ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Pare-feu

www.ofppt.info

OFPPT

DIRECTION **R**ECHERCHE ET **I**NGENIERIE DE **F**ORMATION

SECTEUR NTIC

Sommaire

1. Présentation des pare-feu et des mandataires

La principale méthode pour se défendre des assaillants venus d'Internet est de mettre en place un pare-feu. Un pare-feu est un composant matériel, logiciel ou les deux. Le pare-feu Internet a pour but d'empêcher les paquets IP malveillants ou non souhaités d'accéder à un réseau sécurisé.
Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique. La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.
Cette menace est d'autant plus grande que la machine est connectée en permanence à internet pour plusieurs raisons :

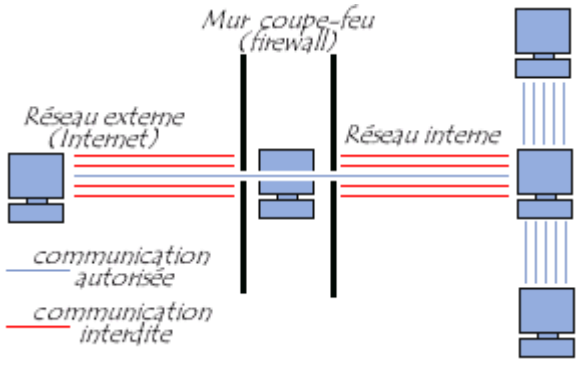
- La machine cible est susceptible d'être connectée sans pour autant être surveillée ;
- La machine cible est généralement connectée avec une plus large bande passante ;
- La machine cible ne change pas (ou peu) d'adresse IP.

Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des intrusions réseaux en installant un dispositif de protection.

2. Qu'est-ce qu'un pare-feu?.

Un **pare-feu** (appelé aussi *coupe-feu*, *garde-barrière* ou **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.



Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le traffic ;
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.
-

Dans le cas où le système pare-feu est fourni dans une boîte noire « clé en main », on utilise le terme d'« appliance ».

3. Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (*allow*) ;
- De bloquer la connexion (*deny*) ;
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

L'ensemble de ces règles permet de mettre en oeuvre une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées :
- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

4. Services proxy

Dans le secteur des réseaux, un service proxy est un logiciel qui interagit avec des réseaux extérieurs au nom d'un hôte client.

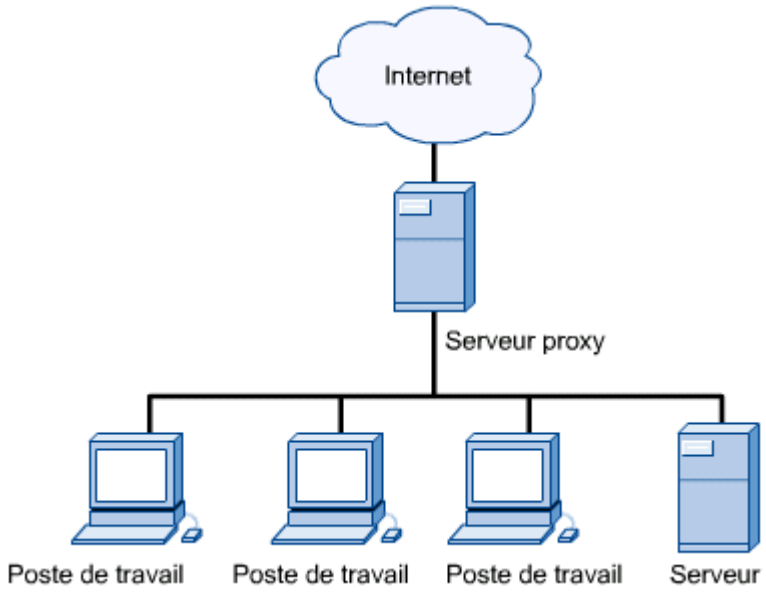


Figure 1

La figure 1représente le serveur proxy qui répond aux postes de travail.

