP		Hotline file transfer connection	Unofficial
5517	TCP		Setiqueue Proxy server client for SETI@Home project	Unofficial
5550	TCP		Hewlett-Packard Data Protector	Unofficial
5555	TCP		Freeciv versions up to 2.0, Hewlett-Packard Data Protector, McAfee EndPoint Encryption Database Server, SAP, Default for Microsoft Dynamics CRM 4.0	Unofficial
5556	TCP	UDP	Freeciv	Official
5591	TCP		Default for Tidal Enterprise Scheduler master-Socket used for communication between Agent-to-Master, though can be changed	Unofficial
5631	TCP		pcANYWHEREdata, Symantec pcAnywhere (version 7.52 and later[56])[57] data	Official
5632		UDP	pcANYWHEREstat, Symantec pcAnywhere (version 7.52 and later) status	Official
5656	TCP		IBM Sametime p2p file transfer	Unofficial

5666	TCP		NRPE (Nagios)	Unofficial
5667	TCP		NSCA (Nagios)	Unofficial
5678		UDP	Mikrotik RouterOS Neighbor Discovery Protocol (MNDP)	Unofficial
5721	TCP	UDP	Kaseya	Unofficial
5723	TCP		Operations Manager	Unofficial
5741	TCP	UDP	IDA Discover Port 1	Official
5742	TCP	UDP	IDA Discover Port 2	Official
5800	TCP		VNC remote desktop protocol—for use over HTTP	Unofficial
5814	TCP	UDP	Hewlett-Packard Support Automation (HP OpenView Self-Healing Services)	Official
5850	TCP		COMIT SE (PCR)	Unofficial
5852	TCP		Adeona client: communications to OpenDHT	Unofficial
5900	TCP	UDP	Virtual Network Computing (VNC) remote desktop protocol (used by Apple Remote Desktop and others)	Official
5912	TCP		Default for Tidal Enterprise Scheduler agent-Socket used for communication between Master-to-Agent, though can be changed	Unofficial
5938	TCP	UDP	TeamViewer[58] remote desktop protocol	Unofficial
5984	TCP	UDP	CouchDB database server	Official
5999	TCP		CVSup [59] file update tool	Official
6000	TCP		X11—used between an X client and server over the network	Official
6001		UDP	X11—used between an X client and server over the network	Official
6005	TCP		Default for BMC Software Control-M/Server—Socket used for communication between Control-M processes—though often changed during installation	Official
6005	TCP		Default for Camfrog Chat & Cam Client http://www.camfrog.com	Unofficial
6050	TCP		Brightstor Arcserve Backup	Unofficial
6050	TCP		Nortel Software	Unofficial
6051	TCP		Brightstor Arcserve Backup	Unofficial
6072	TCP		iOperator Protocol Signal Port	Unofficial
6086	TCP		PDTP—FTP like file server in a P2P network	Official
6100	TCP		Vizrt System	Unofficial
6100	TCP		Ventrilo This is the authentication port that must be allowed outbound for version 3 of Ventrilo	Official
6101	TCP		Backup Exec Agent Browser	Unofficial
6110	TCP	UDP	softcm, HP Softbench CM	Official
6111	TCP	UDP	spc, HP Softbench Sub-Process Control	Official
6112		UDP	"dtspcd"—a network daemon that accepts requests from clients to execute commands and launch applications remotely	Official
6112	TCP		"dtspcd"—a network daemon that accepts requests from clients to execute commands and launch applications remotely	Official
6112	TCP		Blizzard's Battle.net gaming service, ArenaNet gaming service, Relic gaming sercive	Unofficial
6112	TCP		Club Penguin Disney online game for kids	Unofficial
6113	TCP		Club Penguin Disney online game for kids	Unofficial
6129	TCP		DameWare Remote Control	Official
6257		UDP	WinMX (see also 6699)	Unofficial
6260	TCP	UDP	planet M.U.L.E.	Unofficial
6262	TCP		Sybase Advantage Database Server	Unofficial
6343		UDP	SFlow, sFlow traffic monitoring	Official

6346	TCP	UDP	gnutella-svc, gnutella (FrostWire, Limewire, Shareaza, etc.)	Official
6347	TCP	UDP	gnutella-rtr, Gnutella alternate	Official
6350	TCP	UDP	App Discovery and Access Protocol	Official
6389	TCP		EMC CLARiiON	Unofficial
6432	TCP		PgBouncer - A connection pooler for PostgreSQL	Official
6444	TCP	UDP	Sun Grid Engine—Qmaster Service	Official
6445	TCP	UDP	Sun Grid Engine—Execution Service	Official
6502	TCP	UDP	Netop Business Solutions - NetOp Remote Control	Unofficial
6503		UDP	Netop Business Solutions - NetOp School	Unofficial
6522	TCP		Gobby (and other libobby-based software)	Unofficial
6523	TCP		Gobby 0.5 (and other libinfinity-based software)	Unofficial
6543		UDP	Paradigm Research & Development Jetnet[60] default	Unofficial
6566	TCP		SANE (Scanner Access Now Easy)—SANE network scanner daemon	Unofficial
6571			Windows Live FolderShare client	Unofficial
6600	TCP		Music Playing Daemon (MPD)	Unofficial
6619	TCP	UDP	odette-ftps, Odette File Transfer Protocol (OFTP) over TLS/SSL	Official
6646		UDP	McAfee Network Agent	Unofficial
6660–6664	TCP		Internet Relay Chat (IRC)	Unofficial
6665–6669	TCP		Internet Relay Chat (IRC)	Official
6679	TCP	UDP	Osorno Automation Protocol (OSAUT)	Official
6679	TCP		IRC SSL (Secure Internet Relay Chat)—often used	Unofficial
6697	TCP		IRC SSL (Secure Internet Relay Chat)—often used	Unofficial
6699	TCP		WinMX (see also 6257)	Unofficial
6702	TCP		Default for Tidal Enterprise Scheduler client-Socket used for communication between Client-to-Master, though can be changed	Unofficial
6771		UDP	Polycom server broadcast	Unofficial
6789	TCP		Datalogger Support Software Campbell Scientific Loggernet Software	Unofficial
6881–6887	TCP	UDP	BitTorrent part of full range of ports used most often	Unofficial
6888	TCP	UDP	MUSE	Official
6888	TCP	UDP	BitTorrent part of full range of ports used most often	Unofficial
6889–6890	TCP	UDP	BitTorrent part of full range of ports used most often	Unofficial
6891–6900	TCP	UDP	BitTorrent part of full range of ports used most often	Unofficial
6891–6900	TCP	UDP	Windows Live Messenger (File transfer)	Unofficial
6901	TCP	UDP	Windows Live Messenger (Voice)	Unofficial
6901	TCP	UDP	BitTorrent part of full range of ports used most often	Unofficial
6902–6968	TCP	UDP	BitTorrent part of full range of ports used most often	Unofficial
6969	TCP	UDP	acmsoda	Official
6969	TCP		BitTorrent tracker	Unofficial
6970–6999	TCP	UDP	BitTorrent part of full range of ports used most often	Unofficial

7000	TCP		Default for Vuze's built in HTTPS Bittorrent Tracker	Unofficial
7001	TCP		Default for BEA WebLogic Server's HTTP server, though often changed during installation	Unofficial
7002	TCP		Default for BEA WebLogic Server's HTTPS server, though often changed during installation	Unofficial
7005	TCP		Default for BMC Software Control-M/Server and Control-M/Agent for Agent-to-Server, though often changed during installation	Unofficial
7006	TCP		Default for BMC Software Control-M/Server and Control-M/Agent for Server-to-Agent, though often changed during installation	Unofficial
7010	TCP		Default for Cisco AON AMC (AON Management Console) [61]	Unofficial
7025	TCP		Zimbra LMTP [mailbox]—local mail delivery	Unofficial
7047	TCP		Zimbra conversion server	Unofficial
7133	TCP		Enemy Territory: Quake Wars	Unofficial
7144	TCP		Peercast	Unofficial
7145	TCP		Peercast	Unofficial
7171	TCP		Tibia	Unofficial
7306	TCP		Zimbra mysql [mailbox]	Unofficial
7307	TCP		Zimbra mysql [logger]	Unofficial
7312		UDP	Sibelius License Server	Unofficial
7400	TCP	UDP	RTPS (Real Time Publish Subscribe) DDS Discovery	Official
7401	TCP	UDP	RTPS (Real Time Publish Subscribe) DDS User-Traffic	Official
7402	TCP	UDP	RTPS (Real Time Publish Subscribe) DDS Meta-Traffic	Official
7473	TCP	UDP	Rise: The Vieneo Province	Official
7547	TCP	UDP	CPE WAN Management Protocol Technical Report 069	Official
7615	TCP		ISL Online[62] communication protocol	Unofficial
7670	TCP		BrettspielWelt BSW Boardgame Portal	Unofficial
7676	TCP		Aqumin AlphaVision Remote Command Interface	Unofficial
7700		UDP	P2P DC (RedHub)	Unofficial
7777	TCP		iChat server file transfer proxy	Unofficial
7777	TCP		Oracle Cluster File System 2	Unofficial
7777	TCP		Windows backdoor program tini.exe default	Unofficial
7777	TCP		Xivio.com Chat Server Interface	Unofficial
7777	TCP		Terraria default server	Unofficial
7778	TCP		Bad Trip MUD	Unofficial
7777-7788		UDP	Unreal Tournament series default server	Unofficial
7777-7788	TCP		Unreal Tournament series default server	Unofficial
7787-7788	TCP		GFI EventsManager 7 & 8	Official
7831	TCP		Default used by Smartlaunch Internet Cafe Administration[63] software	Unofficial
7880	TCP	UDP	PowerSchool Gradebook Server	Unofficial
7915	TCP		Default for YSFlight server [3]	Unofficial
7935	TCP		Fixed port used for Adobe Flash Debug Player to communicate with a debugger (Flash IDE, Flex Builder or fdb).[64]	Unofficial
7937-9936	TCP	UDP	EMC^2 (Legato) Networker or Sun Solcitice Backup	Official
8000		UDP	iRDMI (Intel Remote Desktop Management Interface)[65]—	Official

			sometimes erroneously used instead of port 8080	
8000	TCP		iRDMI (Intel Remote Desktop Management Interface)[65]—sometimes erroneously used instead of port 8080	Official
8000	TCP		Commonly used for internet radio streams such as those using SHOUTcast	Unofficial
8001	TCP		Commonly used for internet radio streams such as those using SHOUTcast	Unofficial
8002	TCP		Cisco Systems Unified Call Manager Intercluster	Unofficial
8008	TCP		HTTP Alternate	Official
8008	TCP		IBM HTTP Server administration default	Unofficial
8009	TCP		ajp13—Apache JServ Protocol AJP Connector	Unofficial
8010	TCP		XMPP File transfers	Unofficial
8011-8014	TCP		HTTP/TCP Symon Communications Event and Query Engine	Unofficial
8074	TCP		Gadu-Gadu	Unofficial
8078	TCP	UDP	Default port for most Endless Online-based servers	Unofficial
8080	TCP		HTTP alternate (http_alt)—commonly used for Web proxy and caching server, or for running a Web server as a non-root user	Official
8080	TCP		Apache Tomcat	Unofficial
8080		UDP	FilePhile Master/Relay	Unofficial
8081	TCP		HTTP alternate, VibeStreamer, e.g. McAfee ePolicy Orchestrator (ePO)	Unofficial
8086	TCP		HELM Web Host Automation Windows Control Panel	Unofficial
8086	TCP		Kaspersky AV Control Center	Unofficial
8087	TCP		Hosting Accelerator Control Panel	Unofficial
8087	TCP		Parallels Plesk Control Panel	Unofficial
8087		UDP	Kaspersky AV Control Center	Unofficial
8089	TCP		Splunk Daemon	Unofficial
8090	TCP		HTTP Alternate (http_alt_alt)—used as an alternative to port 8080	Unofficial
8100	TCP		Console Gateway License Verification	Unofficial
8116		UDP	Check Point Cluster Control Protocol	Unofficial
8118	TCP		Privoxy—advertisement-filtering Web proxy	Official
8123	TCP		Polipo Web proxy	Official
8192	TCP		Sophos Remote Management System	Unofficial
8193	TCP		Sophos Remote Management System	Unofficial
8194	TCP		Sophos Remote Management System	Unofficial
8200	TCP		GoToMyPC	Unofficial
8222	TCP		VMware Server Management User Interface[66] (insecure Web interface).[67] See also port 8333	Unofficial
8243	TCP	UDP	HTTPS listener for Apache Synapse [68]	Official
8280	TCP	UDP	HTTP listener for Apache Synapse [68]	Official
8291	TCP		Winbox—Default on a MikroTik RouterOS for a Windows application used to administer MikroTik RouterOS	Unofficial
8303		UDP	Teeworlds Server	Official
8332	TCP		Bitcoin JSON-RPC server[69]	Unofficial
8333	TCP		Bitcoin[70]	Unofficial
8333	TCP		VMware Server Management User Interface[66] (secure Web interface).[67] See also port 8222	Unofficial
8400	TCP	UDP	cvp, Commvault Unified Data Management	Official
8442	TCP	UDP	CyBro A-bus, Cybrotech Ltd.	Official