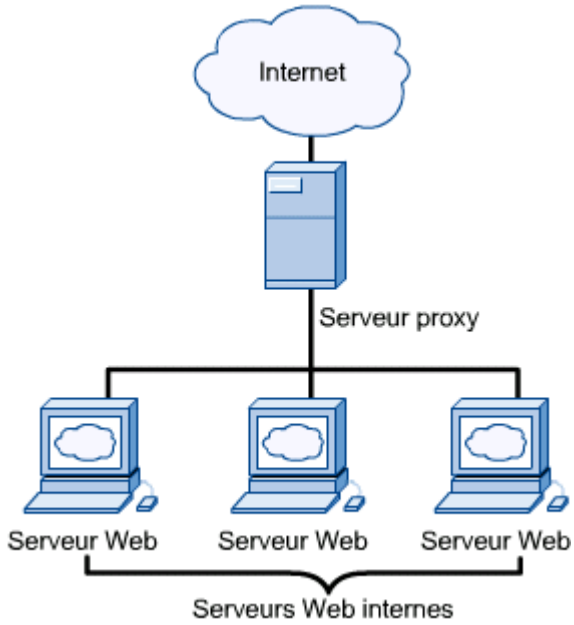


Figure 2

La figure 2représente un serveur proxy avec des serveurs Web internes. En règle générale, les hôtes client d'un réseau local sécurisé demandent une page Web à un serveur qui exécute des services proxy. Le serveur proxy accède alors à Internet pour récupérer la page Web. La page Web

est copiée sur le serveur proxy. Ce processus est appelé caching. Enfin, le serveur proxy transmet la page Web au client. En passant par l'intermédiaire des services d'un serveur proxy, le client n'a jamais à interagir directement avec les hôtes extérieurs. Les clients sont ainsi protégés des éventuelles menaces venues d'Internet. Les administrateurs peuvent configurer les serveurs proxy de manière à ce qu'ils rejettent certaines demandes client ou certaines réponses Internet extérieures. Par exemple, les écoles peuvent utiliser des serveurs proxy pour contrôler les sites Web accessibles. Étant donné que toutes les demandes Web sont dirigées vers le serveur proxy, les administrateurs contrôlent parfaitement les demandes traitées. Microsoft fournit un service proxy complet pour son NOS, appelé Microsoft Proxy Server 2.0.

Les serveurs proxy isolent les réseaux locaux et protègent les hôtes des menaces extérieures. L'efficacité des serveurs proxy repose sur leur capacité à mettre en cache les pages Web. La possibilité d'utiliser un service proxy pour HTTP constitue un réel avantage. De nombreux clients peuvent accéder au contenu HTTP avec un meilleur délai de réponse. Cette amélioration du délai de réponse est due au caching du contenu HTTP auquel les utilisateurs accèdent fréquemment sur un serveur local.

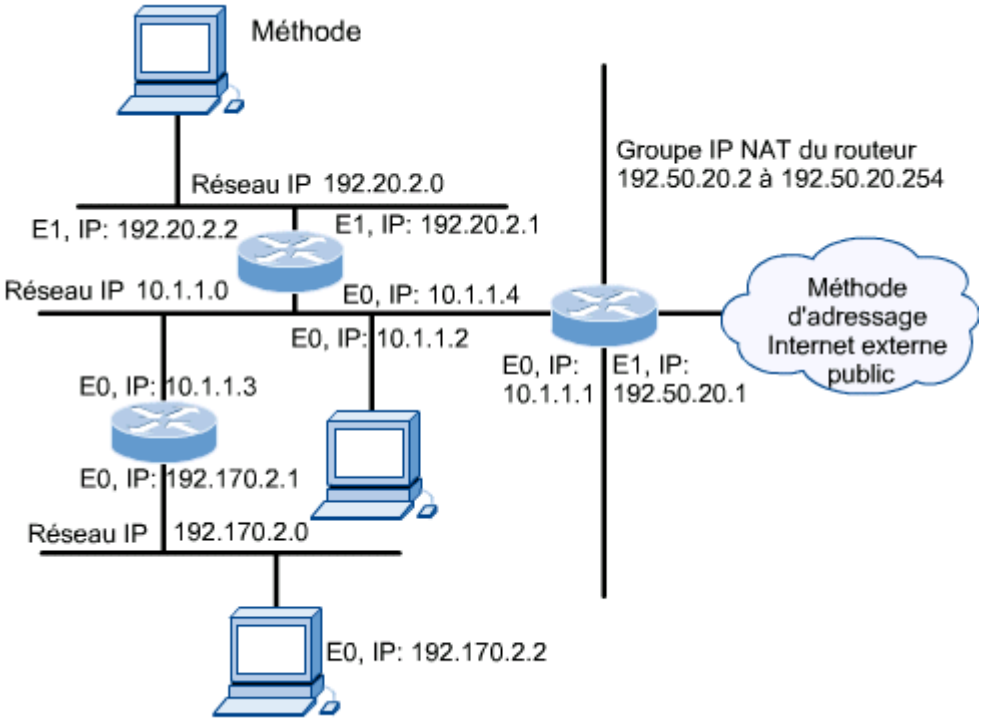
5. Traduction d'adresses réseau (NAT)

5.1. Principe du NAT

Le mécanisme de **translation d'adresses** (en anglais *Network Address Translation* noté **NAT**) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).