8443	TCP		SW Soft Plesk Control Panel, Apache Tomcat SSL, Promise WebPAM SSL, McAfee ePolicy Orchestrator (ePO)	Unofficial
8484	TCP	UDP	MapleStory	Unofficial
8500	TCP	UDP	ColdFusion Macromedia/Adobe ColdFusion default and Duke Nukem 3D—default	Unofficial
8501	TCP		[4] DukesterX —default	Unofficial
8601	TCP		Wavestore CCTV protocol [5]	Unofficial
8602	TCP	UDP	Wavestore Notification protocol	Unofficial
8691	TCP		Ultra Fractal default server port for distributing calculations over network computers	Unofficial
8701		UDP	SoftPerfect Bandwidth Manager	Unofficial
8702		UDP	SoftPerfect Bandwidth Manager	Unofficial
8767		UDP	TeamSpeak—default	Unofficial
8768		UDP	TeamSpeak—alternate	Unofficial
8880		UDP	cddbp-alt, CD DataBase (CDDB) protocol (CDDBP) alternate	Official
8880	TCP		cddbp-alt, CD DataBase (CDDB) protocol (CDDBP) alternate	Official
8880	TCP		WebSphere Application Server SOAP connector default	Unofficial
8880	TCP		Win Media Streamer to Server SOAP connector default	Unofficial
8881	TCP		Atlasz Informatics Research Ltd [6] Secure Application Server	Unofficial
8882	TCP		Atlasz Informatics Research Ltd [7] Secure Application Server	Unofficial
8883	TCP	UDP	Secure MQ Telemetry Transport (MQTT over SSL)	Official
8887	TCP		HyperVM HTTP	Official
8888	TCP		HyperVM HTTPS	Official
8888		UDP	NewsEDGE server	Official
8888	TCP		NewsEDGE server	Official
8888	TCP		Sun Answerbook dwhttpd server (deprecated by docs.sun.com)	Unofficial
8888	TCP		GNUmp3d HTTP music streaming and Web interface	Unofficial
8888	TCP		LoLo Catcher HTTP Web interface (www.optiform.com)	Unofficial
8888	TCP		D2GS Admin Console Telnet administration console for D2GS servers (Diablo 2)	Unofficial
8888	TCP		Earthland Relams 2 Server (AU1_2)	Unofficial
8888	TCP		MAMP Server	Unofficial
8889	TCP		MAMP Server	Unofficial
8889	TCP		Earthland Relams 2 Server (AU1_1)	Unofficial
8983	TCP		Default for Apache Solr 1.4	Unofficial
9000	TCP		Buffalo LinkSystem Web access	Unofficial
9000	TCP		DBGp	Unofficial
9000	TCP		SqueezeCenter web server & streaming	Unofficial
9000		UDP	UDPCast	Unofficial
9001	TCP	UDP	ETL Service Manager[71]	Official
9001			Microsoft Sharepoint Authoring Environment	Unofficial
9001			cisco-xremote router configuration	Unofficial
9001			Tor network default	Unofficial
9001	TCP		DBGp Proxy	Unofficial
9009	TCP	UDP	Pichat Server—Peer to peer chat software	Official
9030	TCP		Tor often used	Unofficial
9043	TCP		WebSphere Application Server Administration Console secure	Unofficial
9050	TCP		Tor	Unofficial
9051	TCP		Tor	Unofficial
9060	TCP		WebSphere Application Server Administration Console	Unofficial

9080		UDP	glrpc, Groove Collaboration software GLRPC	Official
9080	TCP		glrpc, Groove Collaboration software GLRPC	Official
9080	TCP		WebSphere Application Server HTTP Transport (port 1) default	Unofficial
9090	TCP		Webwasher, Secure Web, McAfee Web Gateway - Default Proxy Port	Unofficial
9090	TCP		Openfire Administration Console	Unofficial
9090	TCP		SqueezeCenter control (CLI)	Unofficial
9091	TCP		Openfire Administration Console (SSL Secured)	Unofficial
9100	TCP		PDL Data Stream	Official
9101	TCP	UDP	Bacula Director	Official
9102	TCP	UDP	Bacula File Daemon	Official
9103	TCP	UDP	Bacula Storage Daemon	Official
9105	TCP	UDP	Xadmin Control Daemon	Official
9110		UDP	SSMP Message protocol	Unofficial
9119	TCP	UDP	MXit Instant Messenger	Official
9191	TCP		Catamount Software - PocketMoney Sync	Unofficial
9293	TCP		Sony PlayStation RemotePlay	Unofficial
9300	TCP		IBM Cognos 8 SOAP Business Intelligence and Performance Management	Unofficial
9303		UDP	D-Link Shareport Share storage and MFP printers	Unofficial
9306	TCP		Sphinx Native API	Official
9312	TCP		Sphinx SphinxQL	Official
9418	TCP	UDP	git, Git pack transfer service	Official
9420	TCP		MooseFS distributed file system—master server to chunk servers	Unofficial
9421	TCP		MooseFS distributed file system—master server to clients	Unofficial
9422	TCP		MooseFS distributed file system—chunk servers to clients	Unofficial
9535	TCP	UDP	mngsuite, LANDesk Management Suite Remote Control	Official
9536	TCP	UDP	laes-bf, IP Fabrics Surveillance buffering function	Official
9561	TCP	UDP	Network Time System Server	Unofficial
9600		UDP	Omron FINS, OMRON FINS PLC communication	Official
9675	TCP	UDP	Spiceworks Desktop, IT Helpdesk Software	Unofficial
9676	TCP	UDP	Spiceworks Desktop, IT Helpdesk Software	Unofficial
9695		UDP	CCNx	Official
9800	TCP	UDP	WebDAV Source	Official
9800			WebCT e-learning portal	Unofficial
9875	TCP		Club Penguin Disney online game for kids	Unofficial
9898		UDP	MonkeyCom	Official
9898	TCP		MonkeyCom	Official
9898	TCP		Tripwire—File Integrity Monitoring Software	Unofficial
9987		UDP	TeamSpeak 3 server default (voice) port (for the conflicting service see the IANA list)	Unofficial
9996	TCP	UDP	The Palace "The Palace" Virtual Reality Chat software.—5	Official
9999			Hydranode—edonkey2000 TELNET control	Unofficial
9999	TCP		Lantronix UDS-10/UDS100[172] RS-485 to Ethernet Converter TELNET control	Unofficial
9999			Urchin Web Analytics	Unofficial
10000			Webmin—Web-based Linux admin tool	Unofficial
10000			BackupExec	Unofficial