En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.

Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.



D'autre part, le mécanisme de translation d'adresses permet de **sécuriser** le réseau interne étant donné qu'il camoufle complètement l'adressage interne. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de la même adresse IP.

5.2. Espaces d'adressage

L'organisme gérant l'espace d'adressage public (adresses IP routables) est l'Internet Assigned Number Authority (IANA). La RFC 1918 définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse IP publique allouée par l'IANA. Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :

- Classe A : plage de 10.0.0.0 à 10.255.255.255 ;
- Classe B : plage de 172.16.0.0 à 172.31.255.255 ;
- Classe C : plage de 192.168.0.0 à 192.168.255.55 ;

Toutes les machines d'un réseau interne, connectées à internet par l'intermédiaire d'un routeur et ne possédant pas d'adresse IP publique doivent utiliser une adresse contenue dans l'une de ces plages. Pour les petits réseaux domestiques, la plage d'adresses de 192.168.0.1 à 192.168.0.255 est généralement utilisée.

5.3. Translation statique

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.
La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas

le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

5.4. Translation dynamique

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP. C'est la raison pour laquelle le terme de « mascarade IP » (en anglais IP masquerading) est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.
Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (PAT - Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

6. Filtrage de paquets

6.1. Le filtrage simple de paquets

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « *stateless packet filtering* »). Il analyse les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).
-

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80

4	Deny	any	any	any	any	any

Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).
Le port 23 est par exemple souvent bloqué par défaut par les dispositifs pare-feu car il correspond au protocole Telnet, permettant d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes à distance. Les données échangées par Telnet ne sont pas chiffrées, ce qui signifie qu'un individu est susceptible d'écouter le réseau et de voler les éventuels mots de passe circulant en clair. Les administrateurs lui préfèrent généralement le protocole SSH, réputé sûr et fournissant les mêmes fonctionnalités que Telnet.

6.2. Le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.
Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de **filtrage dynamique de paquets** est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglo-saxon est « **stateful inspection** » ou « *stateful packet filtering* », traduisez « *filtrage de paquets avec état* ».
Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.
Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en terme de sécurité.

7. Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.
Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).
Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou « proxy »), car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.
Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.
Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles afférentes pour être efficace.
Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission.

8. Les limites des firewalls

Un système pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité. C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du pare-feu.
De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.
Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer le pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et

les anomalies. Par ailleurs, il est recommandé d'effectuer une veille de sécurité (en s'abonnant aux alertes de sécurité des CERT par exemple) afin de modifier le paramétrage de son dispositif en fonction de la publication des alertes.
La mise en place d'un firewall doit donc se faire en accord avec une véritable politique de sécurité.

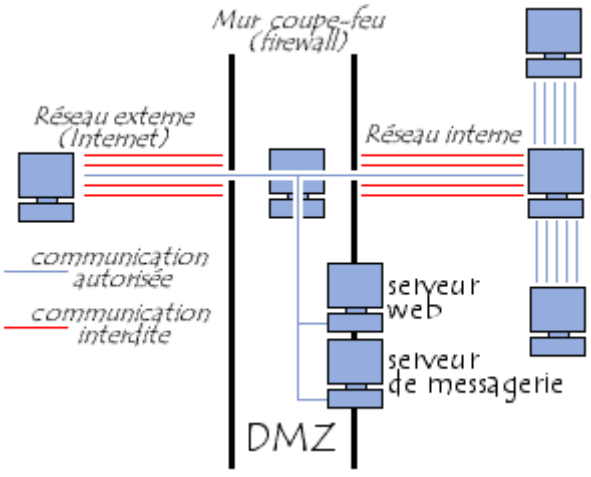
9. DMZ (Zone démilitarisée)

9.1. Notion de cloisonnement

Les sytèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feux permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « **cloisonnement des réseaux** » (le terme *isolation* est parfois également utilisé).

9.2. Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « **zone démilitarisé** » (notée **DMZ** pour *DeMilitarized Zone*) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.



Les serveurs situés dans la DMZ sont appelés « **bastions** » en raison de leur position d'avant poste dans le réseau de l'entreprise.
La politique de sécurité mise en oeuvre sur la DMZ est généralement la suivante :

- Traffic du réseau externe vers la DMZ autorisé ;
- Traffic du réseau externe vers le réseau interne interdit ;

- Traffic du réseau interne vers la DMZ autorisé ;
- Traffic du réseau interne vers le réseau externe autorisé ;
- Traffic de la DMZ vers le réseau interne interdit ;
- Traffic de la DMZ vers le réseau externe refusé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.
Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

10. Emplacement du pare-feu

Il est aussi essentiel de savoir où placer un pare-feu Internet que de savoir configurer les règles du filtrage des paquets.

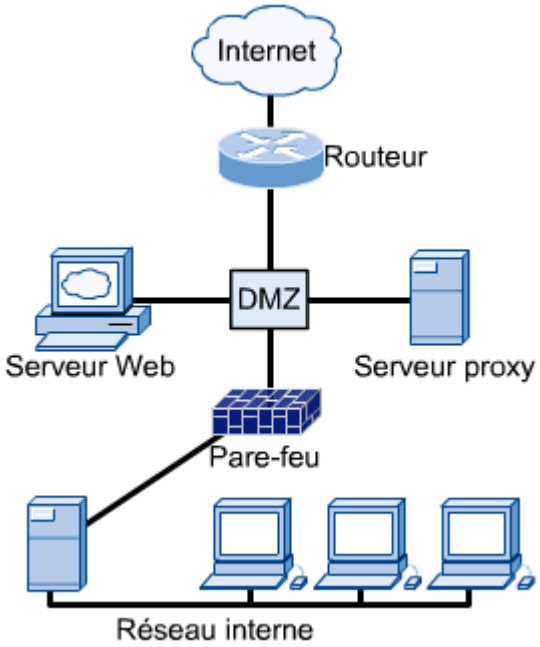


Figure 3

La figure 4 illustre l'emplacement standard du pare-feu. Un routeur de frontière connecte le réseau local de l'entreprise à son FAI ou à Internet. L'interface de réseau local du routeur de frontière pointe vers un réseau conçu pour l'accès public. Ce réseau contient des serveurs NOS qui permettent d'accéder au Web, à la messagerie, ainsi qu'à d'autres services de l'Internet public. Ce réseau public est parfois appelé réseau local sacrifié. Ce qualificatif est dû au fait que les demandes publiques sont autorisées sur le réseau. Il est parfois nommé également zone DMZ (zone démilitarisée). La DMZ fonctionne comme une zone de mémoire tampon. Le routeur de frontière doit comporter un filtre IP qui protègera

le système contre les failles évidentes. Par exemple, le protocole de gestion SNMP ne doit pas être autorisé en entrée sur le réseau. Les serveurs NOS de la DMZ doivent être configurés rigoureusement. Le routeur de frontière ne doit autoriser que certains types de trafic particuliers sur ces serveurs. Dans la figure 4, le routeur de frontière ne doit autoriser que les trafics HTTP, FTP, messagerie et DNS.
Une solution de pare-feu dédié, du type PIX (Cisco Private Internet eXchange), établit une connexion entre la DMZ et le réseau local protégé. Ce dispositif offre des fonctions supplémentaires de filtrage IP, filtrage dynamique, services proxy et/ou NAT.
La DMZ est conçue pour protéger le réseau interne. L'exemple illustré à la figure 4 présente une configuration basique. Vous serez souvent amené à rencontrer des variations complexes des éléments présentés dans cette section.

11. Utilisation d'un pare-feu

Un firewall est un logiciel contrôlant les échanges entre un réseau (local ou Internet) et votre ordinateur. Le pare-feu examine les données entrantes et les données sortantes de l'ordinateur.

11.1. 1.a Les données entrantes

Le contrôle des données entrantes est utilisé principalement pour la connexion au réseau Internet : en effet, lorsque vous êtes connectés, un grand nombre d'autres ordinateurs viennent interroger le vôtre pour voir si votre ordinateur "répond". Le pare-feu protège votre ordinateur en gardant les "portes d'accès" appelées les ports. Dans la plupart des cas, le firewall bloque automatiquement ces ports afin d'éviter qu'un intrus pénètre dans votre ordinateur.