10000			Ericsson Account Manager (avim)	Unofficial
10001	TCP		Lantronix UDS-10/UDS100[73] RS-485 to Ethernet Converter default	Unofficial
10008	TCP	UDP	Octopus Multiplexer, primary port for the CROMP protocol, which provides a platform-independent means for communication of objects across a network	Official
10009	TCP	UDP	Cross Fire, a multiplayer online First Person Shooter	Unofficial
10010	TCP		Open Object Rexx (ooRexx) rxapi daemon	Official
10017			AIX,NeXT, HPUX—rexd daemon control	Unofficial
10024	TCP		Zimbra smtp [mta]—to amavis from postfix	Unofficial
10025	TCP		Zimbra smtp [mta]—back to postfix from amavis	Unofficial
10050	TCP	UDP	Zabbix-Agent	Official
10051	TCP	UDP	Zabbix-Trapper	Official
10110	TCP	UDP	NMEA 0183 Navigational Data. Transport of NMEA 0183 sentences over TCP or UDP	Official
10113	TCP	UDP	NetIQ Endpoint	Official
10114	TCP	UDP	NetIQ Qcheck	Official
10115	TCP	UDP	NetIQ Endpoint	Official
10116	TCP	UDP	NetIQ VoIP Assessor	Official
10200	TCP		FRISK Software International's *fpscand* virus scanning daemon for Unix platforms [74]	Unofficial
10200	TCP		FRISK Software International's *f-protd* virus scanning daemon for Unix platforms [75]	Unofficial
10201–10204	TCP		FRISK Software International's *f-protd* virus scanning daemon for Unix platforms [75]	Unofficial
10308			Lock-on: Modern Air Combat	Unofficial
10480			SWAT 4 Dedicated Server	Unofficial
10823		UDP	Farming Simulator 2011 Default Server	Unofficial
10891	TCP		Jungle Disk (this port is opened by the Jungle Disk Monitor service on the localhost)	Unofficial
11211			memcached	Unofficial
11235			Savage:Battle for Newerth Server Hosting	Unofficial
11294			Blood Quest Online Server	Unofficial
11371			OpenPGP HTTP key server	Official
11576			IPStor Server management communication	Unofficial
12010	TCP		ElevateDB default database port [76]	Unofficial
12011	TCP		Axence nVision	Unofficial
12012	TCP		Axence nVision	Unofficial
12012	TCP		Audition Online Dance Battle, Korea Server—Status/Version Check	Unofficial
12012		UDP	Audition Online Dance Battle, Korea Server—Status/Version Check	Unofficial
12013	TCP	UDP	Audition Online Dance Battle, Korea Server	Unofficial
12035		UDP	Linden Lab viewer to sim on SecondLife	Unofficial
12222		UDP	Light Weight Access Point Protocol (LWAPP) LWAPP data (RFC 5412)	Official
12223		UDP	Light Weight Access Point Protocol (LWAPP) LWAPP control (RFC 5412)	Official
12345			NetBus—remote administration tool (often Trojan horse). Also used by NetBuster. Little Fighter 2 (TCP).	Unofficial
12489	TCP		NSClient/NSClient++/NC_Net (Nagios)	Unofficial

12975	TCP		LogMeIn Hamachi (VPN tunnel software; also port 32976)—used to connect to Mediation Server (bibi.hamachi.cc); will attempt to use SSL (TCP port 443) if both 12975 & 32976 fail to connect	Unofficial
12998–12999		UDP	Takenaka RDI Mirror World on SecondLife	Unofficial
13000–13050		UDP	Linden Lab viewer to sim on SecondLife	Unofficial
13008	TCP	UDP	Cross Fire, a multiplayer online First Person Shooter	Unofficial
13075	TCP		Default[77] for BMC Software Control-M/Enterprise Manager Corba communication, though often changed during installation	Official
13195-13196	TCP	UDP	Ontolux Ontolux 2D	Unofficial
13720	TCP	UDP	Symantec NetBackup—bprd (formerly VERITAS)	Official
13721	TCP	UDP	Symantec NetBackup—bpdbm (formerly VERITAS)	Official
13724	TCP	UDP	Symantec Network Utility—vnetd (formerly VERITAS)	Official
13782	TCP	UDP	Symantec NetBackup—bpcd (formerly VERITAS)	Official
13783	TCP	UDP	Symantec VOPIED protocol (formerly VERITAS)	Official
13785	TCP	UDP	Symantec NetBackup Database—nbdb (formerly VERITAS)	Official
13786	TCP	UDP	Symantec nomdb (formerly VERITAS)	Official
14439	TCP		APRS UI-View Amateur Radio[78] UI-WebServer	Unofficial
14567		UDP	Battlefield 1942 and mods	Unofficial
15000	TCP		psyBNC	Unofficial
15000	TCP		Wesnoth	Unofficial
15000	TCP		Kaspersky Network Agent	Unofficial
15000	TCP		hydap, Hypack Hydrographic Software Packages Data Acquisition	Official
15000		UDP	hydap, Hypack Hydrographic Software Packages Data Acquisition	Official
15567		UDP	Battlefield Vietnam and mods	Unofficial
15345	TCP	UDP	XPilot Contact	Official
16000	TCP		shroudBNC	Unofficial
16080	TCP		Mac OS X Server Web (HTTP) service with performance cache[79]	Unofficial
16200	TCP		Oracle Universal Content Management Content Server	Unofficial
16250	TCP		Oracle Universal Content Management Inbound Refinery	Unofficial
16384		UDP	Iron Mountain Digital online backup	Unofficial
16567		UDP	Battlefield 2 and mods	Unofficial
17500	TCP		Dropbox LanSync Protocol (db-lsp); used to synchronize file catalogs between Dropbox clients on your local network.	Official
17500		UDP	Dropbox LanSync Discovery (db-lsp-disc); used to synchronize file catalogs between Dropbox clients on your local network; is transmitted to broadcast addresses.	Official
18010	TCP		Super Dancer Online Extreme(SDO-X)—CiB Net Station Malaysia Server	Unofficial
18104	TCP		RAD PDF Service	Official
18180	TCP		DART Reporting server	Unofficial
18200	TCP	UDP	Audition Online Dance Battle, AsiaSoft Thailand Server—Status/Version Check	Unofficial
18201	TCP	UDP	Audition Online Dance Battle, AsiaSoft Thailand Server	Unofficial
18206	TCP	UDP	Audition Online Dance Battle, AsiaSoft Thailand Server—	Unofficial

			FAM Database	
18300	TCP	UDP	Audition Online Dance Battle, AsiaSoft SEA Server—Status/Version Check	Unofficial
18301	TCP	UDP	Audition Online Dance Battle, AsiaSoft SEA Server	Unofficial
18306	TCP	UDP	Audition Online Dance Battle, AsiaSoft SEA Server—FAM Database	Unofficial
18333	TCP		Bitcoin testnet[80]	Unofficial
18400	TCP	UDP	Audition Online Dance Battle, KAIZEN Brazil Server—Status/Version Check	Unofficial
18401	TCP	UDP	Audition Online Dance Battle, KAIZEN Brazil Server	Unofficial
18505	TCP	UDP	Audition Online Dance Battle, Nexon Server—Status/Version Check	Unofficial
18506	TCP	UDP	Audition Online Dance Battle, Nexon Server	Unofficial
18605	TCP	UDP	X-BEAT—Status/Version Check	Unofficial
18606	TCP	UDP	X-BEAT	Unofficial
19000	TCP	UDP	Audition Online Dance Battle, G10/alaplaya Server—Status/Version Check	Unofficial
19001	TCP	UDP	Audition Online Dance Battle, G10/alaplaya Server	Unofficial
19226	TCP		Panda Software AdminSecure Communication Agent	Unofficial
19283	TCP	UDP	K2 - KeyAuditor & KeyServer, Sassafras Software Inc. Software Asset Management tools	Official
19294	TCP		Google Talk Voice and Video connections [81]	Unofficial
19295		UDP	Google Talk Voice and Video connections [81]	Unofficial
19302		UDP	Google Talk Voice and Video connections [81]	Unofficial
19315	TCP	UDP	KeyShadow for K2 - KeyAuditor & KeyServer, Sassafras Software Inc. Software Asset Management tools	Official
19540	TCP	UDP	Belkin Network USB Hub	Unofficial
19638	TCP		Ensim Control Panel	Unofficial
19771	TCP	UDP	Softros LAN Messenger	Unofficial
19812	TCP		4D database SQL Communication	Unofficial
19813	TCP		4D database Client Server Communication	Unofficial
19814	TCP		4D database DB4D Communication	Unofficial
19880	TCP		Softros LAN Messenger	Unofficial
19999			DNP - Secure (Distributed Network Protocol - Secure), a secure version of the protocol used in SCADA systems between communicating RTU's and IED's	Official
20000			DNP (Distributed Network Protocol), a protocol used in SCADA systems between communicating RTU's and IED's	Official
20000			Usermin, Web-based user tool	Unofficial
20014	TCP		DART Reporting server	Unofficial
20720	TCP		Symantec i3 Web GUI server	Unofficial
21001	TCP		AMLFilter, AMLFilter Inc. amlf-admin default port	Unofficial
21011	TCP		AMLFilter, AMLFilter Inc. amlf-engine-01 default http port	Unofficial
21012	TCP		AMLFilter, AMLFilter Inc. amlf-engine-01 default https port	Unofficial
21021	TCP		AMLFilter, AMLFilter Inc. amlf-engine-02 default http port	Unofficial
21022	TCP		AMLFilter, AMLFilter Inc. amlf-engine-02 default https port	Unofficial
22136	TCP		FLIR Systems Camera Resource Protocol	Unofficial
22222	TCP		Davis Instruments, WeatherLink IP	Unofficial
22347	TCP	UDP	WibuKey, WIBU-SYSTEMS AG Software protection system	Official
22350	TCP	UDP	CodeMeter, WIBU-SYSTEMS AG Software protection system	Official
23073			Soldat Dedicated Server	Unofficial