11.2. Les données sortantes

Le contrôle des données sortantes ne peut s'effectuer automatiquement : c'est à l'utilisateur de demander au firewall de fermer ou d'ouvrir les portes d'accès. Les données sortantes sont en fait les programmes qui demandent une connexion à Internet, soit pour vérifier s'il existe des mises à jour, soit pour transmettre des statistiques, soit pour fonctionner (On imagine mal qu'un navigateur Internet comme Internet Explorer ou Mozilla Firefox vous permette de naviguer sur le Web si vous lui refusez l'accès à l'Internet) etc ...

Certains programmes peuvent être équipés de spywares !! Et peuvent ainsi transmettre vos informations personnelles aux sites web. Par exemple, le lecteur Windows Media 9 transmettait des informations à Microsoft sur le nom des DVD que les utilisateurs visionnaient. Un virus ou un cheval de troie disposant de son propre exécutable est alors facilement identifiable pour l'utilisateur. Il est donc impératif de ne pas négliger les données sortantes !

11.3. Comment utiliser un firewall ?

11.3.1. Les alertes

Lorsqu'un échange se prépare, le firewall informe l'utilisateur du type de données (sortantes/entrantes), de l'adresse IP et du port concernés (sous la forme IP.IP.IP.IP:PORT), le nom de domaine (le "site") qui envoie la demande (si disponible), et, dans le cas du contrôle de programme, le firewall demande à l'utilisateur s'il faut bloquer ou ouvrir les ports. Pour les données entrantes, il est possible de désactiver les alertes dans la mesure où le firewall n'attend pas de réponse de l'utilisateur et bloque automatiquement les ports.

11.3.2. 2.b Comment savoir s'il faut ouvrir ou bloquer les ports ? (Contrôle des programmes)

Tout d'abord, il faut impérativement savoir identifier le programme qui tente de se connecter à Internet, dans le cas contraire, il vaut mieux bloquer l'accès temporairement et chercher avec un moteur de recherche à quoi correspond l'exécutable. Si le programme fonctionne uniquement grâce à Internet (navigateur, antivirus, module de connexion, logiciel de messagerie instantanée ...) vous pouvez alors ouvrir les ports (Il est possible d'attribuer un choix par défaut, afin d'éviter de toujours cliquer sur "bloquer" ou "autoriser"). Si le programme n'a aucune raison de se connecter à Internet (à moins de vous prévenir d'une nouvelle version mise à jour) (Traitement de texte, logiciel de gravure, et autres logiciels ne fonctionnant pas grâce à Internet), il est alors conseillé de bloquer les ports. Si vous ne connaissez pas le logiciel, bloquez les ports, et renseignez-vous sur le forum.

11.3.3. Comment utiliser mon firewall avec plusieurs connexions réseau ?

Lorsque vous utilisez un réseau local, le firewall va également filtrer ce réseau. Pour y remédier, il suffit d'enregistrer les adresses IP des ordinateurs du réseau local ou le nom de la carte réseau en tant que 'Zone sûre', ou d'autoriser toute connexion vers cette adresse IP. Vous pouvez également placer des IP ou cartes réseau dans une 'Zone dangereuse' ; définissez ensuite un niveau de protection élevé pour le réseau Internet, moyen ou désactivé pour la zone sûre (le niveau Moyen est conseillé, désactivez le firewall uniquement si vous rencontrez des problème avec un niveau de protection moyen) et "Bloquer tout" pour la zone dangereuse.

Votre pare-feu est maintenant prêt à l'utilisation !

11.3.4. Un firewall est-il compliqué à utiliser ?

On ne peut pas promettre que tout va se faire en un clin d'oeil. Tout d'abord, tâchez de choisir un pare-feu simple d'utilisation, plutôt que de choisir un pare-feu complet pour lequel il nous faudra nous-même définir les règles de filtrage. Un firewall comme ZoneAlarm vous avertira la première fois qu'une intrusion a été détectée, vous aurez simplement à

lui demander de ne plus afficher les alertes pour qu'il vous laisse tranquille. Par contre, les alertes pour les connexions sortantes (pour autoriser les programmes à se connecter à Internet) resteront affichées. Mais il est heureusement possible de demander au logiciel d'enregistrer les paramètres choisis.

En résumé, après l'installation d'un pare-feu, il nous suffit de quelques jours d'utilisation de la machine pour lui expliquer quels programmes autoriser ou interdire d'accéder à Internet. Ensuite, il se fait discret.