23399			Skype Default Protocol	Unofficial
23513			Duke Nukem 3D#Source code Duke Nukem Ports	Unofficial
24444			NetBeans integrated development environment	Unofficial
24465	TCP	UDP	Tonido Directory Server for Tonido which is a Personal Web App and P2P platform	Official
24554	TCP	UDP	BINKP, Fidonet mail transfers over TCP/IP	Official
24800			Synergy: keyboard/mouse sharing software	Unofficial
24842			StepMania: Online: *Dance Dance Revolution* Simulator	Unofficial
25000	TCP		Teamware Office standard client connection	Official
25003	TCP		Teamware Office client notifier	Official
25005	TCP		Teamware Office message transfer	Official
25007	TCP		Teamware Office MIME Connector	Official
25010	TCP		Teamware Office Agent server	Official
25565			Minecraft Dedicated Server	Unofficial
25565			MySQL Standard MySQL port	Unofficial
25826		UDP	collectd default port [82]	Unofficial
25888		UDP	Xfire (Firewall Report, UDP_IN) IP Address (206.220.40.146) resolves to gameservertracking.xfire.com. Use unknown.	Unofficial
25999	TCP		Xfire	Unofficial
26000		UDP	id Software's *Quake* server	Official
26000	TCP		id Software's *Quake* server	Official
26000	TCP		CCP's EVE Online Online gaming MMORPG	Unofficial
26900	TCP		CCP's EVE Online Online gaming MMORPG	Unofficial
26901	TCP		CCP's EVE Online Online gaming MMORPG	Unofficial
27000		UDP	(through 27006) id Software's *QuakeWorld* master server	Unofficial
27000-27009	TCP		FlexNet Publisher's License server (from the range of default ports)	Unofficial
27010			Source engine dedicated server port	Unofficial
27014			Source engine dedicated server port (rare)	Unofficial
27015			GoldSrc and Source engine dedicated server port	Unofficial
27016			Magicka server port	Unofficial
27017			mongoDB server port	Unofficial
27374			Sub7 default.	Unofficial
27500		UDP	(through 27900) id Software's *QuakeWorld*	Unofficial
27888		UDP	Kaillera server	Unofficial
27900-27901			Nintendo Wi-Fi Connection	Unofficial
27901		UDP	(through 27910) id Software's *Quake II* master server	Unofficial
27960		UDP	(through 27969) Activision's *Enemy Territory* and id Software's *Quake III Arena*, *Quake III* and *Quake Live* and some ioquake3 derived games	Unofficial
28000			Bitfighter Common/default Bitfighter Server	Unofficial
28001			Starsiege: Tribes Common/default Tribes v.1 Server	Unofficial
28395	TCP		www.SmartSystemsLLC.com Used by Smart Sale 5.0	Unofficial
28785		UDP	Cube 2 Sauerbraten[83]	Unofficial
28786		UDP	Cube 2 Sauerbraten Port 2[83]	Unofficial
28910			Nintendo Wi-Fi Connection	Unofficial
28960		UDP	*Call of Duty*; *Call of Duty: United Offensive*; *Call of Duty 2*; *Call of Duty 4: Modern Warfare*; *Call of Duty: World at War* (PC Version)	Unofficial
29000			Perfect World International Used by the Perfect World	Unofficial

			International Client	
29900-29901			Nintendo Wi-Fi Connection	Unofficial
29920			Nintendo Wi-Fi Connection	Unofficial
30000			Pokémon Netbattle	Unofficial
30301			BitTorrent	Unofficial
30564	TCP		Multiplicity: keyboard/mouse/clipboard sharing software	Unofficial
30718		UDP	Lantronix Discovery for Lantronix serial-to-ethernet devices	Unofficial
30777	TCP		ZangZing agent	Unofficial
31337	TCP		Back Orifice—remote administration tool (often Trojan horse)	Unofficial
31415			ThoughtSignal—Server Communication Service (often Informational)	Unofficial
31456	TCP		TetriNET IRC gateway on some servers	Unofficial
31457	TCP		TetriNET	Official
31458	TCP		TetriNET Used for game spectators	Unofficial
32123	TCP		x3Lobby Used by x3Lobby, an internet application.	Unofficial
32245	TCP		MMTSG-mutualed over MMT (encrypted transmission)	Unofficial
32769	TCP		FileNet RPC	Unofficial
32976	TCP		LogMeIn Hamachi (VPN tunnel software; also port 12975)—used to connect to Mediation Server (bibi.hamachi.cc); will attempt to use SSL (TCP port 443) if both 12975 & 32976 fail to connect	Unofficial
33434	TCP	UDP	traceroute	Official
34443			Linksys PSUS4 print server	Unofficial
34567	TCP		dhanalakshmi.org EDI service[84]	Official
36963		UDP	Any of the USGN online games, most notably Counter Strike 2D multiplayer (2D clone of popular CounterStrike computer game)	Unofficial
37659	TCP		Axence nVision	Unofficial
37777	TCP		Digital Video Recorder hardware	Unofficial
40000	TCP	UDP	SafetyNET p Real-time Industrial Ethernet protocol	Official
41823	TCP	UDP	Murealm Client	Unofficial
43047	TCP		TheòsMessenger second port for service TheòsMessenger	Official
43048	TCP		TheòsMessenger third port for service TheòsMessenger	Official
43594–43595	TCP		Jagex, RuneScape, FunOrb, etc.	Unofficial
47001	TCP		WinRM - Windows Remote Management Service [85]	Official
47808	TCP	UDP	BACnet Building Automation and Control Networks (47808_{10} = $BAC0_{16}$)	Official
49151	TCP	UDP	Reserved[1]	Official

Dynamic, private or ephemeral ports: 49152–65535

The range above the registered ports contains dynamic or private ports that cannot be registered with IANA. It is used for custom or temporary purposes and for automatic allocation of ephemeral ports.

EAL (Evaluation Assurance Level)

Un article de Wikipédia, l'encyclopédie libre
(Redirigé depuis EAL4 +)

L'Evaluation Assurance Level (EAL1 travers EAL7) d'un produit ou système TI est une note numérique attribuée à l'issue d'un Common Criteria évaluation de la sécurité, une norme internationale en vigueur depuis 1999. Les niveaux d'assurance reflètent l'augmentation des exigences d'assurance ajoutée qui doivent être remplies pour obtenir la certification Common Criteria. L'intention des niveaux plus élevés est de fournir une plus grande confiance que les caractéristiques du système de sécurité fiable principaux sont mis en œuvre. Le niveau EAL ne mesure pas la sécurité du système lui-même, il indique simplement à quel niveau du système a été testé.

Pour parvenir à un EAL particulier, le système informatique doit répondre aux *exigences d'assurance* spécifique. La plupart de ces exigences impliquent la documentation de conception, d'analyse de conception, les tests fonctionnels, ou des tests de pénétration. L'EAL supérieur impliquent une documentation plus détaillée, l'analyse et de tests que ceux du bas. Atteindre un plus haut score EAL coûte généralement plus d'argent et prend plus de temps que d'atteindre un niveau inférieur. Le nombre EAL attribué à un système certifié indique que le système complété toutes les exigences pour ce niveau.

Bien que chaque produit et le système doit remplir les exigences *d'assurance* même d'atteindre un niveau particulier, ils n'ont pas à remplir les mêmes exigences *fonctionnelles.* Les caractéristiques fonctionnelles pour chaque produit certifié sont établis dans la *cible de sécurité* de documents adaptés à l'évaluation de ce produit. Par conséquent, un produit avec une plus grande EAL n'est pas nécessairement "plus sûr" dans une application particulière d'un avec un faible EAL, car ils peuvent avoir des listes très différentes des caractéristiques fonctionnelles dans leurs objectifs de sécurité. Un produit de fitness pour une application de sécurité en particulier dépend de la façon dont les caractéristiques énumérées dans la cible de sécurité du produit satisfaire aux exigences de sécurité de l'application. Si les objectifs de sécurité pour deux produits contiennent tous deux des fonctions de sécurité nécessaires, alors la plus élevée d'ALA *doivent* indiquer le produit le plus fiable pour cette application.

Contenu

Les niveaux d'assurance

EAL1: Testé fonctionnellement

EAL1 est applicable lorsqu'une certaine confiance dans le bon fonctionnement est nécessaire, mais les menaces à la sécurité ne sont pas considérées comme graves. Il sera d'une valeur où l'assurance indépendante est nécessaire pour appuyer l'affirmation selon laquelle un grand soin a été exercé à l'égard de la protection des renseignements personnels ou similaire. EAL1 fournit une évaluation de la TOE (cible d'évaluation) en tant que mises à la disposition du client, y compris des essais indépendants contre une spécification, et un examen de la documentation d'orientation fournis. Il est prévu que l'évaluation pourrait être EAL1 mené avec succès sans l'aide du développeur de la TOE, et pour un coût minime. Une évaluation à ce niveau doit fournir la preuve que la TOE fonctions d'une manière conforme à sa documentation, et qu'il offre une protection efficace contre les menaces identifiées.

EAL2: Testé structurellement

EAL2 nécessite la coopération des développeurs en termes de fourniture d'informations de conception et les résultats des tests, mais ne devrait pas exiger plus d'effort de la part du développeur que ce qui est conforme aux bonnes pratiques commerciales. Comme telle, elle ne devrait pas nécessiter un investissement considérablement augmenté du coût ou de temps. EAL2 est donc applicable dans les cas où les développeurs ou les utilisateurs ont besoin d'une faible à modéré le niveau de sécurité assuré indépendamment en l'absence de disponibilité de l'enregistrement complet de développement. Une telle situation peut survenir lorsque la sécurisation des systèmes hérités.

EAL3: Testé et vérifié méthodiquement

EAL3 permet un développeur de conscience à obtenir une assurance maximale de l'ingénierie de sécurité positive au stade de la conception sans modification substantielle des pratiques existantes de développement solide. EAL3 est applicable dans les cas où les développeurs ou les utilisateurs ont besoin d'un niveau modéré de la sécurité assurée indépendamment et nécessitent une enquête approfondie de la TOE et son développement sans substantielle ré-ingénierie.

EAL4: Méthodiquement conçu, testé et vérifié

EAL4 permet à un développeur d'obtenir une assurance maximale de l'ingénierie de la sécurité positive fondée sur les bonnes pratiques de développement commercial qui, bien que rigoureuse, ne nécessitent pas de connaissances spécialisées considérables, les compétences et autres ressources. EAL4 est le niveau le plus élevé au cours de laquelle il est susceptible d'être économiquement viable pour moderniser une ligne de produits existante. EAL4 est donc applicable dans les cas où les développeurs ou les utilisateurs ont besoin d'un niveau modéré à élevé de sécurité indépendamment assurée dans les orteils des matières premières traditionnelles et sont prêts à engager des coûts supplémentaires de sécurité spécifiques à l'ingénierie.

Commercial systèmes d'exploitation traditionnels qui fournissent des fonctions de sécurité basée sur l'utilisateur sont généralement évaluées à EAL4. Des exemples de tels systèmes d'exploitation sont AIX , [1] HP-UX , [1] FreeBSD , Novell NetWare , Solaris , [1] SUSE Linux Enterprise Server 9 , [1] [2] SUSE Linux Enterprise Server 10 , [3] Rouge Hat Enterprise Linux 5 , [4] Windows 2000 Service Pack 3, Windows 2003 , [1] [5] Windows XP [1] [5] , Windows 7 , [1] [6] et de Windows Server 2008 R2 [1] [6] .

Les systèmes d'exploitation qui fournissent sécurité multiniveau sont évalués à un minimum de niveau EAL4. Les exemples incluent Trusted Solaris , Solaris 10 11/06 Trusted Extensions , [7] une première version de la XTS-400 , et VMware ESXi version 3.0.2, [8] 3.5 et 4.0 (EAL 4 +).

EAL5: semi-formelle Conçu et testé

EAL5 permet à un développeur d'obtenir une assurance maximale de l'ingénierie de la sécurité basée sur des pratiques rigoureuses de développement commercial soutenu par l'application modérée de techniques d'ingénierie spécialiste de la sécurité. Une telle TOE sera probablement conçue et développée avec l'intention de réaliser EAL5 assurance. Il est probable que les coûts supplémentaires imputables à la EAL5 exigences, relatives au développement rigoureuse, sans l'application de techniques spécialisées, ne sera pas grande. EAL5 est donc applicable dans les cas où les développeurs ou les utilisateurs exigent un niveau élevé de sécurité indépendamment assurée dans un développement planifié et nécessitent une approche de développement rigoureux, sans entraîner de coûts excessifs attribuables à des techniques d'ingénierie spécialiste de la sécurité.

De nombreuses cartes à puce appareils ont été évalués à EAL5, comme l'ont fait à plusieurs niveaux dispositifs sécurisés tels que le Tenix lien interactif . XTS-400 (STOP 6) est un système d'exploitation à usage général qui a été évalué à EAL5 augmentée.

LPAR sur IBM System z est certifié EAL5. [9]

EAL6: Conception semi-formelle vérifié et testé

EAL6 permet aux développeurs d'obtenir une assurance élevée de l'application de techniques d'ingénierie de sécurité à un environnement de développement rigoureux afin de produire une TOE prime pour la protection des actifs de grande valeur contre les risques importants. EAL6 est donc applicable au développement de la TOE de sécurité pour une application dans des situations à haut risque où la valeur des biens protégés justifie les coûts supplémentaires.

Green Hills Software INTÉGRITÉ-178B RTOS a été certifié pour EAL6 augmentée. [1]

EAL7: Conception Formellement vérifié et testé

EAL7 est applicable au développement de la TOE de sécurité pour une application dans des situations de risque extrêmement élevé et / ou lorsque la valeur élevée des actifs justifie les coûts plus élevés. L'application pratique de EAL7 est actuellement limitée aux orteils avec des fonctionnalités de sécurité

étroitement ciblée qui se prêtent à l'analyse formelle extensive. Le Tenix lien interactif Diode Device Data et la diode de données Fox [10] ont été évalués à EAL7 augmentée.

Kernel Labs ouvert a également effectué la vérification formelle de leurs seL4 micronoyau OS, [11] permettant appareils exécutant seL4 pour atteindre EAL7. [12]

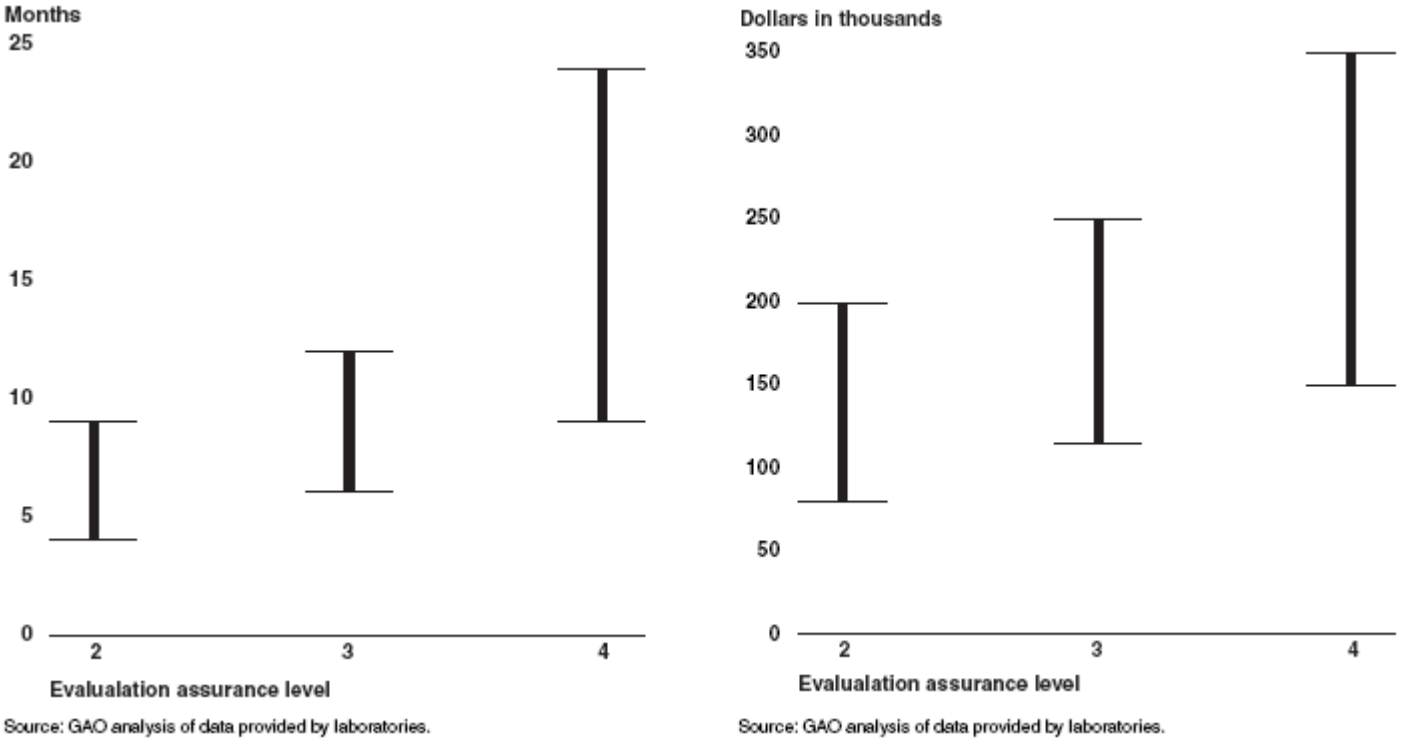
Fox-IT prétendent avoir certifié son sens unique de données dispositif de communication connu sous le nom «diode Fox données" à EAL7 +. [13]

Conséquences des niveaux d'assurance

Techniquement parlant, un plus EAL signifie rien de plus, ou moins, que l'évaluation complétée d'un ensemble d'exigences plus strictes d'assurance qualité. On suppose souvent que le système qui permet d'atteindre un plus haut EAL fournira ses fonctionnalités de sécurité plus fiable (et les tierces requises analyses et tests effectués par des experts en sécurité des preuves raisonnables dans ce sens), mais il ya peu ou pas de preuves publiées le soutien de cette hypothèse.

Impact sur les coûts et le calendrier

En 2006, les Etats-Unis Government Accountability Office a publié un rapport sur les évaluations selon les Critères communs qui résume toute une gamme de coûts et des horaires rapportés pour les évaluations effectuées au niveau EAL2 travers EAL4.



Gamme de temps de réalisation et les coûts pour les évaluations des critères communs à travers EAL2 EAL4.

Du milieu à la fin des années 1990, les vendeurs ont déclaré passer dollars américains 1 million et même des États-Unis $ 2,5 millions sur les évaluations comparables au niveau EAL4. Il n'ya pas eu de rapports publiés sur le coût des différents Microsoft Windows évaluations de sécurité.

Augmentation des besoins en ALA

Dans certains cas, l'évaluation peut être *augmentée* pour inclure les exigences d'assurance-delà du minimum requis pour un EAL particulier. Officiellement cela est indiqué par la suite le nombre EAL avec le mot **augmenté** et généralement avec une liste de codes pour indiquer les exigences supplémentaires. Comme la sténographie, les vendeurs vont souvent ajouter simplement un signe "plus" (comme dans **EAL4 +)** pour indiquer les exigences augmentées.

Notation EAL

Les normes Common Criteria EAL désigner comme indiqué dans cet article: le préfixe "EAL" concaténé avec un chiffre 1 à 7 (Exemples: EAL1, EAL3, EAL5). En pratique, certains pays accordent un espace entre le préfixe et le chiffre (EAL 1, EAL 3, EAL 5). L'utilisation d'un signe plus pour indiquer l'augmentation est une abréviation utilisée par les vendeurs informels de produits (EAL4 + ou EAL 4 +).